

**Chokepoints: Internet Intermediaries and the
Private Regulation of
Counterfeit Goods on the Internet**

Natasha Marie Tusikov

July 2014

A thesis for the degree of Doctor of Philosophy of

The Australian National University

Canberra, Australia

Declaration

I hereby state that the following thesis is entirely my own original work and has not been submitted for any other degree at any other university or education institution. All sources of information used in the thesis have been indicated and due acknowledgement has been given to the work of others.

Signed:

Natasha Marie Tusikov

Date: 13 July 2014

Acknowledgements

I would like to thank the people who helped me with this project. Thanks first to my supervisor Peter Drahos and my advisors Peter Grabosky and Kathryn Henne for providing good advice, asking critical questions and encouraging me to look at the big picture. It was a great privilege to write this dissertation at the Regulatory Institutions Network and I benefited immensely from the collegial intellectual environment.

I want to express my gratitude to the interviewees who agreed to participate in this research and generously shared their knowledge and experience with me.

To my uncles—Vit and Valdi Tusikov—for providing a beachside retreat in Mollymook with wine and oysters, my sincere gratitude. Thanks also my parents, Peter and Barbara Tusikov, and my sister Katrina for patiently listening to years of discussions of transnational private regulation and counterfeit goods. I also want to thank Charles Murray, a lifelong friend. Finally, and most importantly, my deep thanks to my partner, Blayne Haggart, for all your support and help.

Abstract

This dissertation examines non-state regulation on the Internet, specifically the capacity of corporate actors to create private regulatory arrangements and the degree to which those efforts may rely upon the state. It critically traces the interactions and inter-dependencies between corporate actors and the state through the lens of corporate online anti-counterfeiting enforcement efforts. Between 2010 and 2013, small groups of multinational corporations and government officials from the United States, United Kingdom and the European Commission created a global private regulatory regime to control websites selling counterfeit goods. In this regime, for the first time, major U.S.-based Internet firms, like Google and PayPal, adopted so-called “voluntary best practices” agreements that guide their regulation of these websites on behalf of rights holders of intellectual property. This project examines eight of these agreements that pertain to five Internet sectors: advertising, domain name, marketplace, payment, and search services.

In this particular case of private regulation, the state plays a strong, even central role. “Voluntary agreements” are a deliberate misnomer as government actors, acting in concert with rights holders, employed varying degrees of coercion to pressure major Internet firms and payment providers to adopt industry-derived best practices. Despite these coercive elements, however, there are common financial and reputational interests between rights holders and Internet firms. More importantly, these agreements serve strategic economic and national security interests, particularly those of the United States. The U.S. government, the principal architect of the regime, has interests in the protection of intellectual property because of its large stable of successful rights holders. In addition, it has national security interests in tapping into the vast troves of personal and commercial data that firms, such as Google and Yahoo, collect from their users.

Corporate agreements to regulate the online distribution of counterfeit goods speak to private regulation on the Internet more generally. This dissertation contends that

large corporate actors—both rights holders and Internet firms—can act as arbiters on the legality of technologies, services and applications on the Internet. In doing so, they can have significant influence in determining what types of new technologies and services prosper and which fail. Corporate anti-counterfeiting efforts demonstrate not only the considerable regulatory capacity of these Internet firms but also state and corporate interests in working with these firms to set rules and standards that govern Internet services.

Table of Contents

List of Tables	xii
List of Appendices	xii
Abbreviations	xiii
Chapter 1: Non-State Regulation on the Internet	1
i) <i>From Failed Legislation to Backroom Deals</i>	3
I) Research Problem and Questions	7
II) Why Trademark Infringement?	10
i) <i>Importance of Intellectual Property</i>	10
ii) <i>Trademarks and Counterfeiting</i>	12
iii) <i>Trademarks are Forever</i>	14
iv) <i>Protecting Multi-Billion-Dollar Brands</i>	16
v) <i>Rights Holders Controlling Value Chains</i>	20
vi) <i>Reaping Rewards from Intellectual Property</i>	22
IV) From Flea Markets to eBay	24
i) <i>Evolution of Anti-Counterfeiting Efforts</i>	24
ii) <i>Corporate Anti-Counterfeiting Efforts</i>	25
iii) <i>Infringing Sites and the Problem of “Whack a Mole”</i>	27
iv) <i>State and Corporate Inter-dependencies</i>	30
V) Review of Literature: Where Transnational Policing and Corporate Regulation Meet	32
VI) Theoretical Framework and Methodology	34
i) <i>Theoretical Framework</i>	34
ii) <i>Methodology</i>	35
iii) <i>Research Methods</i>	37
VII) Argument	38
VIII) Overview of Chapters	41
Chapter 2: Regulating Through the State	42
I) Conceptualising the State’s Role in Regulation	43
i) <i>Governing through Regulation</i>	44
II) Corporations as Regulators	45
i) <i>Corporations Setting and Enforcing Rules</i>	45

ii) <i>Corporate and State Interest in Private Regulation</i>	47
III) Regulatory Regimes	48
i) <i>Employing the Concept of Private Regimes</i>	48
IV) Private Authority	50
i) <i>Claiming Private Authority</i>	
ii) <i>Seeking Legitimacy for Private Authority</i>	53
iii) <i>Limitations of Private Authority</i>	54
iv) <i>Role of the State in the Private Anti-Counterfeiting Regime</i>	55
V) Techno-Regulation	57
i) <i>From Cyber-libertarianism to Techno-Regulation</i>	57
ii) <i>Regulation in the Online Environment</i>	59
iii) <i>Regulation Through Technology</i>	60
iv) <i>The Rise of Macro-intermediaries</i>	62
VI) The Private Anti-Counterfeiting Regime	64
i) <i>Corporate Online Anti-Counterfeiting Efforts</i>	64
Chapter 3: Macro-Intermediaries and Informal Private Regulation on the Internet	67
I) Setting Standards Globally to Protect Intellectual Property Rights	69
i) <i>Trade Associations Shaping Public Policy</i>	70
ii) <i>Shaping Policymaking Through Trade Agreements</i>	72
iii) <i>Shaping Policies through Economic Sanctions</i>	75
iv) <i>Rights Holders' Authority to Set Rules</i>	77
II) From TRIPS to Regulation of Online Infringement	79
i) <i>Challenges and Advantages of Online Enforcement</i>	80
ii) <i>The DMCA: Setting the Standard for Online Enforcement</i>	82
III) Expansion of Online Enforcement Efforts Against Infringement	84
i) <i>Emergence of "Voluntary" Enforcement Initiatives</i>	85
ii) <i>Four Doomed Intellectual Property Bills in the United States</i>	88
a) <i>Combating Online Infringements and Counterfeits Act</i>	88
b) <i>Protect Intellectual Property Act</i>	89
c) <i>Stop Online Piracy Act</i>	90
d) <i>Online Protection and Enforcement of Digital Trade Act</i>	92
e) <i>Protests over PIPA and SOPA</i>	92
f) <i>Legitimising Intermediaries as Gatekeepers</i>	93
IV) Framing the Debate over Online Enforcement	94
i) <i>Framing the Concept of Intellectual Property</i>	95
ii) <i>Advocates for SOPA</i>	96
iii) <i>Opponents of SOPA</i>	97
iv) <i>Inter-Play of Interests</i>	98

V) Creation of Private Enforcement Agreements	99
i) <i>Inter-dependent Interests</i>	100
ii) <i>Uncertain Regulatory Landscape</i>	102
iii) <i>Limitations of Private Authority</i>	103
iv) <i>Office of the U.S. Intellectual Property “Czar”</i>	104
v) <i>Agreements in the United Kingdom and European Union</i>	105
vi) <i>Global Private Regulatory Regime</i>	107
Chapter 4: Revenue Chokepoints using Payment and Advertising Intermediaries	109
I) Online Payment and Advertising Industries	111
i) <i>How Online Payment Processing Works</i>	114
ii) <i>How Online Advertising Works</i>	117
II) Pressure on Marketplaces from State and Industry	118
i) <i>Regulating Payment Providers</i>	120
ii) <i>Payment Providers’ Informal Agreements</i>	121
iii) <i>Regulating Advertising Platforms</i>	124
iv) <i>Advertising Platforms’ Informal Agreements</i>	127
III) Intermediaries’ Enforcement Programs	131
i) <i>Payment Intermediaries’ Enforcement Policies</i>	133
ii) <i>Payment Providers’ Private Enforcement Agreements</i>	133
iii) <i>Account Termination Programs</i>	133
a) International Anti-Counterfeiting Coalition Program	134
b) Canadian Anti-Fraud Centre Program	135
iii) <i>Advertising Intermediaries’ Enforcement Policies</i>	136
iv) <i>Advertising Intermediaries’ Enforcement Programs</i>	137
a) Ad Networks’ Private Enforcement Agreement	138
b) Digital Trading Standards Group	139
IV) Analysis of Intermediaries’ Enforcement Measures	140
i) <i>Payment Macro-Intermediaries</i>	141
ii) <i>Advertising Macro-Intermediaries</i>	143
V) State Pressure and Actors’ Interests	144
i) <i>Role of the State</i>	145
ii) <i>State and Corporate Interests in Informal Private Regulation</i>	147
iii) <i>Consumers’ Interests</i>	148
VI) Conclusion	149
Chapter 5: Access Chokepoints: Search and Domain Intermediaries	151
I) Search and Domain Names Service Industries	153
i) <i>How Search Engines Work</i>	156
ii) <i>How the Domain Name System Works</i>	157

II) Pressure on Marketplaces from State and Industry	159
i) <i>Regulating Search Engines</i>	161
ii) <i>Regulating Domain Registrars</i>	163
iii) <i>Creation of Private Enforcement Agreements</i>	164
III) Intermediaries' Enforcement Programs	168
i) <i>Search Intermediaries' Enforcement Policies</i>	169
a) <i>Search Engine Code of Conduct</i>	170
b) <i>Changes to Google's Enforcement Practices</i>	173
ii) <i>Domain Intermediaries' Enforcement Policies</i>	174
a) <i>Centre for Safe Internet Pharmacies</i>	176
IV) Analysis of Intermediaries' Enforcement Measures	178
i) <i>Google's Regulatory Capacity</i>	179
ii) <i>GoDaddy's Regulatory Capacity</i>	180
V) State Pressure and Actors' Interests	182
i) <i>The Role of the State</i>	182
ii) <i>State and Corporate Interests in Informal Private Regulation</i>	184
iii) <i>Consumers' Interests</i>	186
VI) Conclusion	188
Chapter 6: Online Marketplaces and Private Enforcement Agreements	190
I) Online Marketplaces	193
i) <i>eBay and Taobao Marketplaces</i>	193
ii) <i>How Online Marketplaces Work</i>	195
II) Pressure on Marketplaces from Industry and State	197
i) <i>Legislative frameworks</i>	197
ii) <i>Pressure from Rights Holders</i>	199
iii) <i>Pressure Through the State</i>	203
III) Intermediaries' Enforcement Programs	205
i) <i>eBay's Enforcement Policies</i>	206
a) <i>European Commission's Memorandum of Understanding</i>	208
ii) <i>Taobao's Enforcement Policies</i>	210
b) <i>Taobao's Memorandum of Understanding</i>	211
IV) Analysis of Intermediaries' Enforcement Measures	212
i) <i>Results of Private Enforcement Agreements</i>	213
ii) <i>Perspectives on Private Regulation</i>	215
V) State Pressure and Actors' Interests	216
i) <i>Role of the State</i>	217
ii) <i>State and Corporate Interests in Informal Private Regulation</i>	218
iii) <i>Consumers' Interests</i>	219

VI) Conclusion	220
Chapter 7: Private Regimes and the Public Interest	222
I) Private Anti-Counterfeiting Regime	224
i) <i>State Coercion Underlying Private Regulation</i>	226
a) Soft Pressure	227
b) Shaming, Threats of Legislation and Legal Action	228
c) Market Leverage	229
II) Nature and Limitations of Private Authority	231
i) <i>Rights Holders Making Rules</i>	231
ii) <i>Constraints on Rights Holders' Authority</i>	232
iii) <i>Calling Upon the State</i>	233
III) Corporate Interests in Private Informal Regulation	234
i) <i>Reputational and Legal Concerns</i>	234
ii) <i>Flexibility and Beneficial Terms</i>	235
iii) <i>Disadvantages for Macro-Intermediaries</i>	236
a) No Immunity from Liability	236
b) Costs of Enforcement	237
IV) State Interests In Informal Private Regulation	238
i) <i>Inter-dependence amongst Corporate and State Interests</i>	238
a) Ever-Increasing Protection of Intellectual Property	239
b) Entrenched Interests and the Rising "Big Tech" Lobbying Force	240
c) Expanding States' Regulatory Capacity Online	242
ii) <i>Flexibility and Secrecy: Plausible Deniability</i>	244
V) Regulation through Technology	246
i) <i>Politics Shaping Technologies</i>	247
ii) <i>Drawbacks to Regulating through Technology</i>	248
a) Weak Due-Process Measures	249
VI) Missing Voices: Consumer Interests in the Private Regime	250
i) <i>Consumers' Interests in Marketplaces</i>	251
i) <i>Negative Economic Effects of Informal Private Agreements</i>	252
a) Anti-Competitive Behaviour	253
VIII) Conclusion	255
i) <i>Locating the Public Interest in Private Regulatory Regimes</i>	256
ii) <i>Toward a Digital Bill of Rights</i>	257
a) A Call for Transparency	258
b) Marco Civil – a Useful Roadmap	258
c) A Path to Digital Rights	260

Chapter 8: Locating the Public Interest in Private Regulation	262
I) Overview and Key Findings	263
II) Challenging Private Regulation on the Internet	267
i) <i>Procedural and Normative Problems</i>	268
ii) <i>Preliminary Steps for Greater Transparency</i>	270
a) Industry Transparency Reports	271
iii) <i>Transparency and the State</i>	274
III) Conclusion: A Future with Digital Rights	275
 References	 279
I) Legislation, Legal Cases, and Agreements	279
II) Academic	280
III) Government	292
IV) Industry	296
V) Media	300

List of Tables

Table 1.1: Internet Intermediaries	4
Table 1.2: Internet Macro-intermediaries' Enforcement Capabilities	6
Table: 1.3: Key Private Enforcement Agreements	8
Table 1.4: Billion-Dollar Brands	18
Table 1.5: Findings From Intellectual Property Industry Studies	23
Table 3.1: Comparison of Intermediaries – Private Right of Action	90
Table 3.2: Comparison of Intermediaries – Voluntary Actions	91
Table: 3.3: Private Enforcement Agreements	106
Table 4.1: Processing Payments Online	116
Table 4.2: U.S. Informal Agreements with Advertising Actors	128
Table 4.3: Merchant-Account Termination Programs	142
Table 5.1: Comparison of Codes for Search Engines	171
Table 5.2: Comparison of Proposed and Actual Rules for Search Engines	174
Table 5.3: Domain Intermediaries' Enforcement Measures	175
Table 6.1: Key Provisions in European Commission's Agreement	209

Appendices

Appendix A: List of Interviews	308
Appendix B: Best Practices to Address Copyright Infringement and the Sale of Counterfeit Products on the Internet	313
Appendix C: Best Practices for Rights Holders with Payment Processors	317
Appendix D: UK search: the way ahead (Search Engines' Proposed Code)	319
Appendix E: Responsible Practices for Search Engines in Reducing Online Infringement Proposal for a Code of Practice (Rights Holders' Proposed Code)	328

Abbreviations

ACTN	Advisory Committee for Trade Negotiations
ANA	Association of National Advertisers
BSA	Business Software Alliance
CAFC	Canadian Anti-Fraud Centre
COICA	Combatting Online Infringements and Counterfeits Act
CSIP	Centre for Safe Internet Pharmacies
DCMS	Department for Culture, Media and Sport
DMCA	Digital Millennium Copyright Act
FDA	U.S. Food and Drug Administration
GATT	General Agreement on Tariffs and Trade
IAB	Interactive Advertising Bureau
IACC	International Anti-Counterfeiting Coalition
ICANN	Internet Corporation of Assigned Names and Numbers
INTA	International Trademark Association
ITIF	Information Technology and Innovation Foundation
IPC	Intellectual Property Committee
IPEC	Intellectual Property Enforcement Coordinator
MPAA	Motion Picture Association of America
OECD	Organisation for Economic Cooperation and Development
OPEN	Online Protection and Enforcement of Digital Trade Act
PIPA	Protect Intellectual Property Act
RIAA	Recording Industry Association of America
SOPA	Stop Online Piracy Act

TPP	Trans-Pacific Partnership
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property
U.K.	United Kingdom
U.S.	United States
USTR	Office of the United States Trade Representative
WIPO	World Intellectual Property Organisation
WTO	World Trade Organisation

Chapter 1: Non-State Regulation on the Internet

The famous Internet Blackout on January 18, 2012, represented the culmination of months of protests against two intellectual property bills in the United States. These bills were the *Stop Online Piracy Act* (SOPA) in the U.S. House of Representatives and its sister bill from the U.S. Senate, the *Protect Intellectual Property Act* (PIPA). Before that day, intellectual property had generally been regarded, at least in public discourse, as a relatively arcane, commercial matter. SOPA and PIPA would have targeted websites (hereafter “sites”) globally that sold counterfeit goods. Counterfeit goods are unauthorised reproductions of trademarked products and a form of trademark infringement. Trademarks are the symbols or logos that represent a particular company or product, like the famous Nike ‘swoosh.’ These bills also would have targeted sites that offer unauthorized downloads of copyrighted content, particularly movies, music or software, that are protected in intellectual property law as creative or artistic works.¹

Internet “intermediaries” were a key target of the bill. These intermediaries play an increasingly large and complex role in addressing various types of online wrongdoing, including the infringement of intellectual property rights. Internet intermediaries facilitate access to or the hosting of information on the Internet, like search engines. They also enable transactions or interactions among Internet users. This includes social media platforms, like Facebook and Twitter, and payment providers, like PayPal. PIPA and SOPA would have required intermediaries to play a greater role regulating sites that infringe intellectual property rights. Regulation in this dissertation refers to the process of setting, implementing and enforcing rules or standards, whether by state or non-state actors.

PIPA and SOPA focused on the problem of so-called “infringing sites.”² This broadly conceived term referred to all manner of websites that may distribute

¹ Another type of intellectual property, which was not included in SOPA or PIPA is patents, which relate to industrial methods or processes, like pharmaceutical formulas.

² SOPA defined “foreign infringing sites” as sites or a “portion thereof” that were directed toward and used by individuals in the United States, in which the site operator “is committing or

counterfeit or copyright-infringing goods. SOPA and PIPA would have required action against infringing sites from the following intermediaries:

- payment providers (e.g., Visa and PayPal);
- search engines (e.g., Google, Yahoo and Microsoft's Bing);
- advertising platforms (e.g., Google and Yahoo); and
- domain name registrars (e.g., GoDaddy).³

Under the proposed legislation, rights holders of intellectual property, such as Apple or Pfizer, could seek court orders to require these intermediaries to withdraw their services from sites distributing copyright-infringing or counterfeit goods. Under certain circumstances, the bills also would have granted rights holders a private right of action to work directly with intermediaries to target sites identified by rights holders as infringing sites.⁴ In some cases the bills also would have permitted certain intermediaries to act voluntarily against particular types of infringing sites that unlawfully distributed pharmaceuticals.⁵

Critics of the bills said they would endanger free expression on the Internet, extend punitive U.S.-style enforcement strategies globally and, because of the types of technical enforcement measures proposed, potentially damage Internet infrastructure (see Lemley, Levin, and Post 2011).⁶ These bills were explicitly designed to favour rights holders, particularly large institutional copyright owners in the movie and music industries, at the expense of Internet firms that provide essential Internet services. Entirely absent from the bills was any consideration of Internet users or the general public that rely upon the Internet to participate fully in economic, social and cultural life. Public anger against the bills brought together a transnational coalition of academics, technologists, civil-society activists, Internet users and Internet giants (Sell 2013).

facilitating the commission of criminal violations," including trafficking in counterfeit goods or services (SOPA Sec. 102).

³ Domain registrars, likely the least familiar of this group, help manage the global domain name system and enable individuals and companies to register and operate domain names (e.g., nytimes.com).

⁴ SOPA Sec. 103.

⁵ SOPA Sec. 105.

⁶ SOPA proposed to use the domain name system, which enables users to access the same sites from anywhere in the world to block access to infringing sites. Critics argued it would destabilise the system (Lemley, Levin, and Post 2011).

The scale of the protest startled U.S. legislators, who had never before encountered such heated public opposition in relation to intellectual property. At the zenith of the protest, on January 18, more than 15,000 websites blacked out part or all of their webpages to protest the bills, including web giants Google, Wikipedia and Reddit (Sell 2013). On that day, over four million people signed Google's online petition against the bills (Netburn 2012). In fact, so many people attempted to contact their elected representatives that the surge in traffic temporarily took down some webpages of members of the U.S. Senate (McCullagh 2012). It was the largest Internet protest in history, described by U.S. Representative Darrell Issa, a Republican from California and a staunch opponent of the bills, as an "Internet mutiny" (Franzen 2012).

Two days after the Internet Blackout, politicians sponsoring the bills in the U.S. House of Representatives and Senate withdrew them, effectively killing the legislation. Activists protested against SOPA and PIPA so vehemently because the bills aimed to change fundamentally online enforcement efforts against copyright and trademark infringement. The protest was the first major political defeat for U.S. intellectual property proponents in over thirty years, a monumental achievement of Internet activism (Sell 2013).

i) *From Failed Legislation to Backroom Deals*

Once the U.S. Congress withdrew the bills, many opponents assumed the bills were dead, at least until the next attempt at legislation. Protestors were unaware that proponents of SOPA had successfully transformed the reviled bills, which were soundly defeated by a groundswell of public opposition, into a series of secret, handshake agreements among powerful corporations. While protestors were campaigning against these bills, U.S. policymakers and rights holders supportive of SOPA and PIPA were active behind the scenes. They quietly negotiated agreements with firms providing essential Internet services, including Google, PayPal, Visa, and Microsoft. These agreements were not based on legislation but rather on what U.S. policymakers described as "voluntary, industry-led initiatives" (Espinell 2013). These initiatives were voluntary in the sense that they were non-legislative, non-legally binding general principles or "best practices" that would guide the firms' enforcement

efforts against infringing sites.⁷ Through these non-binding (i.e., informal) agreements, proponents of SOPA bypassed public opposition to the bill and incorporated into the agreements many of SOPA's toughest provisions (see Table 1.1). The negotiation over and creation of these agreements took place outside democratic, legislative processes.

The same firms targeted by SOPA and PIPA, some of whom opposed the proposed legislation, adopted the agreements. Signatories include large, well-known firms, from Google, Yahoo and PayPal to Visa, MasterCard and Microsoft (and its search engine Bing). SOPA's shift from an unpopular bill into a series of informal industry agreements was dramatic, and reached beyond the United States. Between 2010 and 2013 rights holders, backed by government support, negotiated multiple similar agreements in the European Union, particularly the United Kingdom, and Canada. These agreements comprise a little-known private regulatory effort undertaken by prominent U.S. and European rights holders and their trade associations to crack down on the online distribution of counterfeit goods.

Table 1.1: Internet Intermediaries

Intermediary type	Example	In SOPA	In private agreements
Payment	PayPal, Visa, MasterCard	Yes	Yes
Advertising	Google, Yahoo, Bing	Yes	Yes
Search	Google, Yahoo, Bing	Yes	Yes
Domain	GoDaddy	Yes	Yes
E-commerce	eBay	No	Yes

Examining these agreements and the circumstances in which they emerged provides a valuable opportunity to study how corporate actors set and enforce rules globally in the online environment. More broadly, these agreements also offer an opportunity to trace interactions and inter-dependencies between corporate actors and the state in the construction of these agreements and explore the extent to which non-state (in this case, corporate) regulation relies upon the state. This dissertation explores this kind of corporate online regulation

⁷ These "best practices" are identified and determined by industry and therefore do not represent objectively evaluated measures.

through an empirically grounded analysis of eight private enforcement agreements covering five Internet service sectors: advertising, domain name, marketplace, payment and search.⁸

There are strong commonalities among these eight agreements. They are the product of closed-door meetings among small groups of industry stakeholders and government officials without participation from consumer or civil-society groups. They contain non-legally binding measures agreed to by industry stakeholders that establish minimum standards or general principles to guide intermediaries' enforcement efforts. There are common enforcement strategies: the removal of content that infringes intellectual property rights (hereafter "infringing content") and the withdrawal of services from infringing sites. In terms of the removal of infringing content, eBay, for example, removes sales listings from its marketplace that advertise counterfeit goods (termed "infringing listings"). Search engines like Google remove search results that are hyperlinks to infringing webpages (termed "infringing search results"). Other service providers agree to withdraw their services from infringing sites. Payment providers like Visa or PayPal, for example, withdraw their payment services from targeted sites, which leaves sites unable to process payments.

The Internet intermediaries involved in these agreements are not typical Internet firms. Given their vast platforms and tremendous surveillance and enforcement capacities, these firms should be understood as "macro-intermediaries."⁹ This dissertation focuses on the following macro-intermediaries: Google, Yahoo, Bing (Microsoft's search engine), PayPal, Visa, MasterCard, American Express, eBay and GoDaddy. These firms have a significant regulatory capacity as they can reach globally and strip websites' payment processing abilities, deprive them of advertising revenue and withdraw their domain name services (see Table 1.2). By withdrawing services from targeted sites, macro-intermediaries can render sites commercially non-viable. This enforcement strategy is intended to enact regulatory "chokepoints" to impede the functioning of infringing sites by throttling their access to essential services like the provision of payment

⁸ There is some overlap amongst these categories as search engines, like Google, also operate digital advertising services.

⁹ This term is drawn from ideas of "macro-gatekeepers" used to describe companies that facilitate the flow of information on the Internet (see Barzilai-Nahon 2008; Laidlaw 2010).

processing. As the agreements are non-binding and struck between private actors, there is no judicial or state oversight of the regulatory activities. Enforcement can therefore be rapid, global, and largely secret.

Table 1.2: Internet Macro-intermediaries' Enforcement Capabilities

Macro-intermediary	Enforcement action
PayPal, Visa, MasterCard, American Express	Withdraw payment processing
Google, Yahoo, Bing	Withdraw advertising services
Google, Yahoo, Bing	Remove search results
GoDaddy	Withdraw domain name services
eBay	Remove sales listings

At first glance, macro-intermediaries' adoption of these private agreements appears to be contrary to their interests as the agreements increase their regulatory responsibilities to police their platforms for third-party wrongdoing on behalf of rights holders. This is because the term "voluntary initiatives" is a misnomer: the agreements are the product of coercive state activity. The state is central to the agreements. Government agencies in the United States and United Kingdom, and the European Commission employed varying degrees of coercion to compel the Internet firms to adopt these informal enforcement agreements. In addition to furthering the protection of intellectual property, there are other strategic interests at play in these agreements. For the U.S. government, the principal architect of agreements, the regulation of online infringement is inextricably linked with its interests in shaping broader regulatory and standard-setting efforts on the Internet as a whole.

In the United States, policymakers' circumvention of legislative processes is particularly provocative as it came in the wake of SOPA's resounding defeat. Similar evasive manoeuvres around public interest are also evident in state-facilitated enforcement agreements created in the United Kingdom and in the European Union by the European Commission. These agreements are backroom deals drafted among small groups of powerful, U.S.-based Internet firms and payment providers in concert with large, multinational rights holders from the United States and Europe. Consumer organisations are entirely absent from the process, as is any representation of the public's interests in relation to

the use and regulation of Internet services. The secretive way in which industry and government actors created these agreements is antithetical to legislative and democratic processes. It also violates broadly accepted principles of Internet policymaking that emphasise multi-stakeholder dialogue, such as those adopted in 2011 by the Organisation for Economic Development and Cooperation (OECD 2011).

The private informal agreements among rights holders, macro-intermediaries and key governmental bodies also speak to broader issues of regulation on the Internet. This industry-state anti-counterfeiting coalition raises critical questions about the nature of ostensibly non-state regulation and the degree to which private actors involved in this type of regulation rely upon the state. It also elicits questions about the conditions under which the state prefers private regulation, its interests in facilitating this particular regulatory arrangement, and the interplay between corporate and state online surveillance practices.

The rest of this chapter is organised into seven parts. The first part lays out the research problems and questions while the next part defines key terms and explains why the research focuses on the private online regulation of trademark infringement. The third part gives a brief overview of the context of corporate anti-counterfeiting efforts. Next, the chapter situates the research in the relevant literatures while the fifth sets out the dissertation's methodology and theoretic framework. The sixth part sets out the dissertation's argument and the final part outlines the chapters to follow.

I) Research Problem and Questions

Nation-states (hereafter "states") and, increasingly, private actors have recognised Internet firms' regulatory potential and the advantages of intermediary-facilitated enforcement, such as the mass surveillance and policing of hundreds of millions of transactions and users. Through a focus on regulatory efforts against sites selling counterfeit goods, this dissertation investigates the creation and operation of a private regulatory regime through an examination of eight informal enforcement agreements (see Table 1.3). The dissertation's main research questions are:

1. How do macro-intermediaries regulate sites selling counterfeit goods using informal enforcement agreements on behalf of rights holders?
2. Why did these macro-intermediaries adopt informal agreements that increased their regulatory responsibilities for third-party infringement on their platforms?
3. What explains government intervention among private parties to compel Internet firms and payment providers to adopt informal agreements that primarily benefit rights holders?

Table: 1.3: Key Private Enforcement Agreements

Participants	Site / Initiative
American Express, Visa, MasterCard, PayPal, Google, GoDaddy, Yahoo, Bing	U.S. – Centre for Safe Internet Pharmacies to address illegal online pharmacies
MasterCard, Visa, PayPal, American Express,	U.S. – International Anti-Counterfeiting Coalition (payment-account termination program)
Visa	Canada – Canadian Anti-Fraud Centre (payment-account termination program)
eBay	E.U. – Memorandum of Understanding for the sale of Counterfeit Goods via the Internet (marketplaces)
Taobao	U.S./China – Memorandum of Understanding (marketplace)
Google, Yahoo U.K., Bing	U.K. – Digital Standards Trading Group (advertising)
Google, Yahoo, AOL, Bing	U.S. – Ad Networks' Statement of Best Practices
Google, Yahoo, Bing	U.K. – Search Engine Code of Conduct

To answer these questions, this dissertation examines the eight private agreements listed in Table 1.3. Analysis focuses on these agreements because they comprise states at the forefront of informal regulatory efforts to protect intellectual property (the United Kingdom, the United States, as well as the European Commission, which is the executive arm of the European Union). I include the Canadian agreement to examine variances in the degree of state coercion in the creation of non-binding enforcement agreements. In addition,

the dissertation examines the agreement with the China-based Taobao marketplace because China is the primary target of rights holders' enforcement efforts. China is both a major manufacturer of counterfeit goods and a country with a rapidly growing e-commerce sector in which U.S. and European rights holders want to expand their market share. By examining eight agreements that cover a range of Internet services, this dissertation can analyse how state and corporate actors created and operate a global private regulatory regime.

The macro-intermediaries examined in this project have considerable regulatory capacity given the global scale of their platforms and the technological sophistication of their surveillance and enforcement programs. Moreover, they have significant latitude to make and enforce rules governing the use of their platforms and services by Internet users, as well as to issue sanctions to those who violate their rules. These macro-intermediaries, by virtue of their provision of essential Internet amenities, like search and payment services, have the capacity to shape how individuals access and use certain Internet services and technologies. As a result, states or corporate actors can exert control over considerable portions of the Internet by controlling Internet macro-intermediaries. State influence over macro-intermediaries, particularly by authoritarian governments, raises concerns of censorship and repression of human rights (see Deibert et al. 2011). Corporate actors, working through macro-intermediaries, can also wield tremendous control over the types of content Internet users can access and the services they can use, without any sort of judicial or democratic oversight. Corporate regulatory efforts, like that of authoritarian regimes, can be largely invisible to many Internet users who may not realise how intermediaries have changed their rules until they are unable to access certain information or use a particular service. This amounts to state-sanctioned control by (largely) U.S. rights holders over the Internet.

Despite the growing prominence of corporate regulatory efforts of the Internet, particularly in terms of intellectual property, this type of private regulation is critically under-studied. This dissertation endeavours to remedy that gap in its contribution to the scholarly understanding of online private regulation, particularly by and via macro-intermediaries. It also contributes to our understanding of corporate actors' regulatory capacity and limitations, as well

as how and under what conditions their efforts rely upon the state. Before it describes how macro-intermediaries operate and outlines their evolution as regulators on behalf of rights holders, this chapter first explains the choice of intellectual property as a way to explore non-state regulation and then defines trademarks and counterfeit goods.

II) Why Trademark Infringement?

i) *Importance of Intellectual Property*

Intellectual property is a valuable and, I argue, intriguing lens through which to examine non-state regulation on the Internet. Intellectual property is an issue of significant economic and political importance to the United States, the foremost global proponent of stronger protection for intellectual property rights (Drahos and Braithwaite 2002). Individuals and corporations in industrialised countries, particularly the United States but also countries in Europe, own the greatest proportion of intellectual property rights.¹⁰ Economic benefits from intellectual property primarily flow to those who own the rights. In the case of trademarks, this means that rights holders in the United States and Europe receive considerable revenue from the manufacture of products, even though the production of those goods increasingly takes place in lower-cost countries, particularly China (Dedrick, Kraemer, and Linden 2009).

In the modern, globalised economy, ownership of intellectual property rights is central to economic dominance. This is why the United States, on behalf of its industries, continues to pursue ever-stronger intellectual property rights protection. The United States uses bilateral and multi-lateral trade agreements to export its preferred policies on intellectual property globally (Drahos and Braithwaite 2002). Historically, U.S.-based rights holders and their trade associations have exerted considerable influence over public policymaking (Braithwaite and Drahos 2000; Drahos and Braithwaite 2002; Sell 2003). U.S. intellectual property actors (rights holders and trade associations) successfully created a narrative in the late 1970s that linked the protection of intellectual

¹⁰ This is demonstrated in recent studies that examine the concentration of ownership of these rights (see U.S. Commerce 2012; OHIM 2012).

property to continued U.S. economic dominance (Drahos and Braithwaite 2002). As chapter 3 will discuss, at that time, U.S. industry faced rising competition from emerging economies in Asia, and foreign debt and trade deficits (Halbert 1997). The protection of U.S. intellectual property offered a nationalistic and protectionist solution to U.S. economic problems and, importantly for this dissertation, conceptually linked intellectual property with trade (Drahos and Braithwaite 2002; Sell 2003). This socially constructed idea of intellectual property explains the importance that the United States, as well as the European Union, accord to the protection of intellectual property (Drahos and Braithwaite 2002).

Since the 1970s, U.S. rights holders and their trade associations have been central to the U.S. government's campaign to push for new international rules and standards that would establish a global baseline for the protection of intellectual property rights. These corporate actors played important roles in persuading and pressuring foreign governments and corporations to adopt rules that would disproportionately favour U.S. industries, as well as those in a handful of other industrialised countries (Drahos and Braithwaite 2002; Sell 2003). During this period, the U.S. government formalised a role for these industry actors as trade advisors to the government and, in doing so, entrenched the inter-dependent relationship between the U.S. government and its intellectual property actors.¹¹

The influence of U.S.-based rights holders and their trade associations continues today. They lobby states worldwide to toughen laws protecting intellectual property and increase enforcement against the infringement of intellectual property rights. They also pressure companies that they contend are involved in or facilitate infringement to adopt suitably tough (i.e., U.S.-style) enforcement policies and processes. This process is never complete as rights holders pursue ever-increasing standards of protection. Each successful effort that 'ratchets up' rules and standards results in an ever-rising 'floor' that becomes the new baseline for subsequent efforts (Sell 2010).

¹¹ In 1981, the United States created the Advisory Committee for Trade Negotiations (ACTN) to advise the U.S. government on trade policy. This committee, which is discussed in greater detail in chapter 3, is run by the Office of the United States Trade Representative (USTR) (Drahos and Braithwaite 2002; Sell 2003).

The private regulation of trademark infringement on the Internet is a compelling issue to study because rights holders and their trade associations consider the online distribution of counterfeit goods to be a growing and serious problem. As a result, rights holders are innovative, aggressive and highly motivated in their efforts to protect their rights. The online environment presents particular enforcement challenges, from difficulties in locating and identifying offenders to problems with uncooperative foreign jurisdictions, as will be explored in chapter 3. However, it also offers certain advantages. Macro-intermediaries, like Google and Visa, possess a considerable regulatory capacity by virtue of their dominant market share, vast networks and sophisticated surveillance and enforcement apparatuses. By persuading and coercing macro-intermediaries to work with them to address infringement, rights holders can dramatically expand their capacity to regulate infringing sites. Regulatory efforts on this scale are new as they previously would have been prohibitively expensive or technologically unfeasible. Before exploring how macro-intermediaries became private enforcers for rights holders, the chapter first explains how trademarks function and their vital importance as revenue generators for rights holders.

ii) ***Trademarks and Counterfeiting***

As consumers, we see and likely recognise hundreds of trademarks daily in locales as diverse as media to the grocery store and even our workplaces. A trademark is a type of intellectual property that is classified as industrial property along with patents, industrial designs and trade secrets.¹² Like all forms of intellectual property, trademark law is a complex and fast-evolving field but it is important to highlight a few basic points about trademarks. Trademarks can consist of words, letters, numerals, drawings, symbols, colours, audible sounds, fragrances, three-dimensional shapes, logos, pictures, or a combination of these or other characteristics (Ricketson 1994). Well-known trademarks are McDonald's "golden arches," Nike's "swoosh" and Toblerone's distinctive triangle-shaped chocolate bars. Originally, trademarks were intended to indicate a product's origin, such as from a particular guild or artisan

¹² The other category of intellectual property refers to copyright and related rights granted to the authors of literary and artistic works, and the rights of performers, producers of phonograms and broadcasting organizations.

(Ricketson 1994). However, as systems of production and distribution became more complex and globalised, contemporary trademarks identify the ‘proprietor’ of the trademark (e.g., Apple) rather than its place of manufacture (Ricketson 1994).

Trademarks are distinctive signs intended to enable consumers to identify the commercial origin of goods (e.g., Nike) and to distinguish specific goods from other similar offerings in the marketplace (Ricketson 1994). They enable consumers, for example, to distinguish Apple’s iPhones from Samsung’s Galaxy phones. Trademarks convey information to consumers about the character, quality and reputation of a particular good (Ricketson 1994). They promise but do not legally guarantee reliability or the maintenance of certain standards, which is the function of certification marks (Ricketson 1994). Laws require certification stickers from the Underwriters’ Laboratories, for example, on certain products, such as electrical goods. Trademarks need not be registered. Parties can acquire rights in relation to trademarks merely by using them, though registering trademarks offers protection (Ricketson 1994). Trademarks are registered in a process that verifies that no other individuals or companies have registered the same sign in the same industry sector (Ricketson 1994). Once registered in one country, the trademark can be registered internationally in all countries that are signatories to the 1891 *Madrid Agreement*.¹³

The owner of a registered trademark has the exclusive right to use that mark and prevent all others from using “identical or similar signs for goods or services which are identical or similar to those in respect of which the trademark is registered where such use would result in a likelihood of confusion.”¹⁴ There are limited exceptions, such as the use of a competitor’s trademark for comparison in advertising. Counterfeit goods, meanwhile, are unauthorised reproductions of products or packaging that infringe a rights holder’s registered trademark. Specifically, they are defined as

¹³ This refers to the 1891 Madrid Agreement Concerning the International Registration of Marks and the Protocol Relating to the Madrid Agreement, which was adopted in 1989 and came into operation on 1 April 1996. The International Bureau of the World Intellectual Property Organisation administers the system.

¹⁴ 1994 *Agreement on Trade-Related Aspects of Intellectual Property* (TRIPS), Art 16.1. This multilateral agreement, which established standards internationally for the protection of intellectual property rights is discussed in chapter 3.

any goods, including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such goods, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the owner of the trademark in question under the law of the country of importation.¹⁵

Many people have likely encountered or even purchased counterfeit goods at some point in their lives, perhaps at local flea markets or along Canal Street in New York City. Counterfeiting affects a broad range of goods from luxury clothing and accessories, cosmetics and perfume, and food and alcohol to personal care items like toothpaste and condoms. Industrial products, such as commercial circuit-breaks, vehicle brake pads and pumps for mining operations may also be counterfeited.¹⁶

A counterfeit product may have value or utility apart from its identical resemblance to a legitimately trademarked version of the same good. For example, an individual could wear counterfeit apparel and not recognise or care about the goods' unauthorised trademark. However, for those who produce and sell counterfeit goods, their value is the trademark. Individuals desire products with certain trademarks because of what that mark represents (Gentry 2001). Someone who desires a Gucci purse may knowingly purchase a counterfeit version and find satisfaction with it because of the qualities they associate with the Gucci brand. Consumers desire counterfeit goods because they are "counterfeits of some brand" (Gentry 2001:264).

iii) ***Trademarks are Forever***

Trademarks are often considered synonymous with "brands." A brand can be understood as "the soul of a product" (Rothacher 2004:2). It can represent reliable qualities and consistent pricing and even evoke emotional attachment in consumers (Rothacher 2004:2). Marketers strategically shape brands to have

¹⁵ TRIPS Art. 51(a).

¹⁶ This is according to interviews conducted for this research as well as reports published by bodies like the Office of the U.S. Trade Representative, see <http://www.ustr.gov/about-us/press-office/reports-and-publications>.

certain attributes and consumers may imbue those brands with certain personality characteristics, whether real or perceived (de Chernatony, MacDonald, and Wallace 2011). These characteristics can extend beyond the functional qualities of the product (de Chernatony and Riley 1998). For example, consumers may identify one model of vehicle with rugged independence in the backcountry, while another, similar model evokes ideas of downtown, urbane elegance. Brands can also be understood as symbolic devices or signifiers that consumers use to act “as an informational cue, personal identity signal or cultural symbol” (Schmitt 2012:12). Consumers use brands to convey aspects of their personal identities to others, such as creativity, refinement, independence or rebellion. They may signal their status through, for example, the consumption of luxury goods (de Chernatony, MacDonald, and Wallace 2011; Schmitt 2012) or the selection of locally sourced goods over imported ones.

Developing and protecting brands is a serious, multi-billion-dollar business because trademarks can last forever. Trademarks have no expiry date and can be renewed indefinitely, as long as they are in use. This means that unlike copyrights and patents, which have expiry dates, trademarks can provide a potentially unending source of revenue. Successful brands are valuable because they “guarantee future income streams” (de Chernatony, MacDonald, and Wallace 2011:29). Rights holders want to attract and maintain lifelong customers. Much of the massive marketing literature on brands is in areas devoted to studying how consumers perceive brands, which brands they identify with and how they form associations with brands (Schmitt 2012). Brand perception and attachment are intensely subjective processes. Consumers can develop strong preferences for one brand over another, even when there are few differences between the products. As brands can be made or broken on consumer loyalty, which can be intensely fickle, there are enormous amounts of money at stake in the construction and marketing of brands to consumers that will inspire and maintain loyalty.

iv) ***Protecting Multi-Billion-Dollar Brands***

Multinational rights holders with well-known brands are thus aggressive in their efforts to protect their products from trademark infringement because billions of dollars are at stake. Companies that are most publicly prominent in their anti-counterfeiting efforts are typically those with sought-after brands in the apparel and accessories sector. These firms include Louis Vuitton, Chanel, Gucci, Coach, the Gap, Nike, and Adidas. Many multinational rights holders in other industry sectors, such as pharmaceuticals or industrial goods, also have anti-counterfeiting programs but these are often conducted within the company or quietly undertaken by a trade association.¹⁷ Further, in contrast with some apparel firms, companies with a problem with counterfeit pharmaceuticals or circuit breakers may be reluctant to publicise their anti-counterfeiting efforts because of concerns of driving away customers. Apparel and accessory firms are particularly energetic in their enforcement efforts because surveys indicate that individuals who knowingly purchase counterfeit goods choose to purchase counterfeit apparel and accessories because they do not perceive these products as potentially harmful.¹⁸ They may purchase some counterfeit goods as trial versions or substitutes for genuine branded goods (Bryce, Horton, and Limmer 2010; Penz and Stöttinger 2008; Rutter and Bryce 2008). These surveys also find that some consumers also conceptually separate the brand from the product, which means they choose to consume a brand (counterfeit Gucci purse) but not a specific product (Gucci purse) (Gentry 2001:264).¹⁹ This de-coupling of brands from products is particularly worrying for producers of luxury goods where the brand is the product.

Rights holders involved in the private enforcement agreements examined in this dissertation typically operate through their trade associations. This makes it difficult at times to determine which rights holders are participating in these

¹⁷ For example, the U.K.-based British Electrical and Allied Manufacturers' Association regularly conducts enforcement operations in China and the Middle East against factories manufacturing counterfeit goods on behalf of its members.

¹⁸ For example, a consumer survey of counterfeit purchase habits by the Business Action to Stop Counterfeiting and Piracy (BASCAP) found that consumers believe counterfeit apparel to be less harmful than pharmaceuticals (BASCAP 2009).

¹⁹ This research demonstrates that in contrast to rights holders' claims of damage to their brands because of counterfeit goods, some consumers purchase counterfeit goods while ascribing value to the brand (Gentry 2001).

agreements, as these agreements are negotiated in closed-door meetings and not widely publicised. Despite these challenges, I identified parties involved in these programs through interviews with rights holders and their trade associations, particularly the influential Washington, D.C.-based International Anti-Counterfeiting Coalition (IACC). The IACC, which has decades of experience lobbying for increased protection for intellectual property rights, counts some of the largest global brands among its membership.²⁰ The IACC's members include Louis Vuitton, Nike, Calvin Klein, Chanel and Apple, as well as the pharmaceutical companies Pfizer and Merck. The agreement negotiated by the European Commission in relation to counterfeit goods in online marketplaces publicly lists its participants (European Commission 2013). Participants include Adidas, Burberry, Louis Vuitton, Nike, and Proctor & Gamble.

These brands generate massive revenue. *Forbes'* annual Fortune 500 list²¹ calculates, for example, that Apple generated \$156.5 billion in revenue in 2013, while Proctor & Gamble generated \$85.1 billion and Nike \$24 billion (*Forbes* 2013). These companies all have highly valuable brands (see Table 1.4). For U.S.-based apparel companies, the brand-valuation firm Interbrand estimates Nike's brand at \$17 billion, whereas it values the brands Ralph Lauren and the Gap at \$4.5 billion and \$3.9 billion respectively (Interbrand 2013). Non-U.S. brands involved in anti-counterfeiting efforts also command considerable value. The France-based Louis Vuitton's brand, for example, is valued at \$24.8 billion, according to Interbrand, while the Germany-based Adidas' brand is estimated to be worth \$7.5 billion.

As brands are intangible assets, these figures are only estimates and there are variances among brand-valuation companies in the values they place on brands. The value of brands shifts over the years and also rises and falls with firms' fortunes and scandals. Nonetheless, these staggeringly large figures offer an idea of the importance of corporate brands and the considerable economic interests that firms have in protecting their trademarks. Further, they show that

²⁰ The IACC's membership also includes prominent copyright owners, including The Walt Disney Company, Sony Music Entertainment and Warner Brothers Entertainment. For a full list of the IACC membership, see: <http://www.iacc.org/member-companies.html>.

²¹ Throughout the dissertation, all figures are in U.S. dollars unless otherwise noted.

these rights holders are wealthy corporate actors that can persuasively lobby governments to protect their intellectual property rights.

Table 1.4: Billion-Dollar Brands²²

Macro-Intermediaries	Estimated Revenue 2013	Brand Valuation 2013
Google	\$52.2 billion	\$93.2 billion
Yahoo	\$5 billion	\$5.2 billion
Microsoft	\$73.7 billion	\$59.4 billion
PayPal	\$6.6 billion	\$7.1 billion
Visa	\$10.4 billion	\$5.4 billion
MasterCard	\$7.4 billion	\$4.2 billion
American Express	\$33 billion	\$17.6 billion
GoDaddy	\$1.43 billion	Unavailable (privately held)
eBay	\$14.1 billion	\$13.1 billion
Prominent Rights Holders	Estimated Revenue 2013	Brand Valuation 2013
Apple	\$156.5 billion	\$98.3 billion
Proctor & Gamble	\$85.1 billion	\$3.1 billion
Louis Vuitton	\$9.4 billion	\$24.8 billion
Nike	\$24 billion	\$17 billion
Adidas	\$14.5 billion	\$7.5 billion

The largest Internet firms and payment providers similarly command multi-billion-dollar revenues and brand valuations. As discussed earlier in this chapter, these firms are macro-intermediaries because of their global operations and significant market share in the provision of key Internet services. This dissertation focuses on Google, Yahoo, Microsoft, PayPal, Visa, MasterCard, American Express, GoDaddy and eBay. Some of these firms provide services across multiple sectors. Google, Yahoo and Microsoft, for example, all operate search engines and digital advertising platforms that generate, in the case of Google, most of its revenue. GoDaddy is the world's largest domain name registrar, which means it provides and registers domain

²² Figures for estimated revenue are drawn from the *Forbes* 500 listing (*Forbes* 2013a) and figures for the brand estimates are from Interbrand (Interbrand 2013). The exception is GoDaddy, which is from (Kharif 2013) as the company is privately held. Bloomberg estimated in July 2013 that GoDaddy was on track for an annual corporate revenue of \$1.43 billion and could be worth \$6 billion at an initial public offering that is forecast for 2014 (Kharif 2013)

names.²³ It also provides web-hosting services that enable sites to be accessible via the World Wide Web. eBay, which is one of the top global marketplaces, owns and operates PayPal, one of the top online payment services.

These companies are all headquartered in the United States, suggesting the considerable commercial influence of U.S. companies on the Internet. Although these companies operate globally, they do not dominate markets equally in all jurisdictions. For example, Google is the world's largest search engine but in China nearly 80% of the market belongs to the China-based Baidu search engine (Su 2014). Similarly, eBay is eclipsed in China by the China-based Taobao marketplace, which is operated by the massive Alibaba Group that provides a range of e-commerce services. Chapter 6 examines the Alibaba Group's Taobao marketplace because U.S. and European rights holders complain that it facilitates the trade in counterfeit versions of their products.

As these companies are some of the largest Internet firms globally, it is unsurprising that they generate billions in revenue (see Table 1.4). *Forbes'* Fortune 500 list calculated that Google generated \$52.2 billion in revenue in 2013, eBay \$14.1 billion and Yahoo \$5 billion (*Forbes* 2013a). For payment providers, Visa and MasterCard generated \$10.4 and \$7.4 billion respectively (*Forbes* 2013a). These firms also have extremely valuable brands. According to Interbrand, Google's brand, for example, is valued at \$98.2 billion, which is in second place on the list of top one hundred brands just behind Apple, and eBay's is worth an estimated \$13.1 billion (Interbrand 2013).

Colloquially, these macro-intermediaries can be thought of as part of "Big Tech" alongside the more traditional corporate powerhouses of Big Banking, Big Oil, Big Pharma, and Big Tobacco. This term reflects the massive revenue generated by and the global operations of these companies. Given the tremendous wealth and growing corporate influence of these macro-intermediaries, how were they persuaded to act as enforcers for rights holders? Why would they agree voluntarily to increase their regulatory responsibilities to police third-party infringement on their platforms and networks? The primary

²³ Domain names are the easy-to-remember names for websites, e.g., nytimes.com.

reason is that each of the states involved in these agreements (the United States, United Kingdom and European Union) used coercion to threaten macro-intermediaries to adopt the private enforcement agreements. In addition to state coercion, rights holders' also pressured the macro-intermediaries with threats of legal action. As well, macro-intermediaries have some common financial interests with rights holders, and, more broadly, with the United States and European Union, in the protection of intellectual property.

To explore these common interests, the chapter now examines the massive revenue generated for certain multinational rights holders through their ownership of valuable intellectual property.

v) *Rights Holders Controlling Value Chains*

Value-chain analysis allows researchers to track how rights holders generate revenue through their control of intellectual property rights. The term "value chain" refers to all the activities in delivering a product to market, from design and manufacture to distribution and marketing (Dedrick, Kraemer, and Linden 2009). Multiple companies in different countries may perform separate functions in this chain. The globalization of manufacturing and distribution processes means that corporations may find it economically advantageous to outsource some or all of their production activities to lower-cost countries, particularly China. Apple, for example, outsources more than 90% of its manufacturing functions to the Taiwanese-owned company Foxconn in China (Guglielmo 2014). Analysis of value chains can determine the relative proportion of value that is captured at different stages of the process and by different companies.

Multinational firms that own valuable trademarks, like Apple and Nike, tend to receive the largest share of value in the production of their products (Dedrick, Kraemer, and Linden 2009; Gereffi and Memedovic 2003; Kraemer, Linden, and Dedrick 2011). These corporations keep within their internal operations the most profitable activities, which are typically the design, branding, and marketing of products, not their manufacture (Gereffi and Frederick 2010:12). Thus, control over the intangible aspects of production, such as design and marketing of trademarks, is more important to corporations' power and

profitability than tangible aspects like manufacturing (Gereffi and Frederick 2010:12). Corporations that own valuable intellectual property can locate their manufacturing and distribution facilities in lower-cost countries and shift their activities according to changing conditions in cost, supply or demand.

Analyses of Apple's value chains demonstrate that the company captures the greatest share of value from its products. A study in 2011 of Apple's production of iPads and iPhones reveals that manufacturers in China receive approximately \$10 per iPad or \$8 per iPhone in direct labour wages (Kraemer, Linden and Dedrick 2011:4).²⁴ This amounts to 1.8% and 1.6% of the value of the iPhone and iPad respectively, which is in stark contrast to the 58% and 30% of the value that Apple captures from the same products (Kraemer, Linden, and Dedrick 2011:11).²⁵ Apple captures the greatest proportion of value because it owns the trademarks and patents involved in the manufacture and keeps product design, software development, and product management in the United States (Kraemer, Linden, and Dedrick 2011:2). Apparel manufacturing is similarly structured, with multinational apparel corporations like Nike capturing the greatest amount in the value chain (Gereffi and Frederick 2010). Companies that control the intellectual property can exert considerable power over their manufacturers in highly competitive environments. Apple, for example, shifts among multiple manufacturers and is willing "to switch key suppliers from one model to the next" (Dedrick, Kraemer, and Linden 2010:102).

These value-chain analyses show that not only does revenue disproportionately flow to the rights holders, but it also, by extension, flows to the rights holders' home country. As the research on Apple's value chain aptly reveals, the United States benefits from tax revenue and through Apple's retention of its high-value services in the United States.²⁶ China, in contrast, receives only a sliver of the value for the role of its citizens in manufacturing. The value captured by

²⁴ This study focuses 2010 figures associated with manufacturing the \$549 iPhone 4 and the \$499 16GB iPad. Researchers calculated the value added breakdown for the wholesale price in two components: 1) gross profits earned by companies, which they describe as value capture and 2) the cost of direct labour (Kraemer, Linden, and Dedrick 2011:10).

²⁵ Researchers examining value-chain analysis of technology firms acknowledge that product-level costs are difficult to obtain, as these firms "often require the silence of their suppliers and contractors through non-disclosure agreements" (Dedrick, Kraemer, and Linden 2009:87).

²⁶ The amounts of tax revenue a country does and should receive from multinational firms are always difficult and sometimes controversial issues.

industrialised countries, particularly the United States, shows, in part, why the United States pursues ever-increasing protections for intellectual property.

vi) *Reaping Rewards from Intellectual Property*

The “entire U.S. economy relies on some form of intellectual property,” remarks Victoria Espinel, head of the Office of the Intellectual Property Enforcement Coordinator (IPEC), “because virtually every industry either produces intellectual property or uses it” (Espinel 2012b). While advocates of intellectual property regularly make claims like this, it was not until 2012 that the U.S. government first attempted to quantify the number of U.S. jobs reliant upon intellectual property.²⁷ In March 2012, the U.S. Department of Commerce published a report that measured and ranked the country’s most intellectual property-intensive industries. Over a year later and based on the U.S. report, a similar report was published in the European Union by the Office of Harmonisation for the Internal Market (OHIM), the agency responsible for promoting and managing intellectual property.

The studies measure the contributions of intellectual property to their respective economies as the number of registered trademarks, patents or copyrights owned by a company per 1,000 employees (OHIM 2013:68). The reports find that the U.S. and E.U. economies are heavily reliant upon intellectual property-intensive industries (see Table 1.5). The U.S. report calculates that these industries directly contributed 27.1 million jobs in the U.S. economy in 2010 (U.S. Commerce 2012:vi). Indirect activities provided an additional 12.9 million jobs in the same year, for a total of 40 million jobs or 27.7% of all jobs in the economy (U.S. Commerce 2012:vi). These industries accounted for \$5.06 trillion (or 34.8%) of value added to the U.S. gross domestic product in 2010 (U.S. Commerce 2012:vi). The European Union study concludes that intellectual property-intensive industries generated 56.5 million jobs directly with another 20 million indirect jobs for a total of 77 million jobs or 35.1% of all jobs (OHIM 2013:6). These industries account for almost 39% of total economic activity in the European Union, worth € 4.7 trillion (OHIM 2013:6).

²⁷ The impetus for the study of IP-intensive industries was a request from Victoria Espinel, U.S. Intellectual Property Enforcement Coordinator (U.S. Commerce 2012:iii).

Table 1.5: Findings From Intellectual Property Industry Studies²⁸

Findings	United States	European Union
Total related employment	40 million (27.7% all jobs)	77 million (35.1% all jobs)
Value to GDP	\$5.06 trillion (34.8%)	€ 4.7 trillion (39%)
Number of trademark-intensive industries	55 industries	277 industries
Examples of top trademark-intensive sectors	Pharmaceuticals, toiletry products, motion pictures	Pharmaceuticals, toiletry products, wine

The reports also rank trademark-intensive industries and identify the top-performing industry sectors. The U.S. report identifies 55 trademark-intensive industries and its top sectors include pharmaceuticals, toiletry products, motion pictures, and newspaper and book publishing (U.S. Commerce 2012:17). The E.U. identifies 277 intensive industries and its top sectors includes “leasing of intellectual property,” pharmaceuticals, wine, biotechnology, toiletries, and games and sporting goods (OHIM 2013:52).²⁹ Among the top-ranked trademark-intensive sectors are a few odd cases with no obvious direct connection to trademarks. The manufacture of wallpaper, for example, ranks fifteenth in the EU report while grocery stores rank eleventh in the U.S. report.

Both studies acknowledge significant methodological limitations. They admit that trademark usage is difficult and complex to measure in comparison with patent usage and as a field of study trademark measurement is critically under-developed (U.S. Commerce 2012). These findings, moreover, are not uncontroversial. Critics of ever-increasing protection of intellectual property rights argue that intellectual property amounts to rent-seeking that stifles innovation and the creation of future products, inventions and artistic works (see Mazzone 2011; Raustiala and Sprigman 2012). Despite this, these reports are useful because they indicate how important the U.S. government and

²⁸ Figures for the United States are from the 2012 study produced by the U.S. Department of Commerce (U.S. Commerce 2012) and those for the European Union are from the 2013 study by the Office for the Harmonization in the Internal Market (OHIM 2013).

²⁹ For the European Union, Germany ranks highest in terms of trademark-intensive industries, followed, respectively by the United Kingdom, Spain, Italy and France (OHIM 2012:85).

governments in the European Union perceive intellectual property to be to the integrity of their economies.

IV) From Flea Markets to eBay

The problem of counterfeit goods is, of course, not new. For centuries unscrupulous individuals fraudulently applied artisans' "marks" to products to misrepresent their origin or creator.³⁰ Contemporary anti-counterfeiting efforts began in the late 1970s. At that time, U.S.-based multinational corporations were growing concerned about a rise in counterfeit goods coming from expanding economies in Asia (Drahos and Braithwaite 2002; Halbert 1997). These companies, particularly those from the pharmaceutical, computer and entertainment industries, convinced the U.S. government that the protection of intellectual property was central to the health of the U.S. economy (Sell 2003).

i) *Evolution of Anti-Counterfeiting Efforts*

In the late 1970s, rights holders solidified their lobbying power by creating trade associations to focus on the protection on intellectual property. In 1979, they created the International Anti-Counterfeiting Coalition (IACC) to deal with what rights holders perceived was "a big counterfeiting problem on the horizon."³¹ Throughout the 1980s and early 1990s, the IACC was a key player in efforts by U.S. rights holders, trade associations and government officials to establish international rules and standards protecting intellectual property, as will be explored in chapter 3. Since that time, rights holders and their trade associations, like the IACC and the U.K.-based Alliance for Intellectual Property and the Anti-Counterfeiting Group, have developed a broad range of anti-counterfeiting policies and initiatives. Among other efforts, they provide training to law enforcement agencies, policy advice to governments, and coordinate

³⁰ The misrepresentation or imitation of marks was recognised as a crime as early as the thirteenth century (Paster 1969). However, it was not until the mid-nineteenth century that trademarks were recognised in legislation with provisions protecting against their unauthorised use.

³¹ Interview with Bob Barchiesi, President, International Anti-Counterfeiting Coalition, 24 April 2012, Washington.

enforcement strategies.³² In terms of enforcement, one of their top priorities is to assist their members to address the online distribution of counterfeit goods.

The evolution of e-commerce significantly changed the advertisement and distribution of counterfeit goods. Most people, for instance, have probably received spam perhaps announcing the sale of Viagra to treat erectile dysfunction. These drugs generally come from unlicensed and unlawfully operating online pharmacies that sell counterfeit or diverted medication (McCoy et al. 2012a).³³ Internet users have also likely encountered websites selling suspiciously cheap brand-name goods, like Coach purses or Acushnet golf clubs that are euphemistically described as “replicas.” Although e-commerce has made it easier for counterfeiters to advertise their wares and reach customers, counterfeit goods must still be physically manufactured and shipped from production sites to consumers. This is in contrast to copyright-infringing digital copies of the latest movies or albums that can be downloaded from sources like The Pirate Bay or IsoHunt. Thus, depending on the nature and degree of their problem with counterfeit products, rights holders may have both online enforcement strategies and initiatives directed toward targeting the physical manufacture, importation and distribution of counterfeit goods.

ii) ***Corporate Anti-Counterfeiting Efforts***

Rights holders employ various anti-counterfeiting measures depending upon the perceived importance of the problem and the resources they allocate to address it. I interviewed individuals involved in anti-counterfeiting enforcement activities across a range of industries, including pharmaceuticals, sporting goods, apparel, and consumer electronics. Corporate anti-counterfeiting efforts vary widely in their size, structure and manner of operation. One well-known, U.S.-based multinational firm that I spoke with operated what the firm called its “Global Brand Protection Units,” which had a staff of two individuals.³⁴ Other

³² The International Anti-Counterfeiting Coalition, for example, offers training for law enforcement agencies worldwide.

³³ In this case, diverted medication (also called parallel trade products) refers to legitimate products intended for legal sale in one geographical jurisdiction but diverted to another in violation of commercial licensing agreements.

³⁴ I spoke with these individuals during my attendance at the IACC Annual Conference in May 2012 in Washington, D.C. One of the individuals was in charge of anti-counterfeiting efforts in

companies operate large, sophisticated anti-counterfeiting programs with enforcement units in multiple geographic regions. Those involved in what is termed “brand-protection” efforts commonly work with in-house or external attorneys to undertake their enforcement activities.

Many rights holders also work with third-party firms that provide what the industry refers to as brand-protection services. Firms in this industry vary widely in terms of size, scope and the services offered. Some large, well-known multinational firms like Kroll and Pinkerton offer brand-protection services, along with other security-related functions, such as fraud investigations. Apart from these security giants, most other brand-protection firms are much smaller with a handful to a few dozen employees each.³⁵ They employ contractors when they need a specific skill, like surveillance or a foreign language, or an operative in another country.

The brand-protection industry, which is part of the private security industry, emerged in the 1980s with the outsourcing of manufacturing from industrialised countries to those in Asia, particularly China. According to industry insiders, the industry expanded rapidly with the growth of the Internet and rights holders’ fears of online infringement in the early 2000s. A particular area of growth is in online brand monitoring, in which firms police marketplaces or commercial sites believed to be selling counterfeit goods and send cease-and-desist notices or complaints for the removal of suspicious content. These firms are part of the “high policing” component of the private security industry that specialises in corporate security and investigative work (Brodeur 2007; Bowling and Sheptycki 2012; Sheptycki 2000).³⁶ Similar to other high policing actors, they operate globally on behalf of state or corporate clients and mostly serve clients from the global north (Bowling and Sheptycki 2012; O’Reilly 2011; Sheptycki 1997). This dissertation does not examine the brand-protection industry directly, as it focuses instead on macro-intermediaries’ enforcement efforts on behalf of rights

North and South America and the other was in charge of efforts in Europe, the Middle East and Asia.

³⁵ This brief portrait of the brand-protection industry was established through interviews with individuals working in the brand-protection industry in Australia, the United States and the United Kingdom.

³⁶ “Low policing,” in contrast, involves the protection of physical spaces, commonly airports, parking lots, malls or other high-traffic areas (Brodeur 2007; Sheptycki 2000).

holders. It is beyond the scope of this project to consider both the brand-protection industry and macro-intermediaries. However, I draw upon interviews with those in the brand-protection sector to explain online anti-counterfeiting strategies and examine the development of the private enforcement agreements.³⁷

Rights holders face particular challenges in undertaking anti-counterfeiting efforts in both the real world and online. Enforcement efforts aimed at physical locations, particularly manufacturing facilities, can be legally complex, time consuming, costly and challenging. Government and local officials can be unwilling or incapable of providing assistance.³⁸ Foreign production facilities, often based in China, can be difficult to locate and surprisingly resilient to raids. “There simply isn’t this western conception that there are factories churning out counterfeit goods day by day,” explained a Hong Kong-based lawyer in relation to China. Instead, there “are lots of small on-the-ground facilities.”³⁹ Those involved in the production and large-scale distribution can be difficult to locate and prosecute. “The Mr. Big, they’re never locked up in jail for IP violations,” says the Hong Kong-based lawyer.⁴⁰ In developing countries, the protection of foreign rights holders’ trademark rights is often not a priority for law enforcement agencies that understandably must focus on more serious offences like weapons trafficking. Even within industrialised countries anti-counterfeiting efforts can pose challenges. Enforcement efforts aimed at flea markets or discount outlets, for example, can be resource-intensive and ineffective as sellers shift locations or rapidly replenish their stocks if counterfeits are seized.

iii) *Infringing Sites and the Problem of “Whack a Mole”*

In the online environment, rights holders face some of those same challenges. It is relatively easy for those offering counterfeit goods to set up a website, name it something catchy like www.Nikeoutletsale.com, and spam advertisements to consumers. They may also open multiple seller accounts in online marketplaces

³⁷ The brand-protection industry, its history, evolution and roles, merits a dissertation in itself.

³⁸ In some areas corruption of local and state officials is a significant problem and counterfeiting may provide benefits to the local economy through employment (Mertha 2005).

³⁹ Interview with lawyer at Hong Kong law firm, 7 May 2012, Washington.

⁴⁰ Ibid.

like eBay or iOffer and sell their wares to unsuspecting customers or those looking for a good deal. Rights holders must monitor the sale of their products across multiple online marketplaces and try to identify and shut down sites selling counterfeits. For some popular brands, the scale of the problem is significant as there may be tens of thousands of sales listings for counterfeit goods on online marketplaces and hundreds of sites selling counterfeit products. Individuals operating these sites can be difficult to identify and tough to prosecute, particularly if they are based in jurisdictions that are unwilling or unable to cooperate.

The principal challenge, however, is the resilience of counterfeiters' operations to enforcement efforts. Rights holders may complain to the offending site's web host, which can terminate its service to the targeted site. However, the site owners can simply seek another web hosting company, payment provider, or domain name registrar. "The expression is whack a mole," explains Damian Croker, the head of BrandStrike, a brand-protection firm in the United Kingdom. "The fact is even after you get that site down it comes back up again."⁴¹ Those in the brand-protection community refer to sites selling counterfeit goods as "infringing sites" or, more colourfully, "rogue sites." There is no commonly accepted definition for infringing sites. It includes sites that sell counterfeit goods, as well as those that distribute copyright-infringing music, films, software or books, like the infamous site, The Pirate Bay.⁴² In its breadth, this term is similar to the one proposed by the *Stop Online Piracy Act* (SOPA).

SOPA defined "foreign infringing sites" as sites or a "portion thereof" that were directed toward and used by individuals in the United States in which the site operator "is committing or facilitating the commission of criminal violations," including trafficking in counterfeit goods or services.⁴³ SOPA's definition would have applied to sites selling counterfeit goods and those offering copyright-infringing content. The breadth of SOPA's definition alarmed critics who argued that a "portion thereof" could be interpreted to include sites that had only a small

⁴¹ Interview with Damian Croker, CEO, BrandStrike Limited, 25 September 2012, London.

⁴² The definition also incorporates sites that distribute circumvention devices, which are prohibited in many countries. These devices are software programs that enable users to 'break' the digital 'locks' set by copyright owners.

⁴³ SOPA Sec. 102.

problem with infringement. This could include a site that allegedly offered for sale one counterfeit good amongst all its other legitimate products. It could also include legitimate sites that had hyperlinks to sites that sell counterfeit or copyright-infringing goods.

Legal definitions proposed in legislation like the ill-fated SOPA are subject to judicial interpretation and scrutiny. This gives critics and defendants chances to raise objections. Legal rulings shape how definitions can be used and to what types of situations they apply. In contrast, private agreements among corporate actors provide no similar opportunity for scrutiny. For advocates of these agreements, the looser nature of the agreements is highly useful. It means, for example, that there is no defined threshold of criminality. Rights holders and macro-intermediaries thus have the flexibility to target sites that are selling only one counterfeit item if they choose. For critics of these agreements, however, the looseness is extremely problematic. It means that sites that sell a mixture of legitimate and infringing goods, whether deliberately or unintentionally, could be crippled commercially instead of given a chance to address the infringing items. Despite these challenges, this dissertation adopts the term infringing site because it is commonly used. It does so, however, with the proviso that such sites are designated as infringing based on allegations, not proof, of infringement by rights holders. Macro-intermediaries generally require only a statement of good faith from the rights holders, not any definitive proof of infringement like a test purchase of a suspected counterfeit good.⁴⁴

Rights holders argue that the online distribution of counterfeit goods is too large, complex and difficult for rights holders to address alone. In concert with their trade associations, they have increasingly pressured macro-intermediaries like eBay to crack down on the online distribution of counterfeit goods. Advocates for this shift in regulatory responsibility to Internet intermediaries often emphasise that these intermediaries facilitate criminal activities, whether knowingly or inadvertently. They also say that, in some cases, these

⁴⁴ A test purchase refers to the practice of rights holders (or their investigators) buying a counterfeit good, examining it and documenting the features that prove it is a counterfeit. The European Commission's agreement, for example, does not require that rights holders make test purchases to prove that the targeted goods are indeed counterfeit and not second-hand goods or legitimate goods diverted from another market (see European Commission 2013).

intermediaries benefit financially from providing services those selling counterfeit goods. “eBay is making money out of this,” argues Ruth Orchard, the director of the Anti-Counterfeiting Group, a trade association in the United Kingdom. “They take a commission on each sale whether it’s a counterfeit or a real item.”⁴⁵ Similar arguments have been leveled against Google, PayPal, Visa and MasterCard.

Proponents of increased protection tend to want all types of intermediaries to strengthen their enforcement policies, from marketplaces, web hosts and payment providers to advertising platforms, search engines, and domain service providers. However, they particularly wanted to convince macro-intermediaries—Google, PayPal, Visa, GoDaddy and the handful of others—to adopt tougher policies. Rights holders, particularly those with popular, often-counterfeited brands, sought to enlist macro-intermediaries as their gatekeepers, effectively acting as transnational brand police. Gatekeepers are parties that can facilitate and/or control the flow of particular phenomena, such as individuals, information, behaviour or funds and are not the primary authors or beneficiaries of the wrongdoing (Kraakman 1986; Mazerolle and Ransley 2004).⁴⁶ Rights holders were able to persuade the states involved in the private enforcement agreements to secure macro-intermediaries’ cooperation because of shared interests between rights holders and the governments involved.

iv) *State and Corporate Inter-dependencies*

As discussed earlier in this chapter, the rights holders pushing for private enforcement agreements with macro-intermediaries are billion-dollar brands. They operate persuasive, well-funded lobbying campaigns through prominent trade associations like the International Anti-Counterfeiting Coalition. In concert with these associations, they use the threat of legal action to convince macro-intermediaries to strengthen their enforcement practices, as will be discussed in chapters 4 to 6. They work with government agencies to set tough rules and

⁴⁵ Interview with Ruth Orchard, Director, Anti-Counterfeiting Group, England, 17 September 2012, by Skype.

⁴⁶ Gatekeeping is traditionally understood as a state-steered process for delivering a public good, such as creating safer neighbourhoods. States take an active role in identifying relevant third parties and securing their cooperation. In return, states may compensate or reward gatekeepers (Kraakman 1986; Mazerolle and Ransley 2004).

standards to protect intellectual property, including the privately drafted, non-binding enforcement agreements. They go to these lengths because the stakes are enormous. Multinational rights holders, like Nike and Apple, owe their massive revenue and highly lucrative brands to the careful preservation of their intellectual property rights. They are keen to maintain their advantage by advocating for the ever-increasing protection of these rights. Private enforcement agreements with macro-intermediaries offer rights holders a useful opportunity to shift some of their enforcement burden to Internet firms and payment providers. But more importantly, these agreements allow rights holders to undertake global enforcement campaigns in a manner that previously would have been unattainable or prohibitively expensive. With their vast, global platforms and technologically sophisticated surveillance and enforcement capabilities, macro-intermediaries can conduct mass policing of Internet networks, platforms and services. They can also enact technological chokepoints to throttle suspicious transaction or activities. By partnering with macro-intermediaries, rights holders can police their brands globally, rapidly and in relative secrecy.

Rights holders' interests are clear but what about those of macro-intermediaries and the governments involved? In contrast to rights holders' decades of experience in influencing intellectual property policymaking, Internet firms like Google and GoDaddy are political neophytes and are relatively new to the political-lobbying game (Sell 2013).⁴⁷ Threats of legislation from governments in the United States and United Kingdom and legal action from rights holders are a factor in macro-intermediaries' decision to enhance their enforcement practices. However, this is not purely a story of state coercion. There are important interdependencies between the state and these macro-intermediaries. Governments, particularly the United States, are increasingly reliant upon macro-intermediaries' vast troves of personal and commercial data to facilitate law enforcement, national security and economic policies. This is clearly evident from Edward Snowden's leaked files that show the U.S. National Security

⁴⁷ The protests over the *Stop Online Piracy Act* revealed the gulf in political lobbying capacity between Internet firms like Google, Yahoo and Facebook and the entrenched, institutional power of trade associations like the Motion Picture Association of America (Sell 2013). Since that time, however, Google has been developing its political lobbying capacity.

Agency's dependence on Google and Yahoo.⁴⁸ Macro-intermediaries, in turn, receive a degree of legitimation and protection for their often-controversial corporate surveillance programs and can lobby the U.S. government on issues of concern to their industry, such as privacy and the storage of personal data. This interplay of state-corporate interests, which is explored throughout the dissertation, indicates that Internet firms' adoption of private agreements has broader ramifications than merely the regulation of online infringement.

V) Review of Literature: Where Transnational Policing and Corporate Regulation Meet

The logical literature in which to base this research is that of the private security industry. Corporate anti-counterfeiting activities are part of the brand-protection sector, which itself is a component of the private security industry. In general, however, research on high policing by private actors, which includes investigative and security consultancy work, is critically under-examined (see Brodeur 2007; Bowling and Sheptycki 2012).⁴⁹ This problem is especially acute in relation to corporate actors conducting enforcement activities transnationally (exceptions include Bowling and Sheptycki 2012; O'Reilly 2011; O'Reilly and Ellison 2006). Despite the under-developed nature of this area, a small but useful literature provides helpful insights into mutually beneficial corporate-state interactions that shed light on macro-intermediaries' actions (e.g., Bowling and Sheptycki 2012; Johnston 2000; O'Reilly 2010). Overall, the private security literature is significantly under-developed in relation to transnational corporate investigative work, particularly in regards to the Internet.

Given these gaps, this dissertation draws extensively from the socio-legal literature to explore ideas of corporate regulation through Internet intermediaries and shifting notions of regulatory responsibility among corporate actors (e.g.,

⁴⁸ The leaked Snowden files revealed that the U.S. NSA collected intelligence to help the U.S. position in trade talks. In one case, the NSA obtained information from the Australian security services on a U.S. law firm that was retained by the government of Indonesia (Jabour and Pengelly 2014).

⁴⁹ This is in contrast to the booming literature in front-line private security duties, which includes guarding specific spaces, like malls or airports, or certain populations, like prisoners or tourists (see Brodeur 2007).

Benkler 2011; Weatherall 2012; Zittrain 2006). A rapidly growing literature on intermediaries provides relevant insights into their regulatory capabilities and responsibilities, as well as the procedural and normative concerns raised by their regulatory efforts (e.g., Elkin-Koren 2001; Laidlaw 2009; McIntyre and Scott 2008). Of particular use to this dissertation are analyses of intermediaries' enforcement abilities and limitations particularly those that assess the implications of intermediary-facilitated regulation (Barzilai-Nahon 2006; Kohl 2012; Laidlaw 2012). Much of the research in this area examines the role of Internet service providers, web hosts and search engines in controlling copyright infringement (e.g., McIntyre and Scott 2008). There is, however, a small but growing body of literature that considers the roles of payment, social networking, and domain name intermediaries as gatekeepers (i.e., enforcers) in other types of wrongdoing (e.g., Kohl 2013; Lindenbaum and Ewan 2012; Mellyn 2010).

In relation to corporate anti-counterfeiting efforts, there is a paucity of scholarly research relating to the online or physical world (notable exceptions include Mackenzie 2010 and 2010a). There is a small but highly relevant body of research that critically questions how counterfeiting can (and should) be policed and the public interest in doing so (e.g., Mackenzie 2010; Mertha 2007; Urbas 2005; Wall and Large 2010). Scholarship that argues that counterfeiting can, in some cases, stimulate innovation (e.g., Raustiala and Sprigman 2012) and that heavy-handed corporate enforcement practices can unfairly constrain legitimate behaviour (see Mazzone 2011) provide a useful corrective to industry and government narratives of unmitigated harm. Much of the academic literature on counterfeiting, however, can be rather crudely divided into two broad areas: supply and demand. This literature provides useful detailed analyses of consumer demand for, trends in and challenges of policing counterfeit products. The demand-side literature examines consumer attitudes toward counterfeits of different brands and products, and predictor variables for the purchase of counterfeits (e.g., Arghavan and Zaichkowsky 2000; Rutter and Bryce 2008; Swami et al. 2009). The supply-side literature generally analyses trends in the manufacturing and distribution of counterfeits (e.g., Chaudhry et al. 2009), focuses on specific countries (e.g., for China, see Chow 2003) or products (e.g., for cigarettes see Shen et al. 2010).

VI) Theoretical Framework and Methodology

i) *Theoretical Framework*

To explain the creation of non-binding enforcement agreements and macro-intermediaries' adoption of them, in chapter 2 this dissertation's theoretical framework brings together concepts from two distinct, yet inter-related areas of scholarship. The first is the non-state governance literature within international relations, which accounts for regulatory authority existing outside the state. The second is the law and technology literature, which explores the complexities of regulating through technology, along with attendant procedural and normative concerns. From the non-state governance literature, the dissertation draws upon the concept of "private authority" to explain how and under what conditions corporate actors can set and enforce rules. It also adopts the concept of "regulatory regime" to capture the array of actors involved in regulatory efforts against online infringement. Through the law and technology literature, the dissertation considers ideas of corporate actors regulating through technological intermediaries and the use of technology as a regulatory instrument. The three-part theoretical framework weaves together concepts of regimes, private authority and technologically facilitated regulation to explain the creation and rapid adoption of informal private enforcement agreements.

The concept of a regulatory regime provides a useful analytical framework to explain the emergence of a particular regulatory arrangement, identify all stakeholders and account for complementary and divergent interests. Regimes are understood here as "the full set of actors, institutions, norms and rules" (Eberlein and Grande 2005:91) that comprise a particular regulatory arrangement. The advantage of using the term is that it explicitly recognises corporate actors' capacity to make and enforce rules, particularly through "soft law" measures, such as non-binding industry codes of conduct or best practices. Further, it is sensitive to inter-dependencies between state and non-state actors and importantly recognises that the state plays a key role in directing, shaping or endorsing private regulation.

Private authority, meanwhile, usefully explains how corporate actors can acquire the capacity to set and enforce rules governing the conduct of others and the constraints upon that capacity. This dissertation understands private authority as the capacity of non-state actors “to create rules or standards that other actors adopt” (Green 2013:29).⁵⁰ Rights holders must have the capacity to persuade others, specifically macro-intermediaries, to adopt their rules. Corporate actors’ authority to convince them to do so is limited and, faced with reluctant macro-intermediaries rights holders must solicit assistance from the state. Analysis of corporate actors’ private authority enables the researcher to determine the extent to which the private regulation is dependent upon the state. Private authority is partially derived from the state, as the state arbitrates among competing private interests and makes decisions that favour some actors over others (Braithwaite and Drahos 2000; Peters et al. 2009).

Finally, the law and technology literature offers ways to consider how rights holders and macro-intermediaries use technology to facilitate regulation. “Techno-regulation” refers to deliberate efforts to shape individuals’ behaviour through technology (Leenes 2011). This literature draws on principles from science and technology studies to emphasise that technology is socially constructed, and that technology and politics shape one another (Brey 2005; Franklin 1995; Latour 2005). Rights holders and macro-intermediaries use technology, such as automated surveillance programs, to detect anomalies and possible violations of firms’ policies. Techno-regulation enables analysis of how technology facilitates users’ compliance and shapes the nature of regulation and policing in this space.

ii) ***Methodology***

There is virtually no scholarly research on corporate anti-counterfeiting efforts, particularly through private enforcement agreements. Thus, I undertook an exploratory approach (Blaikie 2000) to gain a deep, detailed understanding of the phenomenon and to trace the actors involved in regulating sites selling counterfeit goods. I first conducted a series of preliminary interviews in several

⁵⁰ Green (2013) employs this definition to examine non-state actors’ involvement in global efforts to set rules in relation to climate change but the definition can usefully be applied to other types of non-state regulation.

Australian cities, as I was based in Australia. These interviews enabled me to gain a thorough understanding of corporate anti-counterfeiting strategies and initiatives and a good knowledge of the brand-protection industry. The Australian interviews and subsequent interviews in the United States and United Kingdom led me to private enforcement agreements in Canada and in China that involved, respectively, payment providers and marketplaces. I sought to examine the core of online anti-counterfeiting efforts undertaken by actors who were directly involved in working with intermediaries and creating the private agreements. The dissertation focuses on eight non-binding private enforcement agreements adopted between 2010 and 2013 by payment, advertising, search, marketplace and domain name macro-intermediaries.

The United States is the epicentre of these efforts. In particular, the Office of the Intellectual Property Rights Enforcement Coordinator (IPEC) shaped many of the agreements. Alongside the United States, the European Union has a strong history of encouraging self-regulation on the Internet. The European Commission took a lead role in facilitating the creation of an informal agreement among marketplaces and rights holders covering the European Economic Area. In the United Kingdom, the Department for Culture, Media and Sport, like IPEC, shaped and facilitated informal enforcement agreements. The European Union and the United States are home to rights holders and trade associations with a long, successful history of lobbying for greater protection for intellectual property rights. Their enforcement activities are at the vanguard of online anti-counterfeiting efforts and their private agreements are the first that pertain to the online distribution of counterfeit goods. By examining informal regulatory efforts in the United States and European Union, I was able to analyse agreements across the payment, advertising, search, marketplace, and domain name sectors. I selected the Canadian merchant-account termination case to provide a counterpoint to that in the United States. Both programs target sites selling counterfeit goods.

iii) *Research Methods*

I conducted 91 semi-structured interviews with rights holders, trade associations, Internet firms and payment providers, government officials,

attorneys, investigative firms and civil-society groups in the United States, the United Kingdom, Canada and Australia. The majority of the interviews were conducted in Washington, DC, New York City and London, United Kingdom. Initial interviews were undertaken in my home base of Australia to gain a detailed understanding of anti-counterfeiting enforcement and to identify the main players, trends and issues in the field. As most of the individuals interviewed were in managerial positions as directors of investigative firms or rights holders' brand-enforcement units, elite interviews were the most appropriate method (Bygnes 2008).

Wanting to speak with individuals with direct experience in creating the informal agreements and in conducting anti-counterfeiting enforcement efforts, I interviewed individuals from a wide range of industries: pharmaceuticals, apparel and accessories, sporting goods, commercial electrical components and consumer electronics. This diversity enabled me to examine the online regulation of counterfeit goods across industry sectors. To consider perspectives critical of corporate anti-counterfeiting enforcement, I interviewed representatives from Public Knowledge, the Centre for Democracy and Technology, the Program on Information Justice and Intellectual Property at American University, and The American Assembly at Colombia University. I modified the interview questions according to the participant's expertise and roles. The interviews were a mixture of in-person, telephone, email and Skype interviews depending on the participant's availability and preferences.

The majority of interviewees agreed to digitally recorded for-attribution interviews and these individuals are named in the research when they are quoted (see Appendix A).⁵¹ Some asked that their comments not be attributed to them. Their names and organizations have been removed in citations accompanying their quotations. Despite repeated requests for interviews, some Internet firms declined to participate in this project. In particular, I was unable to speak with any search, marketplace or domain name intermediaries. However, I remedied this by interviewing attorneys, rights holders and investigative firms

⁵¹ Many of the brand-monitoring and investigative firms interviewed for this dissertation provided detailed background information on the brand-protection industry and corporate anti-counterfeiting efforts but are not cited directly in the text (see Appendix A).

who interact with these firms' for their perspectives on the macro-intermediaries' anti-counterfeiting activities. I also consulted macro-intermediaries' corporate annual reports, press releases, corporate blogs, media interviews, court documents and testimony before government committees in the United States and United Kingdom.

I used judgment-purposive sampling to identify individuals with direct experience in conducting or facilitating online anti-counterfeiting efforts (Teddle and Yu 2007). I identified individuals with relevant experience through trade association websites, such as the U.S.-based International Anti-Counterfeiting Coalition and the U.K.-based Anti-Counterfeiting Group. Based on these interviews, I used snowball sampling to reach other interviewees (Atkinson and Flint 2001).

In addition to interviews, in May 2012, I attended a three-day industry conference hosted by the International Anti-Counterfeiting Coalition in Washington, D.C. that focused on anti-counterfeiting enforcement strategies, which proved invaluable as a window into the state's role in private agreements. I consulted a range of media sources, including specialised technology/intellectual property sites and blogs, particularly, *TechDirt*, *Wired*, *Ars Technica*, *TorrentFreak* and *The Register*. I also regularly reviewed sites and blogs for the Electronic Frontier Foundation, the U.K. Open Rights Group and the European Digital Rights Initiative.

VII) Argument

Despite participants' rhetoric of "voluntary" agreements among macro-intermediaries, the state played a key role in constructing and legitimising the informal private regulatory regime. Government agencies in the United States and the United Kingdom, along with the European Commission, employed various coercive methods to compel macro-intermediaries to adopt the agreements, including threats of legal action and legislation. This coercion stimulated cooperation from macro-intermediaries but these actors also have some common interests with rights holders and the government agencies involved. Both rights holders and macro-intermediaries have strong financial

and reputational interests in protecting their brands from association with criminality and in ensuring safe e-commerce and online environments.

Rights holders' private authority is limited as they were unable to persuade macro-intermediaries to adopt wholesale changes to their rules. Coercive pressure by states, along with rights holders' threats of legal action, convinced macro-intermediaries to adopt the private enforcement agreements. These agreements are a novel development in the online regulation of intellectual property. They accord multinational corporations access to a powerful regulatory capacity—some of the largest Internet firms and payment providers—that was previously only available to the U.S. government to control problems like commercial child pornography sites and the illegal gambling sites (MacCarthy 2010). Macro-intermediaries' adoption of private agreements has fundamentally altered the online regulation of infringement. Their enforcement efforts under the agreements are more coordinated, streamlined, rapid and proactive than their previous efforts.

The United States and European Union intervened on behalf of rights holders because these states have strong economic interests in seeking strengthened protection for intellectual property. In comparison with macro-intermediaries, rights holders' have a long-standing, entrenched position of influencing policymaking in the United States and Europe. The states involved in the private enforcement agreements also have more strategic motives for facilitating macro-intermediaries' global regulatory efforts on the Internet. The United Kingdom and European Union, for example, have interests in exerting greater control on the Internet in terms of illegal content by tapping into macro-intermediaries' considerable surveillance and enforcement capabilities to shut down child pornography sites and extremism sites (Fae 2014; Laidlaw 2012). In terms of national security, state security agencies in the United States and United Kingdom rely upon macro-intermediaries' mass accumulation of users' personal and commercial data, as demonstrated by Edward Snowden's leaked files. More broadly, the U.S. government has economic and national security interests in expanding its standard-setting capacity on the Internet by working with—and through—macro-intermediaries, in areas like encryption and data storage practices.

The private regulatory regime created by the enforcement agreements has distinctive U.S. origins, which underscores the U.S. role as the strongest proponent globally for the protection of intellectual property rights. The regime, based in the United States and Europe with branches in Canada and China, stretches worldwide and enables proponents of stronger enforcement practices to export globally a U.S.-style approach to intellectual property enforcement. This regulatory regime was born in and is conducted from the shadows. Its rules come from closed-door meetings among small groups of powerful corporations and its actors operate without any democratic oversight.

Advocates for intellectual property justify the enforcement campaigns to protect consumers from being deceived or defraud by counterfeit goods. Consumers, however, do not have a voice in the regime and there is no representation from consumer organisations. Government agencies involved in the regime do not represent consumers' interests or, more broadly, those of the public in relation to core digital rights, particularly privacy. Given these problems and governmental interest in facilitating secretive private regulation on the Internet, it is an open question whether these government bodies can represent consumers and the general public. This dissertation argues for the public to become politically engaged over the issue of state-corporate regulation on the Internet. A promising avenue is Brazil's *Marco Civil da Internet*, which is a digital bill of rights introduced in March 2014 and drafted in an open consultative process. The law, which in part is a response to the NSA spying scandal, enshrines protection for digital privacy, among other provisions.⁵²

⁵² An English-language version of the Marco Civil law is available from the Geneva Internet Platform, operated by Diplo, a civil-advocacy group promoting diplomacy and democracy among small and developing countries, see: <http://giplatform.org/resources/text-brazils-new-marco-civil>.

VIII) Overview of Chapters

Chapter 2 situates this dissertation within the non-state governance and regulatory studies literatures and sets out its theoretical framework by drawing upon the concepts of regulatory regimes and private authority from non-state governance literature and techno-regulation from the law and technology literature. Chapter 3 establishes the political, legal and technological context for the emergence of informal enforcement agreements. It examines how Internet firms and payment became gatekeepers for rights holders and traces legislation that has shaped online enforcement efforts, particularly the U.S. *Digital Millennium Copyright Act*, the *European Union E-Commerce Directive*, and the U.S. *Stop Online Piracy Act*.

Chapters 4 to 6 present the dissertation's empirical findings. Chapter 4 analyses private agreements involving payment and advertising macro-intermediaries. Chapter 5 considers how search engines and domain registrars are increasing their regulatory efforts against online infringement. Chapter 6 focuses on online marketplaces' enforcement efforts against the distribution of counterfeit goods. Each of these chapters examines the pressure on macro-intermediaries to become gatekeepers for rights holder, explains their regulatory policies and practices, and explores the involvement of government actors in shaping the agreements. Chapter 7 draws upon the empirical findings to discuss the inter-dependencies and varying interests among actors in the regulation of online infringement and, more generally, corporate regulation on the Internet. It underlines the absence of consumers and suggests ways that the interests of consumers and the public more generally can be represented. Chapter 8 summarises the dissertation's findings, reflects upon the characteristics of corporate online regulation and considers ways to strengthen the private enforcement agreements. The dissertation concludes by proposing ways to raise public awareness of the troubling aspects of the private regulatory regime and calls for greater political engagement by the public in this area.

Chapter 2: Regulating Through the State

The analytical puzzle at the heart of this dissertation is why macro-intermediaries agreed to adopt non-legally binding private enforcement agreements to regulate online infringement on behalf of rights holders. More broadly, the dissertation explores how private regulatory regimes function and the degree to which they rely upon the state. To explore these questions, this dissertation takes an interdisciplinary approach. It brings together two distinct, yet inter-related areas of scholarship: the non-state governance literature within international relations and the law and technology literature. By drawing together these literatures, the dissertation constructs a theoretical framework that explains the role of the state in private regulation and is attentive to corporate-state dynamics in the creation and operation of private anti-counterfeiting efforts on the Internet.

From the non-state governance and the law and technology literatures, the chapter weaves together three concepts: regulatory regimes, private authority, and techno-regulation. Regimes refer to all the actors and rules involved in a particular regulatory arrangement. The concept provides a useful analytical framework to trace the key state and corporate actors involved in constructing the private agreements and examine their overlapping and competing interests. Alongside the concept of regimes, private authority explains how corporate actors can acquire and wield authority, as well as the nature and limitations of that authority. This dissertation understands private authority as the capacity of corporate actors to make rules that other private parties adopt (Green 2013). By pulling together regimes and private authority, the dissertation is attentive to the inter-dependencies between corporate and state actors, and to the relationship between private authority and the state. From the law and technology literature, the chapter uses techno-regulation, which refers to the use of technology as a regulatory instrument to shape human behaviour (Leenes 2011:14). Technology underlies this regulatory regime and techno-regulation helps explain how both rights holders and states shape macro-intermediaries' enforcement practices.

The chapter proceeds as follows. First, it explains how this dissertation understands the authority of the state in relation to private regulation and then situates the dissertation within the non-state governance literature and regulatory studies (a subfield of socio-legal studies). Then the chapter explains how corporations can act as regulators and explores corporate and state interests in private regulation. Third, the chapter discusses the concept of private regulatory regimes and then examines the concept of private authority. Fifth, the chapter turns to explore how technology can be used as a regulatory instrument. The final part draws together the concepts of regimes, private authority and regulation through technology to explain how this dissertation understands the private online anti-counterfeiting regime.

I) Conceptualising the State's Role in Regulation

In considering corporate actors' interactions with the state, it is first important to consider critically the role of the state in these regulatory relationships. A useful way to understand the state is through the theoretical framework of regulatory capitalism, as expounded by John Braithwaite (2005 and 2008) and David Levi-Faur (2005). Regulatory capitalism is premised upon neoliberal principles of privatisation, competition and a decentred state that directs rather than performs regulation (Braithwaite 2000:222).⁵³ Neoliberalism, in this specific context, is understood as referring to ideas of privatisation and deregulation, including a diminished public sphere (Braithwaite 2005:3). However, in many cases, as state functions were privatised, the demand for oversight bodies to monitor those out-sourced functions created an impetus for more not fewer regulatory agencies (see Braithwaite 2005; Levi-Faur 2005).⁵⁴ The proliferation of oversight and regulatory bodies accompanying neoliberalism created what some call the "audit society" (Power 1997) and others refer to as the "regulatory state" (Braithwaite 2000; Majone 1994). In this landscape, the state takes on a meta-regulatory role, while corporate actors interact directly and indirectly with it in the provision and enforcement of rules.

⁵³ For an analysis of the transition from the Keynesian welfare state to the new regulatory state with its neoliberal underpinnings, see Braithwaite (2000) and Majone (1994).

⁵⁴ Braithwaite (2005) describes the creation in Britain of new regulatory agencies following the privatisation of telecommunications, gas, water and electricity sectors in the 1980s. Levi-Faur (2005) tracks the privatisation of the telecommunications and electricity sectors globally and the rise of new regulatory institutions.

i) ***Governing through Regulation***

States, markets and society are not distinct entities in regulatory capitalism; instead, the state is embedded in the economic and social order (Levi-Faur 2005:14). States and markets are part of a condominium, an ensemble that shares the same dynamics of governance (Underhill 2003:757).⁵⁵ States must be understood as embedded in “wider, increasingly transnational social structures” and non-state, typically corporate, actors are “integrated into the institutional processes of states and government” (Underhill 2003:765). Conceptualising state-market relations as a condominium entails recognition that political processes help constitute the market, and that market actors partially construct the state’s policy preferences (Underhill 2003). The degree to which market actors can influence state policymaking depends on their organisational capacities and their power (Underhill 2003:765). While the state shapes and is shaped by the market, it retains interests and goals distinct from those of prominent corporate lobbyists. The state, then, is both a quasi-autonomous actor and a battlefield for social interests in which actors advocate for certain agendas and attempt to influence state policymaking (Haggart 2014).

The regulatory state deploys power “through a regulatory framework rather than through the monopolisation of violence or the provision of welfare” (Walby 1999:123 in Braithwaite 2005:11). Since the 1980s, states have shifted from providing regulation through the production and enforcement of rules to shaping the provision of regulation by non-state actors (Jordana and Levi-Faur 2004). The nature of this shift is captured in the oft-quoted metaphor of “steering” and “rowing.” In this nautical image, the state strategically “steers” or directs regulatory efforts from a position of meta-governance, while non-state actors (e.g., business and civil-society actors) take on the state’s traditional task of “rowing” by creating and operating various regulatory arrangements (Osborne and Gaebler 1992).

The state in regulatory capitalism retains authority by governing through regulation (Levi-Faur 2013:39; Rhodes 2012). Its capacity enables it to direct, empower, endorse, shape or deny regulatory efforts (Büthe 2010; Cutler 2002).

⁵⁵ Here Underhill draws upon ideas from Karl Polanyi and his argument that the state created and enforced the market system (Underhill 2003:765).

The state may direct regulatory efforts by mandating or facilitating a particular regulatory approach. It may also govern indirectly by empowering regulators to enact rules, shaping discourse and distributing resources (Levi-Faur 2013:39; Rhodes 2012). The regulators empowered by the state are an array of state, civil-society and corporate actors who are involved in producing, implementing and/or enforcing rules. The state may also provide incentives to corporate and civil-society actors to create or enforce certain rules and standards.⁵⁶

II) Corporations as Regulators

Building upon the above discussion, the state arbitrates among competing non-state interests and, in doing so, reflects the relative power of specific actors. In addition to recognising the variety of non-state actors, regulatory capitalism also usefully acknowledges the clout of large corporate actors that Braithwaite (2005) terms “mega-corporate.” Such actors have the capacity to lobby for policies that benefit their interests, such as stronger protection of intellectual property rights, that may impose costs on smaller businesses or new entrants to the sector (Braithwaite and Drahos 2000). They also have the capacity to create their own rules and standards, both domestically and transnationally to regulate their individual corporations, their global supply chains, or even industry sectors (Cafaggi 2012). Not all corporate actors, however, have equal resources to persuade states to support their regulatory preferences or command the same degree of influence in shaping state policymaking processes. Similarly, states do not have an equal capacity to influence, stimulate or control corporate regulation in the same degree as powerful, industrialised actors like the U.S. and U.K. governments and the European Commission.

i) Corporations Setting and Enforcing Rules

The non-state governance literature within international relations and the regulatory studies literature are valuable to this dissertation because they usefully account or how corporate actors can set, implement and enforce rules

⁵⁶ Gunningham and Grabosky (1998) and Grabosky (2005) outline the various ways that the state can persuade non-state actors to participate in regulatory activities, such as by providing tax incentives.

transnationally. Of particular use are studies that explain the legal source of corporate actors' authority to set and enforce rules and the degree to which they can impose those rules on other actors. Corporate actors may derive their authority from a public statute to perform a service delegated by the state (Scott 2002). Private security companies that transport and guard prisoners, for example, fall into this category. Another form of authority comes from contracts (Cafaggi 2012; Scott 2002). Corporations can set rules or standards within their supply chains through contracts with their manufacturers and suppliers, for instance, in relation to food standards (Fuchs and Kalfagianni 2010) or environmental standards (Vandenberg 2007). Finally, corporate actors may have no formal legal authority to regulate but instead set rules through litigation, persuasion, or the control and dissemination of information (Scott 2002). Corporate social responsibility codes that are based on non-legally binding agreements fall into this category (Dashwood 2012; Prakash and Potoski 2014).⁵⁷

Analyses of the sources of corporate actors' authority can help explain the types of rules they have the capacity to enforce and the degree to which they can impose those rules on other parties. Companies with supply-chain contractual agreements, for example, can set quality-control standards and terminate their relationship with non-compliant suppliers (Fuchs and Kalfagianni 2010). Rights holders, in contrast, have no such contractual relationship with macro-intermediaries. They can, however, use litigation to try to force the Internet actors to accept their rules. This literature helpfully accounts for how corporate actors use different types of authority to set and enforce rules, which provides a useful context to consider the capacity and limitations of corporate actors to set and enforce rules (Avant, Finnemore, and Sell 2010).

⁵⁷ These codes are often joint agreements between civil-society organizations and corporations to address certain problems resulting from poor industry practices, such as pollution, or to improve industry practices in particular areas, such as human rights or labour standards (e.g., Bartley 2007).

ii) ***Corporate and State Interest in Private Regulation***

The non-state governance and regulatory studies literatures have generated a significant body of research that usefully explains why corporate actors may prefer private regulation to other forms of governance, under what conditions, and for what issues. One of the principal reasons that corporations may form transnational private arrangements is because states are incapable or unwilling to provide transnational governance on certain issues (Cafaggi 2012; Scott 2012), or in a manner that corporations consider appropriate. By creating private standards, corporate actors can attempt to address gaps in regulation or harmonise competing or uneven rules internationally in order to make governance efforts more effective (Büthe 2010; Cafaggi 2012). Multinational corporations working alongside civil-society groups, for example, have created international standards in relation to the commercial use and preservation of forests (Meidinger 2002). Corporate actors may also be strategic in their creation of rules in order to pre-empt possible government regulation (Büthe 2010) or to water down existing rules (Black 2008; Cutler, Hauffler, and Porter 1999). Finally, there may be normative reasons for corporate actors' adoption of private rules, such as to repair or safeguard their reputations. For example, following criticism of Apple's supply-chain practices, the company began disclosing lists of its suppliers of valuable metals used in its products to prove that they are obtained in conflict-free countries.⁵⁸

There are many pragmatic reasons for states to push corporate actors to create private standards or support private governance efforts, although individual states' specific interests may vary by issue. It is important to recognise that states may have diverse and sometimes competing goals and interests, as they are not unitary actors. Private regulation may offer states a regulatory approach that is more responsive and adaptive to changes in technology or circumstances than legislation, international law or agreements (Büthe 2010; Cafaggi 2012). States can also draw upon corporate actors' actual or perceived specialised technical or industry knowledge, and greater access to markets (Cutler, Hauffler, and Porter 1999). In 2012, for example, the U.S. government

⁵⁸ Apple uses third-party auditors to ensure that all of the tantalum smelters in its supply chain are designated conflict free. Tantalum is a hard metal used in making electronics (Apple 2014).

determined that its technology firms were best placed to address the problem of botnets⁵⁹ and requested top companies to form a voluntary working group. States may also perceive corporate actors as more responsive, cost-effective and efficient regulators than government agencies in certain areas (Büthe 2010; Cafaggi 2011; Cutler, Hauffler, and Porter 1999; Eberlein et al. 2013). States can also strategically use private actors to reach beyond their traditional jurisdictional boundaries or to regulate at a scale unfeasible for government agencies (Büthe 2010). The U.S. government, for example, works with U.S. payment providers, including Visa and PayPal, to crack down on illegal gambling websites targeting the United States (MacCarthy 2010).

III) Regulatory Regimes

There is a diverse array of corporate actors involved in online anti-counterfeiting efforts, as they comprise rights holders from a broad range of industries and firms providing a wide range of Internet services. The concept of a regulatory regime, drawn from the non-state governance literature in international relations, provides a useful analytical framework to explain how and why a particular form of regulation emerged, interactions amongst actors, and the interests it serves.

i) *Employing the Concept of Private Regimes*

Private regulatory programs, particularly those that extend transnationally, can be complex in their structure and comprise a diverse array of state, civil-society and corporate actors. The concept of a regime from international relations provides a useful analytical framework to examine the array of actors involved in corporate online anti-counterfeiting efforts. Stephen Krasner and Robert Keohane, along with other international relations scholars, developed the concept of regimes to explain the role of non-state actors in global governance and, in doing so, provided a corrective to state-centric analyses (Cutler 2002:26). Krasner's classic definition of regimes refers to "sets of implicit or

⁵⁹ Botnets are networks of Internet-connected computers that are controlled through software and harnessed to conduct activities, such as the distribution of spam. Participants in the Industry Botnet Group include Microsoft. See: <http://www.industrybotnetgroup.org/>.

explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge" (Krasner 1982:185). This dissertation adopts a definition more focused on regulation and understands regimes as "the full set of actors, institutions, norms and rules" (Eberlein and Grande 2005:91) comprising a particular regulatory arrangement. Scholars of non-state governance within international relations, particularly A. Claire Cutler, Deborah Avant, Virginia Haufler, Thomas Biersteker and Rodney Bruce Hall, further expanded the concept of regimes to explain non-state actors' capacity to set and enforce rules transnationally (see particularly Cutler, Hauffler, and Porter 1999).

Eberlein and Grande's (2005) definition of regimes recognises corporate rule- and norm-making efforts using informal governance practices, such as those involving industry codes of conduct or best practices agreements. It also appreciates that privately set rules or standards may operate independently or may rely upon or complement state laws. The concept of regimes is agnostic as to the level of actors: regimes may encompass actors that operate across states as well as those that work within states. A regime may be defined as transnational according to the scope of the rule-setting actors, the level of the rule-setting institutions, the scope of the rules themselves, or a combination of these factors (Mügge 2006:179). Regardless of a regime's scope, however, it may also have roots within a specific territorial base or embody distinctly local features (Graz and Nölke 2008:10). These local roots may infuse a regime with characteristics that shape its character or operation. Prominent rule-making actors, for example, may all be based within the global north creating rules that govern how transnational mining companies operate in the global south (see Dashwood 2012).

Using regimes provides another advantage. Regimes are also useful to account for similarities and differences among actors' material and ideational interests in relation to the governance of a particular issue. Actors may have conflicting, sometimes irreconcilable differences that shape the composition and function of governance arrangements. Regulatory efforts that materially benefit one party can impose costs on the other. Using regimes can help trace the particular historical and socio-cultural context from which actors emerged to form

particular regulatory arrangements. They can help trace, for example, the long history of U.S. rights holders and trade associations in shaping intellectual property policymaking in the United States and internationally (Drahos and Braithwaite 2002; Sell 2003). The concept is also particularly attentive to the dynamics and inter-dependencies between state and non-state actors. As a result, one can analyse the relative power of actors and account for the growing influence of corporate actors in transnational governance (Hall and Biersteker 2002; Peters et al. 2009).

By focusing attention on state-corporate inter-dependencies, the researcher can investigate the conditions under which corporate actors seek state involvement in private regulatory regimes and the degree to which private regulation relies upon the state (Graz and Nölke 2008). In doing so, analysis can also reveal the governmental interests in facilitating private regulation. Determining the nature of state involvement in private regulation is crucial but can be difficult as not all actors may be publicly visible in their regulatory activities. In the case of private anti-counterfeiting efforts, the state is omnipresent in constructing and endorsing private enforcement agreements on behalf of rights holders but is largely obscured from public view.

The concept of regimes has useful explanatory power to account for interactions and inter-dependencies among actors, their spatial scale, and their ideational and material interests in forming regulatory arrangements. However, the concept does not contain an explanation of power. Used alone, regimes cannot explain how private actors are able to acquire and wield authority over others, which actors can acquire regulatory authority, or the ways in which that authority is limited or constrained.

IV) Private Authority

U.S.-based rights holders and their trade associations have a history of successfully influencing state policymaking in relation to intellectual property stretching back to the 1970s, as was discussed in chapter 1. More difficult, however, has been their task of convincing macro-intermediaries to adopt rules voluntarily that would strengthen their enforcement practices. The principal

challenge rights holders face is that they have a relatively limited capacity to persuade macro-intermediaries because private actors do not possess the coercive capacity of the state. How then can rights holders convince macro-intermediaries to adopt and enforce their rules?

i) ***Claiming Private Authority***

Private actors' capacity to regulate is based on two inter-related concepts: authority and legitimacy. The concept of authority, as noted by Max Weber, is inextricably linked to legitimacy and tied to the idea that states have a monopoly on the legitimate use of force (Whimster 2004, see also Cutler 2002). By adapting this concept to non-state actors, the idea of private authority can explain how corporate actors can create, implement and enforce rules, why other actors may abide by those rules, and the different types of legitimacy they may draw upon (Avant, Finnemore, and Sell 2010; Black 2008; Büthe 2010; Cutler 2010; Cutler, Hauffler, and Porter 1999; Fuchs and Kalfagianni 2010; Hall and Biersteker 2002; Graz and Hartmann 2010; Peters et al. 2009).

This dissertation understands private authority as the capacity of corporate actors "to create rules and standards that other actors adopt" (Green 2013:29). Intellectual property actors are not producing rules to govern their own conduct. Instead, they are seeking to impose their privately drafted rules and standards to govern how macro-intermediaries regulate third-party infringement. Authority is a fluid, rather slippery concept, which can "denote both the power and right to rule" (Peters, Förster, and Koechlin 2009:502). Scholars describe authority in relation to private actors in various ways. It can be understood as inducing "deference" among the governed (Avant, Finnemore, and Sell 2010:9-10), motivating behavioural change (Black 2008:148) or involving "decision-making power" (Cutler, Hauffler, and Porter 1999). It can also refer to "authorship" of policies, practices, rules and norms (Hall and Biersteker 2002:4), or "a presumptive right to speak and act" (Abrahamsen and William 2007:240). Common among these definitions is the capacity to persuade others to accept and follow certain ideas.

Underlying authority is some form of legitimacy, which gives actors the “right” to exert authority (Hall and Biersteker 2002:4; see also Black 2008:144). Actors who lack legitimacy, such as mercenaries or warlords, may have the capacity to enforce obedience through threats or use of force but not the right to do so. Legitimacy involves the perception by those subject to authority that “the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions” (Suchman 1995:574). Authority and legitimacy are complex, inter-dependent and socially constructed concepts. There are also highly malleable constructs (Fuchs and Kalfagianni 2010; Suchman 1995). This means that private actors that seek to govern others can seek authority and legitimacy from diverse sources and can work to construct (or manipulate) narratives that will convince others to accept their claims as legitimate.

Private actors commonly draw authority from two sources: their material resources (structural authority) and their capacity to shape meanings (discursive authority) (Fuchs 2007; Fuchs and Kalfagianni 2010; Koch 2011; Peters et al. 2009; Wilks 2013). Structural authority, which is based upon Susan Strange’s (1997) notions of structural power, traditionally refers to the capacity of transnational corporations to “punish and reward” countries’ policy choices by threatening to or actually relocating investment and jobs (Fuchs and Kalfagianni 2010:13; see Fuchs 2005). It also encompasses corporations’ capacity to make and implement rules to govern their own operations or impose their rules on others, particularly through control over supply chains (Fuchs and Kalfagianni 2010). Structural power represents the capacity of certain transnational corporate actors to control access to or the use of certain markets or services.

Private actors often use discursive authority to enhance or amplify their structural authority (Fuchs 2005). Discursive authority, which understands the importance of norms and ideas to power, here refers to corporate actors’ ability to frame and shape the meaning of ideas, issues or policies in a way that affects public policy setting or decision-making (Fuchs 2007; Fuchs and Clapp 2009). Discursive authority can incorporate other types of authority in which actors shape meanings, such as moral authority and technical authority (Avant, Finnemore, and Sell 2010; Biersteker and Hall 2002; Cutler 2010; Drahos 2010;

Suchman 1995). Actors may invoke moral authority by drawing upon widely accepted principles or values (Avant, Finnemore, and Sell 2010:13) or claiming “normative superiority” on particular issues (Biersteker and Hall 2002:215). They may also claim technical authority by arguing that they have specialised knowledge, technical skills, experience or information that qualifies them to provide expert, scientific, or objective advice (Avant, Finnemore, and Sell 2010; Cutler, Hauffler, and Porter 1999; Cutler 2010; Drahos 2010; Koch 2011).

ii) ***Seeking Legitimacy for Private Authority***

Laying claim to authority is only part of the equation: actors must also seek some sort of legitimacy for their claim by drawing upon certain values, norms and ideas. For instance, actors may claim moral superiority on an issue to justify their right to govern (Suchman 1995).⁶⁰ They may contend that certain individuals or institutions have particular values that would make them appropriate candidates for regulators (Suchman 1995). Environmental groups, for instance, often claim moral legitimacy by arguing that they are serving the public interest when they report corporations for pollution. Those who would be governed may take a pragmatic approach and accept regulators because it is their interests to do so (Suchman 1995). Companies that wish to become suppliers to Apple must abide by its environmental and labour conditions or risk losing contracts (Dedrick, Kraemer, and Linden 2009).

Actors do not simply “extract” legitimacy from the social milieu in a “feat of cultural strip mining” (Suchman 1995:576). There must be some interaction among the would-be governors and governed that includes an element of public recognition or acknowledgement. Actors may make different claims to various “legitimacy communities” because a narrative that resonates in one community may ring hollow in another (Black 2009:21). They may also construct, shape and even manipulate legitimacy claims to serve certain goals (Fuchs and Kalfagianni 2010; Suchman 1995). While social interaction is important, how the recognition of legitimacy occurs and by whom are matters of debate (e.g., Avant, Finnemore, and Sell 2010; Cutler, Hauffler, and Porter 1999; Hall and

⁶⁰ Claims of moral legitimacy do not mean that those seeking to govern are lacking in self-interest (Suchman 1995).

Biersteker 2002; Peters et al. 2009). Some scholars contend that this recognition must involve a “larger public” that often includes states (Hall and Biersteker 2002:4-5). Others argue that private actors may only require “passive acquiescence” (Suchman 1995:575), “tacit and informal” approval (Avant, Finnemore, and Sell 2010:10), or, more calculatingly, apathy (Hall and Biersteker 2002:5). The general public may be largely unaware of the authority, as governments may grant “silent permission” (Cutler 2002: 35) or the authority may even manifest “below the radar of government regulators” (Djelic and Sahlin-Andersson 2006:390 cited in Büthe 2010:21).

iii) *Limitations of Private Authority*

The notion of private authority is conceptually useful as it provides a language and framework to think about how private actors may seek to exert control through regulation and the ways in which these actors interact with and rely upon the state. Corporate actors can attempt to persuade other private actors to conform to their rules by employing campaigns of pressure, shaming, litigating, and granting and withholding business deals. If those actors resist, appeals to the state for assistance are the last possible avenue. Rights holders successfully solicited assistance from governments in the United States and United Kingdom, and from the European Commission, which intervened and employed varying degrees of coercion to compel macro-intermediaries to act as enforcers on behalf of rights holders. In granting rights holders’ requests, these governments legitimised rights holders’ demands that macro-intermediaries work as gatekeepers to regulate online infringement on behalf of rights holders. More broadly, by supporting rights holders’ requests, the governments also legitimised rights holders’ vigorous online enforcement strategies described in chapter 1.

Private actors’ capacity for authority is also constrained because those who are governed may protest or resist any attempts to expand or amend the mandate to govern (Avant, Finnemore, and Sell 2010:11). Private authority, like that of governments, can be fragile. Non-state actors seeking authority can lose credibility or have rivals contest their legitimacy, and the state may weaken or revoke its recognition of the regulatory arrangement (Avant, Finnemore, and

Sell 2010; Hall and Biersteker 2002). Private regimes can fall apart and be replaced by another private regime, or the state can step in and take over governance. Compliance with private authority does not necessarily indicate that the governed acknowledge the legitimacy of the authority. The “reluctant governed,” for example, may fear sanctions for non-compliance or lack the resources or spirit to resist (Avant, Finnemore, and Sell 2010:360).

iv) *Role of the State in the Private Anti-Counterfeiting Regime*

Drawing upon the preceding discussions of private authority, corporate actors have varying degrees of reliance upon the state for their regulatory regimes, depending upon the regime’s participants, rules and overall goals. Where there is relative agreement among participants in relation to the regime or suitable incentives offered (or penalties credibly threatened), there may be little, if any, state involvement. This is the case, for example, when powerful multinational companies, such as Wal-Mart or Apple, require all their suppliers to adhere to certain environmental, labour or quality-assurance standards (Vandenbergh 2007). Wal-Mart and Apple have considerable authority to offer inducements for companies to follow or impose penalties for the violation of their policies. Companies found in violation of these rules can be terminated as preferred suppliers, essentially losing their license “to participate in the global market” (Fuchs and Kalfagianni 2010:3). These regimes require little direct involvement or interaction with the state, as corporations set and enforce rules through their supply chains.⁶¹ Rights holders, in contrast, lack the capacity to offer sufficient incentives or penalties to persuade macro-intermediaries to adopt wholesale changes to their regulatory practices. As a result, the private anti-counterfeiting regime is reliant upon the state.

What explains the state interest in facilitating some private regulatory arrangements and not others? Corporate actors must craft a compelling narrative to the state to solicit its assistance in creating or facilitating private regulation. These corporate actors have varying degrees of structural and

⁶¹ Although these corporations may not interact with the state, they are indirectly reliant upon the state as they use legal contracts to enforce rules and standards that they impose upon their suppliers.

discursive authority that they draw upon to add gravitas to their appeals. Some requests for state assistance resonant more with the state or align more closely with its interests than others. Interactions among private actors and the state that shape non-state governance efforts are “reflexive” (Picciotto 2011:11) and “synergetic” (Peters, Förster, and Koechlin 2009:504). This means that the state and corporate actors have mutually constituted interests (Braithwaite and Drahos 2000; Peters et al. 2009). The state shapes market interests and corporate actors inform the state’s policy preferences, depending, of course, on corporate actors’ authority and the persuasiveness of their claims (Underhill 2003). Private authority should therefore be understood as partially derived from the state (Büthe 2010; Hall and Biersteker 2002; Sassen 2002).

Corporate actors that can successfully lobby the state to shape particular policies or regulatory arrangements demonstrate their relative influence over other actors competing for attention on the same topic. Intellectual property is an issue of significant economic importance to the United States and the European Union, as discussed in chapter 1. Rights holders and trade associations, particularly from the United States, have crafted a narrative that links continued U.S. economic hegemony to strong protection for intellectual property rights and also emphasises the problem of counterfeiting as a threat to public safety and economic integrity (Halbert 1997; Sell 2003). In contrast, macro-intermediaries, which are also powerful, multi-billion-dollar corporations, could not effectively challenge intellectual property actors’ simple but persuasive message that intellectual property requires ever-increasing protection. As these governments and intellectual property actors become partners, their alliance legitimises corporate anti-counterfeiting efforts. The rules, standards and norms set by rights holders in the private enforcement agreements become more authoritative with the power of the state in the background.

Not all private actors have the same capacity to shape states’ policies. Equally, states have varying capabilities to create transnational regulatory arrangements and compel the involvement of wealthy, multinational corporations. Government agencies from the United States, the United Kingdom, and the European Commission compelled macro-intermediaries to adopt private enforcement

agreements by threatening, to varying degrees, legislation or legal action. These threats were credible as the governments had the resources and, more importantly, the will and economic interest to make good on their promises. These countries collectively comprise a massive, highly lucrative market, which gives macro-intermediaries a strong incentive to comply with state demands. If rights holders headquartered in Cambodia or Mexico, for example, were to make similar demands of their governments, it would be difficult to imagine how those governments could compel Google to agree.

V) Techno-Regulation

The concept of private authority usefully explains the conditions in which corporate actors can persuade others to accept their rules and when they fail. It also accounts for state intervention into private regulatory regimes. Ideas about regimes and private authority, however, do not address regulation using technology or some of the distinctive regulatory dynamics in the online environment. To consider these ideas, this chapter employs techno-regulation, which refers to the employment of technology to shape human behaviour (Leenes 2011:149). Paired with the concept of private authority, techno-regulation enables researchers to unpack corporate-state dynamics in relation to the construction of enforcement strategies against online infringement, specifically intermediary-facilitated regulation. Used in this manner, techno-regulation nicely complements private authority as the former explains how actors employ technology as a regulatory instrument in ways that are influenced by corporate-state interactions.

i) *From Cyber-libertarianism to Techno-Regulation*

Techno-regulation provides useful insights into the mutual shaping of technology and politics in relation to the regulation of online behaviour and ways in which state and corporate actors use technology to control certain types of behaviour. To understand technology-facilitated regulation on the Internet, it is important to sketch a brief overview of the conceptual shift from cyber-libertarianism to regulation through technology. Cyber-libertarianism, which characterised much of the early period of the Internet from the 1970s to the

1990s, argues that the Internet is a novel, ungovernable space that operates beyond the reach of nation states (Johnston and Post 1996).⁶² During this early period of the Internet, governance was largely left to the group of academics, engineers and dedicated users that created its various applications and networks (Brown and Ziewitz 2013; Hofmann 2010). The U.S. government, particularly its Department of Defense but also its academic institutions, played a key role in the development of the Internet but was not involved in its regulation, at least in the early years.⁶³ Scholars of Internet governance describe the U.S. government during this period as “passive” (Goldsmith and Wu 2006:32) and an “absentee custodian” (McConnell 1997:72 in Hofmann 2010:10). In the absence of state pressure and reflecting the “overall messiness” of the Internet’s development, governance arrangements “emerged in the shadow or the absence of law” (Brown and Ziewitz 2011:28-29). Regulatory efforts during this time emerged tended to be self-regulatory, created by early users and Internet engineers, and undertaken in loose, informal networks (Hofmann 2010; Zittrain 2008).

In contrast to the cyber-libertarians, cyber-paternalists argue that, far from being ungovernable, the Internet is highly amenable to regulation (Lessig 1999; Reidenberg 1998; Wu and Goldsmith 2006). Lawrence Lessig, an influential scholar on Internet governance, argues, “cyberspace will be the most regulable space humans have ever known” (2006:32). Cyber law scholars focus on the regulatory potential of the technical environment of the Internet: the architecture of computer hardware and software (Brown and Marsden 2013). Rules can be set outside laws and instead be encoded within the Internet’s technical architecture.⁶⁴ Thus, state or non-state actors could introduce rules or standards into the code of software applications that would shape—or even prevent—

⁶² John Perry Barlow, a former lyricist for the Grateful Dead, penned a stirring founding document for cyberspace inhabitants in 1996. It begins with the oft-quoted lines: “Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather” (Barlow 1996).

⁶³ For a detailed history of the development of the Internet from the early 1960s and the roles played by U.S. and European researchers, see Brown and Ziewitz (2013).

⁶⁴ Lessig terms this idea “Code is law” (Lessig 1999) and his ideas have been critiqued, often harshly. For example, Mayer-Schönberger (2008) contends that Lessig misunderstands the dynamism of the relationship of technology and society, as emphasised by science and technology studies, and instead adopts a one-dimensional relationship.

certain types of online activities or behaviour.⁶⁵ The growing area of cyber law explains how online behaviour is controlled in ways other than publicly set laws and explores ways in which technology shapes human behaviour and, in turn, society shapes technology (Brown and Marsden 2013; Zittrain 2008).

ii) ***Regulation in the Online Environment***

Following the laissez-faire approach to Internet regulation in the 1990s, in the early 2000s many countries increased their online regulatory presence considerably following the dot-com bust between 2000 and 2001 and the terrorist attacks in the United States in 2001 (Brown and Marsden 2013). Governments were concerned about various types of old and new crimes ranging from fraud, child pornography and viruses to terrorism. The online environment brings both distinct challenges and advantages to states and private actors wanting to address unwanted activity. Its disadvantages are well known. Wrongdoers can attempt to remain anonymous and locate themselves in jurisdictions infamous for their governments' reluctance or inability to address online offences (Murray 2011). They can also strategically choose Internet service providers, like web hosts or payment providers, which may turn a blind eye to illicit activities.

The advantages of online regulation, however, are likely less widely known, particularly when they involve powerful intermediaries. The U.S. government has partnered with macro-intermediaries since the early 2000s to crack down on child pornography sites (Laidlaw 2012) or sites that illicitly sell tobacco or allow gambling (MacCarthy 2010). When rights holders struck private enforcement agreements with Internet firms and payment providers, it marked the first time that corporate actors were able to direct macro-intermediaries and take advantage of their global regulatory capacity that was previously only available to powerful global actors like the United States. By working with these macro-intermediaries, rights holders are able to dramatically expand their online

⁶⁵ For example, following a consumer backlash against Microsoft, in June 2013 the company removed restrictions that required gamers, even those of offline games, to connect to the Internet daily to authenticate their systems (Stuart 2013).

regulatory strategies and engage novel forms of technologically facilitated enforcement.

iii) ***Regulation Through Technology***

Technology, particularly information and communications, and Internet technologies, enables private actors to expand their rule making and enforcement activities transnationally, particularly with the development of new technologies related to information and communications technologies and the Internet (Brown and Marsden 2013; Marsden 2011). As neither the non-state governance nor regulatory studies literatures focus on explaining regulation through technology, this dissertation looks to the law and technology literature.

Techno-regulation explains how corporate actors use technology to set and enforce rules. The concept has its roots in science and technology studies, a field of research prominently associated with Bruno Latour (2005). This dissertation recognises important insights from science and technology studies, particularly that science, technology, and society are mutually dependent upon and shape each other.⁶⁶ Technology, in this perspective, is never neutral but, at least partly, is socially constructed (Brey 2005; Franklin 1995; Leenes 2011). This means that technology neither solely determines human behaviour, nor is it a passive social construct (Brey 2005; Bendrath and Meuller 2011). Technology is both real and constructed: it shapes and influences behaviour, beliefs and practices and is imbued with norms, concepts and cultural values (Brey 2005; Disco 2005; Franklin 1995). Technology also constrains behaviour in certain ways. Some constraints are physical, while others are socially constructed or combine physical and social factors (Brey 2005:80). Those who design the multitude of technologies that we use in our daily lives intend them to facilitate certain types of use, and, inadvertently or deliberately, discourage or prevent others (Hildebrandt 2008; Murray 2011).

⁶⁶ The ways in which these elements affect one another and with what results are matters of keen debate within science and technology studies. For an analysis of varying deterministic and constructivist perspectives, see Brey (2005).

The recognition that products are designed in ways to shape and constrain how individuals use them is not new.⁶⁷ Fast-food restaurants, like Subway and McDonalds, intentionally choose hard, uncomfortable chairs to encourage diners to scarf down their meals and depart, thereby ensuring a rapid turnover of customers (Robson 1999). Digital architecture can also shape and manipulate how individuals access and use technologies online (Bendrath and Mueller 2011; Katyal 2003). Studies examining how technology facilitates and inhibits behaviour take on greater importance as individuals increasingly rely upon the Internet in their work, social and cultural spheres of life. Techno-regulation explicitly recognises that technologies, like Google's search processes, embody certain norms and ideas, often in ways hidden to users (Hildebrandt 2008; Murray 2011). For example, Google, with its dominant market share, can shape what information individuals access and thereby "shape positions, concepts and ideas" (Elkin-Koren 2001:186).

Technologies can shape behaviour in ways that force compliance and facilitate compliance (Hildebrandt 2008; Koop 2008). Individuals may have no option but to comply with certain rules or norms if the technology prohibits certain behaviour. For example, many ATMs require users to withdraw their card before their cash is issued (Brey 2005:70). Another example is the encoding of digital locks onto the electronic files of books, music and movies to prevent users from copying or modifying the protected content.⁶⁸ This constraint is weaker as tech-savvy individuals can bypass it but others are forced comply with the rules set by the locks. Other constraints promote compliance or discourage non-compliance by using monitoring technologies (Brownsword 2008). These can include policies that require users to register with their name and email address (like Facebook, Twitter or eBay). Monitoring technologies also refer to surveillance mechanisms to track and control transactions across Visa's network or identify breaches of Google's advertisement policies.⁶⁹

⁶⁷ Design-based regulation is not confined to cyberspace but includes efforts to design the physical environment to reduce crime through better lighting or altered population traffic flows (e.g., Clarke 1997; Katyal 2002).

⁶⁸ These digital locks, termed digital rights management (DRM), can be broken by individuals knowledgeable enough to create or use software to remove the codes prohibiting copying. Breaking DRMs, however, is prohibited in many jurisdictions as individuals may do so to violate copyright (Haggart 2014).

⁶⁹ As will be discussed in chapters 4 and 5, Visa and Google have sophisticated surveillance and enforcement programs to detect, monitor and remove users that violate their policies on intellectual property rights.

iv) *The Rise of Macro-intermediaries*

The concept of techno-regulation enables one to explore how technology shapes actors' regulatory strategies and techniques. As Bendorath and Mueller (2011:1156) note in their study of the regulation of digital-copyright infringement, by employing such a framework "one can see technology structuring the politics, and politics constraining and channeling the technology."⁷⁰ The use of new technologies is shaped by existing laws and regulations, as well as by state and non-state actors promoting certain policy goals (Mueller, Kuehn, and Santoso 2012:350). The roles Internet intermediaries can (and should) assume are the subject of lively debate among scholars, policymakers and industry actors (Kohl 2013; McIntyre and Scott). Those favouring intermediary-based regulation contend that intermediaries are often best suited to identify and control wrongdoers (e.g., Lichtman and Posner 2004; Mann and Belzley 2005). Some scholars argue intermediaries should not only be encouraged to assume a greater regulatory role to prevent "harmful transactions" but should also be threatened with formal sanctions if necessary to encourage their gatekeeping duties (Lichtman and Posner 2004).

Despite the breadth of different types of intermediaries, much of the literature in this area focuses on the role of Internet service providers, web hosts, and search engines (see Barzilai-Nahon 2006; Bracha and Pasquale 2008; Elkin-Koren 2001; Laidlaw 2010). As payment providers and domain registrars are relatively new to the world of gatekeeping, it is unsurprising that they have generated less scholarly attention (though exceptions include MacCarthy 2010; Lindenbaum and Ewan 2012; Mellyn 2010). Further, macro-intermediaries' gatekeeping activities on behalf of non-state actors are critically under-explored (see Laidlaw 2012). As the use of macro-intermediaries by non-state actors is growing, particularly with rights holders' private agreements, it is critical to fill this gap in scholarship. This area of study is particularly important as macro-intermediaries can control the flow of information and shape online behaviour in

⁷⁰ Bendorath and Mueller (2011) examined how Internet intermediaries undertake deep-packet inspections, which refers to their scanning and examining aspects of Internet traffic and determining whether any will be blocked or redirected. This practice is employed against a variety of problems, including child pornography and unauthorised downloading.

a manner that than their physical-world counterparts cannot match. Further, they can do so outside judicial processes and in relative secrecy.

Macro-intermediaries can be valuable gatekeepers because their vast, technologically sophisticated surveillance and enforcement programs. By policing problems globally on behalf of states and corporate actors, macro-intermediaries challenge concepts of jurisdiction and territorially based rules, and illustrate the transformed “architecture” of security, particularly in the online environment (Bowling and Sheptycki 2012; Sheptycki 2007). Within this architecture, corporate actors can capitalise upon new technologies, such as automated tools, to serve growing demands for global online enforcement (Bowling and Sheptycki 2012; O'Reilly 2011; Sheptycki 2000).

Automated enforcement processes are often portrayed as objective, accurate and highly targeted. However, by recognizing that the software underlying these enforcement measures is based on certain ideas and norms, researchers can critically interrogate these claims. Automated processes are neither neutral nor are the macro-intermediaries impartial (for an analysis of Google's claims of impartiality, see Kohl 2013). Examining technology entails not only studying its “manifest and desired properties” but also its “intended and unintended side-effects, dangers, and risks” (Disco 2005:38). Given the size and critical importance of macro-intermediaries' operations, these side effects can be significant and wide ranging.⁷¹ For example, macro-intermediaries routinely inaccurately identify and target legitimate content and transactions, as will be examined in chapters 4 to 6.

Pat O'Malley observes in his article on automated regulation in relation to traffic tickets that individuals can be “policed, judged and sanctioned” through their “electronic trace” without any human interaction (2010:795). Automated traffic enforcement, however, relates to a breach in public laws and offers the possibility of challenge or appeal before a human, although the system is designed to minimise such interactions (O'Malley 2010). Macro-intermediaries,

⁷¹ McIntyre and Scott (2008) examine the considerable procedural and normative challenges, including censorship of legitimate content, resulting from Internet service providers' filtering of webpages to block access to child pornography sites.

in contrast, institute automated regulatory processes globally and offer limited channels for appeal. Their regulatory activities demonstrate that privately set rules, standards and norms can be as powerful as laws in the online environment but often much less transparent.

VI) The Private Anti-Counterfeiting Regime

Drawing together concepts of regimes, private authority and macro-intermediaries enables this dissertation to understand how corporate actors form private regulatory arrangements and examine the circumstances under which these actors turn to the state for assistance. The private enforcement agreements examined in this research are popularly referred to as “voluntary initiatives.” They are, however, fundamentally coercive as the state employed various means to compel macro-intermediaries to join them. The terms “informal” and “non-binding,” rather than “voluntary” better captures the regime’s use of non-binding enforcement agreements as these terms can include coercive pressure. Private regulation in this case does not mean that the state is absent from the regulatory process, but that corporate actors play important roles in creating and enforcing rules, and in persuading the state to support the regulatory regime. Despite the state’s key role in this regime, it largely acts from the shadows as it quietly shapes regulatory activities.

i) Corporate Online Anti-Counterfeiting Efforts

The private anti-counterfeiting regime is relatively young, having emerged in the mid-2000s to target the online distribution of counterfeit goods. Some of its rights holders, trade associations and macro-intermediaries, particularly Google, have been active in online enforcement efforts since the late 1990s in efforts targeting digital-copyright infringement (Weatherall 2012; Zittrain 2006). The actors comprising the regime—a broad coalition of trade associations, macro-intermediaries, government agencies, and rights holders from a wide array of industry sectors—are loosely inter-connected. Government agencies from the United States and the United Kingdom, as well as the European Commission play key roles in constructing and endorsing the regime. Some corporate actors share common membership in trade associations, like the International Anti-

Counterfeiting Coalition. In comparison with the tightly knit, highly coordinated copyright industries, those representing the interests of trademark owners in anti-counterfeiting efforts describe themselves as “a bit of a hodgepodge.”⁷² This is because the copyright industries, which comprise the music, movie, book, and software sectors, are dominated by a handful of large firms and prominent trade associations like the Motion Picture Association of America. Counterfeiting affects a broad range of industries and makes it difficult for rights holders to adopt a coordinated or standardised approach. Corporate online anti-counterfeiting efforts involve rights holders from industry sectors ranging from pharmaceuticals, sporting goods, and alcohol to apparel, consumer electronics and industrial electrical products.

The regime’s scope is global, both in terms of the reach of its macro-intermediaries and the scope of their rules through internal terms-of-use agreements. The regime is rooted in the United States, as all of the macro-intermediaries and many intellectual property actors are headquartered there, and Europe, where state and corporate actors have been active in creating private enforcement agreements. The regime’s regulatory practices are diffusing outward as other countries, particularly China, are adopting similar private governance mechanisms to regulate online infringement. The spatial pattern of this regime aligns with ideas from regulatory capitalism, which describes regulatory arrangements that are “shaped in North America and Europe [and] are increasingly internationalized and projected globally” (Levi-Faur 2005:13). The regime’s distribution also accords with non-state governance scholars who argue that cases of transnational private regulation often illustrate a “clear differentiation in North-South relations and centre-periphery dynamics” (Graz and Nölke 2008:10).

By drawing together the concepts of regimes, private authority, and techno-regulation, this dissertation employs a theoretical framework that is sensitive to the role of the state in private regulation. The dissertation uses regimes to trace and critically examine the principal corporate and state actors responsible for creating eight private enforcement agreements that cover a wide range of Internet services. Paired with the concept of regimes, private authority enables

⁷² Interview with Siân Croxon, Partner, DLA Piper, 14 September 2012, London.

the researcher to explore how corporate actors acquire and wield private authority over other private parties and, importantly, the limitations to that authority. Where private authority is constrained, the dissertation's analytical focus examines corporate-state dynamics and the varying ways certain corporate interests align with those of the state. The state in this research retains its capacity to direct, shape and compel regulatory efforts that overlap with its interests. Finally, the dissertation employs techno-regulation to explain how corporations use technology as a regulatory instrument that is shaped by particular corporate-state interactions.

The next chapter establishes the specific historical and legal context in which the private enforcement agreements emerged, and then introduces the main state and corporate actors involved in the creating these agreements. Chapters 4 to 6 apply this theoretical framework to examine these private agreements in the payment, advertising, search, domain name, and marketplace sectors.

Chapter 3: Macro-Intermediaries and Informal Private Regulation on the Internet

Macro-intermediaries' transformation into gatekeepers for large U.S. and European rights holders is a monumental achievement. The eight private enforcement agreements studied in this dissertation, established between 2010 and 2013, mark the first time that rights holders secured macro-intermediaries' voluntary cooperation to address online infringement. With these agreements, intellectual property actors are able to tap into a global regulatory capacity, which was previously only available to powerful countries like the United States. Beginning in the mid-2000s, for example, state and federal authorities in the United States established voluntary enforcement agreements with payment macro-intermediaries, including Visa and MasterCard, to stop payments to websites selling child pornography (MacCarthy 2010).⁷³

This chapter establishes the context in which the private anti-counterfeiting regulatory regime emerged. It traces the policymaking influence of U.S. rights holders and their trade associations back to the early 1970s when the United States first began to lead the charge to strengthen intellectual property rights globally against what rights holders claimed was a tidal wave of counterfeit goods and copyright-infringing content (see Sell 2003). In a span of two decades—from the mid-1970s to mid-1990s—rights holders and their trade associations convinced the United States to prioritise the protection of intellectual property domestically and in its international trade agreements (Drahos and Braithwaite 2002). As evidence of their significant private authority, these actors also played a key role in establishing tough global standards for the protection of intellectual property in 1995 (Sell 2003).⁷⁴ Many of the intellectual property actors who were involved in these early standard-setting efforts are also involved in the private anti-counterfeiting regime.

⁷³ These so-called voluntary agreements between U.S. payment providers and federal and state authorities in the United States also stopped payments sites unlawfully distributing tobacco, as is briefly discussed in chapter 4 (MacCarthy 2010). These agreements are a forerunner to the non-legally binding agreements with macro-intermediaries in relation to online infringement.

⁷⁴ As will be discussed later in this chapter, this refers to the 1995 TRIPS agreement (Trade-Related Aspects of Intellectual Property Rights).

While rights holders and trade associations made significant headway in setting standards internationally, they found enforcement more difficult, particularly with the development of e-commerce in the early 2000s. Rights holders argued that online infringement is too complex and prevalent for rights holders to address alone and that Internet intermediaries should assume greater responsibility for infringement on their systems. In response to lobbying from rights holders, the U.S. Congress introduced four intellectual property bills between 2010 and 2012, including the ill-fated *Stop Online Piracy Act* (SOPA).⁷⁵ These bills adopt a techno-regulatory approach: they propose varying types of Internet intermediaries should become regulators because they provide essential Internet services and have technologically sophisticated systems to detect and police infringement. During the period that the U.S. Congress was considering these bills, the U.S. government was meeting quietly with macro-intermediaries to establish the private enforcement agreements examined in this dissertation and create a global private regulatory regime to address online infringement.

To cover this history and highlight the specific legal and technological developments that shaped the private anti-counterfeiting regulatory regime, this chapter proceeds as follows. First, it describes the period from the mid-1970s to mid-1990s in which rights holders and trade associations successfully established intellectual property as a priority within the United States and helped set standards internationally governing its protection. In the next part, it explores early online enforcement efforts against infringement from the late 1990s to the early 2000s. The third part, which focuses on events from 2009 until 2012, describes the four U.S. intellectual property bills and the protests against the SOPA and *Protect Intellectual Property Act* (PIPA). Then, in the fourth part, the chapter explores how intellectual property actors and macro-intermediaries frame the issue of the regulation of online infringement in their competing efforts to influence the U.S. government's policymaking in this area. The fifth part describes the creation of the private enforcement agreements in the United States and the European Union and then offers a brief conclusion.

⁷⁵ The other three bills are the Combating Online Counterfeits and Infringement Act (COICA), the Protect Intellectual Property Act (PIPA), and the *Online Protection and Enforcement of Digital Trade Act* (OPEN Act).

I) Setting Standards Globally to Protect Intellectual Property Rights

While the United States is now the global champion for the protection of intellectual property rights, it was not always so. It has benefited economically from centuries of disregarding intellectual property laws, as have other industrialised economies (Drahos and Braithwaite 2002; Halbert 1997).⁷⁶ By the 1970s, however, there were growing concerns in the United States that other countries would make economic gains that would undermine its position as an economic powerhouse. At that time, U.S. policymakers were preoccupied with the possible loss of U.S. competitiveness, growing trade deficits, foreign debt, and the rise of manufacturing in Asia, particularly in Japan (Drahos and Braithwaite 2002; Halbert 1997). Fears that these factors were endangering U.S. economic hegemony grew. Key U.S. corporations like IBM, Pfizer and Microsoft loudly complained that infringement of their intellectual property rights by Asian countries threatened their businesses (Drahos 1995). These corporations petitioned the U.S. government for assistance with a nationalistic narrative that compellingly linked strengthened intellectual property with a strong U.S. economy (Drahos 1995). In this narrative, concerns over unfair trading practices gave the United States a clear Asian “villain” and improbably transformed wealthy U.S. industries into “victims” (Halbert 1997).

The U.S. government seized upon this convenient and reassuringly simple explanation for its complex fiscal woes. Thus, the U.S. government, based upon rights holders’ convincing narrative, conceptually coupled intellectual property with international trade (Halbert 1997). The link between intellectual property and economic growth, therefore, is socially constructed and reflects the perceptions and interests of the U.S. government and certain prominent corporate interests, particularly those in the pharmaceutical, software, and movie industries, as will be discussed later in this chapter (Sell 2003). By establishing this link, the United States exploited its crucial advantage in international trade – leverage (Drahos 1995). The U.S. government uses its

⁷⁶ The United States has long copied ideas and practices from European countries “who copied from each other and—something they rarely acknowledge—from the Middle and Far East” (Dutfield 2006:2).

massive economic market as leverage to pressure other countries: it grants countries access to that market or withdraws privileges from countries in relation to its market (Braithwaite and Drahos 2000; Drahos and Braithwaite 2002).

i) ***Trade Associations Shaping Public Policy***

The United States, urged on by key industry actors, sought to use its economic leverage to strengthen intellectual property rights globally in two nearly concurrent efforts between the mid-1970s and mid-1990s. One avenue was to introduce intellectual property into a multilateral agreement governing international trade, the *General Agreement on Tariffs and Trade* (GATT). The second was to amend the protection of intellectual property through the World Intellectual Property Organization (WIPO), the international body that governs agreements on trademarks, copyright and patents. The road to strengthen intellectual property rights globally would prove complex and arduous but would ultimately lead to victory two decades later with the 1994 *Agreement on Trade-Related Aspects of Intellectual Property* (TRIPS).⁷⁷

TRIPS, a multilateral agreement, fundamentally reshaped intellectual property rights in favour of industrialised countries that benefit most from strengthened intellectual property, particularly the United States, as well as Japan and some countries within the European Union (Sell 2003). The agreement required member states to criminalise trademark and copyright infringement and to adopt both civil and criminal penalties and, in doing so, became the first multilateral agreement to incorporate enforcement mechanisms for intellectual property (Sell 2003). TRIPS was part of the Marrakesh Agreement that created the World Trade Organisation (WTO), which means that any country wanting to become a member of the WTO had to implement TRIPS (Matthews 2002).

The intellectual property actors involved in efforts to revise the GATT and WIPO represented the biggest corporations that own copyright, patents and trademarks. In terms of copyright, companies like IBM were concerned about

⁷⁷TRIPS, opened for signature 15 April 1994 (entered into force 1 January 1995).

infringement of their software programs, as was their industry association, the Business Software Alliance (BSA). The music and movie industries were likewise troubled by the mass production of unauthorised versions of their products. The high-profile Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA) represented copyright owners. Global pharmaceutical companies, particularly Pfizer, argued that insufficient protection of their valuable patents from India and Brazil threatened their innovations. Former-president of Pfizer Bruce MacTaggart referred to this practice as “Stealing from the Mind” in his highly influential 1982 *New York Times* opinion article (Drahos and Braithwaite 2002). Alongside these groups, the International Anti-Counterfeiting Coalition (IACC) advocated on behalf of a broad array of industries concerned about protecting their trademarks, copyright and patents. Its corporate members include some of the world’s biggest multinational corporations, ranging from Calvin Klein, Nike and Pfizer to Phillip Morris, Sony and Walt Disney.⁷⁸ Several of these actors, particularly Nike and the IACC, are active in the private anti-counterfeiting regime examined in this dissertation, which shows that the online regulatory effort is a continuation of standard-setting that began in the early 1980s.

The trade associations focused on revising the GATT and WIPO collectively represented a powerful constituency of global corporations with the means and intent of shaping public policymaking to protect their intellectual property. Two of the associations had decades of experience advocating on behalf of their members: the MPAA and RIAA were formed in 1922 and 1952 respectively. The others were born out of rights holders’ modern anxiety to protect their intellectual property in the face of rising economies in Asia. The IACC was formed in 1979 with apparel firm Levi Strauss as one of the founding members.

In 1981, the United States created the Advisory Committee for Trade Negotiations (ACTN) to advise the U.S. government on trade policy (Drahos and Braithwaite 2002; Sell 2003). The ACTN is one of multiple advisory committees organised by the Office of the United States Trade Representative

⁷⁸ For a full list of the IACC’s member organizations, see <http://www.iacc.org/member-companies.html>.

(USTR) with the purpose of providing it with policy advice.⁷⁹ The ACTN illustrates the mutually inter-dependent relationships possible between state and non-state actors when their interests align, as explained by regime theory (see Avant, Finnemore, and Sell 2010). The ACTN formed a powerful Intellectual Property Committee (IPC). Members of the IPC were a small group of executives from major U.S. industries, which included Pfizer, IBM, General Electric, DuPont, Warner Communications, General Motors, and Johnson and Johnson (Matthews 2002). Through the IPC, these actors had the authority, legitimised by the U.S. government, to propose standards and rules at the transnational level to govern the protection of intellectual property.

ii) ***Shaping Policymaking Through Trade Agreements***

As rights holders' lobbying power, which was formalised in the ACTN, shaped U.S. trade policy, industrialised countries, led by the United States, worked to introduce intellectual property into the GATT. The *General Agreement on Tariffs and Trade*, created in 1947, was both a trade agreement and a process for securing international trade agreements.⁸⁰ The GATT took place through a series of negotiations in distinct iterations or "rounds," each of which took months or years to complete. It focused on removing tariffs from industries ranging from textiles and chemicals to steel and agricultural products.⁸¹ The goal of trade associations and industrialised countries was to push for the inclusion of intellectual property into the GATT at the Tokyo Round, which was held from 1973 to 1979.⁸² Negotiations over intellectual property, however, were complex and contentious. Industry actors, particularly the International Anti-Counterfeiting Coalition pushed for continued efforts, which resulted, in 1979, in a draft code offered by the United States and the European Union entitled, the *Agreement on Measures to Discourage the Importation of Counterfeit Goods*

⁷⁹ This committee, which is also referred to as the Advisory Committee for Trade Policy and Negotiations (ACTPN), is organised and administered by the USTR, along with committees on agriculture, trade and the environment and labour. Key functions of the USTR are to develop and coordinate all international trade negotiations for the United States and advise the White House on trade matters.

⁸⁰ The GATT existed until 1994, and then was replaced by the World Trade Organization (WTO) in 1995.

⁸¹ For detailed analyses of GATT negotiations through the Tokyo and Uruguay rounds, see Drahos and Braithwaite (2002), Matthews (2002) and Sell (2003).

⁸² For detailed accounts of efforts to amend the GATT to include intellectual property rights, see Drahos (1995), chapter 6 of Drahos and Braithwaite (2002), and chapter 1 of Matthew (2002).

(Matthews 2002:9). The issue of counterfeit goods gained some traction but countries that opposed its inclusion into the GATT argued that there was a lack of evidence that it was a significant problem (see Matthews 2002). Ultimately, there was a stalemate between industrialised and developing countries.

Rights holders and their trade associations responded to opponents' criticism of a lack of evidence of infringement and by rapidly generating multi-billion-dollar estimates of losses from counterfeiting and copyright infringement (Blakeney 1995). They delivered these estimates to the U.S. Congress, which held hearings on the topic, as well as in informal meetings with government officials (Matthews 2002). In 1984, for example, the Automotive Parts and Accessories Association informed the U.S. House Subcommittee that it lost approximately \$12 billion annually from the counterfeiting of spare parts (Blakeney 1995:4). These estimates, based on industry data and analysis, were difficult to verify but served to convince politicians of the seriousness of the infringement problem (Drahos and Braithwaite 2002). Intellectual property actors also emphasised the narrative of "theft" of American hard work and innovation by "pirates," thus effectively reframing the issue as a moral and economic problem (Halbert 1997). As a result of these efforts, government officials, particularly those in the United States, increasingly considered infringement a serious economic problem. U.S. rights holders' capacity to frame infringement in a way that shaped government policymaking is a demonstration of their considerable private authority, which, as will be discussed later in this chapter, is also evident in the framing of the *Stop Online Piracy Act*.

Alongside efforts to incorporate intellectual property into the GATT, trade associations were also focusing their efforts on the World Intellectual Property Organisation. The organisation, established in 1967 in Geneva, Switzerland, is an agency of the United Nations and coordinates intellectual property policies and information. WIPO is responsible for administering the 1883 *Paris Convention for the Protection of Industrial Property*, which is concerned with the protection of trademarks and patents.⁸³ In the late 1970s, industrialised

⁸³ WIPO also administers the 1891 *Madrid Agreement Concerning the International Registration of Marks* (*Madrid Agreement*) and the *Protocol Relating to the Madrid Agreement*, which came into operation on April 1, 1996. These agreements govern the registration of trademarks internationally. WIPO is also responsible for administering the 1886 *Berne Convention for the*

countries raised alarms of WIPO's "toothlessness" (Blakeney 1995:2) and its apparent inability to counter a growing international trade in copyright-infringing goods and counterfeit products. Trade associations and industrialised countries, again led by the United States, sought to revise the Paris Convention that governs the protection of trademarks and patents.⁸⁴ Signatories to the Paris Convention agree to protect foreign works under domestic laws for intellectual property in the practice termed national treatment. However, critics complained that the Convention lacked strong enforcement provisions and did not have a binding dispute-settlement mechanism for states (Matthews 2002:10). Meetings among signatories between 1980 and 1984 to amend the Paris Convention became polarised because of irreconcilable differences between industrialised and developing countries, much like that of the Tokyo Round at the GATT (Blakeney 1995).⁸⁵ Acknowledging their failure to revise the WIPO conventions, industrialised countries began to move away from the consensus-led style of WIPO, which contributed to diplomatic paralysis, and shift toward bilateral and multilateral trade talks (Drahos 1995).⁸⁶

With the failure of efforts at WIPO, the United States redoubled its efforts targeting the next round of GATT discussions. The Uruguay Round (1986 to 1994) would prove ultimately successful for proponents of intellectual property rights. Industry efforts were key. The Intellectual Property Committee (IPC) developed the U.S. position on protecting intellectual property and then sought to establish consensus with trade associations in Japan and Europe, which became staunch proponents (Sell 2003). These allies then formally supported the IPC's proposals on intellectual property protection⁸⁷ that became the 1994 *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS).

Protection of Literary and Artistic Works, which governs the protection of copyrighted works.

⁸⁴ At the same time, there were also efforts to revise the Berne Convention, also administered by WIPO that governs copyright.

⁸⁵ Developing countries argued that few benefits would flow to them from stronger intellectual property laws. Their views were bolstered by a report by the UN Conference on Trade and Development in 1974 that nationals of five countries owned 84% of patents issued in developing countries (the United States, Germany, France, Switzerland and the United Kingdom) (Matthews 2002:11). The study of trademarks showed that developing countries paid a massively inflated price for pharmaceuticals (Blakeney 1995).

⁸⁶ For example, the United States began negotiations in 1983 with Taiwan over patent protection for chemical compounds and copyright protection (Matthew 2002:16).

⁸⁷ Their proposal in June 1988, the Basic Framework of GATT Provisions on Intellectual Property, which became the basis for TRIPS, advocated minimum standards, national enforcement measures, and a dispute-settlement mechanism (Sell 2003:107).

The Uruguay Round created in 1994 the World Trade Organisation (WTO), which administers TRIPS. All countries that wished to become members of the WTO had to sign onto TRIPS, providing a powerful economic motivation for countries to agree to the agreement.⁸⁸ For the Intellectual Property Committee, this was an incredible effort by twelve executives from U.S.-based corporations who created a law that fundamentally changed the protection and enforcement of intellectual property rights worldwide (Sell 2003).⁸⁹

In two decades, U.S. rights holders and trade associations persuaded the U.S. government to consider intellectual property as an issue integral to its economic dominance and prioritise the protection of intellectual property in its trade deals. This feat alone demonstrates the significant private authority of rights holders and their ability to construct a compelling narrative about the economic importance of intellectual property. It also shows the intertwined economic interests between the U.S. government and its rights holders and trade associations. Further, these intellectual property actors, along with their European counterparts, were key players in establishing global standards to protect intellectual property rights through TRIPS. Intellectual property actors also had powerful new tools of coercion with the Section 301 and Special 301 Processes that are undertaken through the Office of the U.S. Trade Representative (USTR). These processes enable U.S. rights holders, backed by the U.S. government, to push for economic sanctions against countries and non-U.S. companies that rights holders argue do not sufficiently protect intellectual property.

iii) *Shaping Policies through Economic Sanctions*

One of the principal reasons that the United States was successful at the Uruguay Round was its reform of its domestic trade legislation. In 1984, in response to stalemates in international fora and the “increasing cacophony of agitation” (Blakeney 1995:5) from industry, the United States introduced important amendments to Section 301 of its *Trade Act of 1974* (Drahos and

⁸⁸ The incentives for countries to join the WTO include trade liberalization and reduced tariffs in trade with WTO member states (Braithwaite and Drahos 2000).

⁸⁹ For a detailed analysis of the influence of the Intellectual Property Committee in shaping the GATT, see Chapter 5 of Sell (2003) and Chapters 7 and 8 of Drahos and Braithwaite (2002).

Braithwaite 2002). These amendments, drafted in part by industry, allowed the USTR to withdraw trade benefits from or impose duties on a country's goods.⁹⁰ In 1988, again in response to industry pressure, the U.S. further amended the legislation and created the Special 301 process.⁹¹

In the Special 301 process, the USTR evaluates countries as to whether they provide adequate protection of intellectual property or market access for U.S. firms. The USTR's decisions are based on industry complaints and industry-provided data. The Special 301 has three categories of sanctions, which, in order of seriousness, are priority foreign country, priority watch list and watch list.⁹² The United States can then impose varying degrees of pressure on countries with unsatisfactory practices and direct those countries to make specific changes in order to be removed from these lists. As part of the Special 301 process, the USTR publishes an annual survey, called the Special 301 Report that identifies U.S. rights holders' concerns with particular countries. As of 2006, the USTR also publishes a "Notorious Markets List." Entities on this list are both physical marketplaces, like the Silk Market in Beijing, and online businesses, such as the China-based Taobao trading platform. Similar to the process for countries, U.S. rights holders and trade associations submit complaints to the USTR about markets that they contend are have insufficient policies and practices to protect their intellectual property rights.

The Special 301 process is driven by industry.⁹³ Rights holders and trade associations provide resources for the "global surveillance network" required by the initiative, as well as data for estimates on losses (Drahos and Braithwaite 2002:107). The U.S. government legitimises industry efforts and provides the bureaucratic infrastructure that negotiates with, threatens and sanctions targeted countries (Drahos and Braithwaite 2002). For example, when the

⁹⁰ Section 301 does not require that the alleged activity actually violate a trade agreement with the United States in order to be censured (Flynn 2010:5).

⁹¹ The Special 301 process was created in 1988 through an amendment made to *Trade Act of 1974* by the *Omnibus Trade and Competitiveness Act* in 1988.

⁹² A priority foreign country, the most serious category, is one that "has the most onerous and egregious acts" and is not "engaged in good faith negotiations." Countries designated priority watch list are those that do not provide an adequate level of protection or enforcement. Countries on the watch list merited attention to address its intellectual property problems, see the USTR's Special 301 Reports.

⁹³ The USTR also regularly accepts submissions from the public.

USTR placed the Taobao marketplace on its Notorious Markets List in 2008, it directed the Alibaba Group, the owner of Taobao, to work with U.S. rights holders and trade associations to address their concerns (Spelich 2012).⁹⁴ Taobao significantly altered its enforcement policies and practices based on rights holders' complaints (see Spelich 2012), as will be discussed in chapter 6. The Notorious Markets List, and more broadly, the Special 301 process, are backed by the weight of the U.S. government that can credibly threaten trade sanctions against countries like China whose companies U.S. rights holders contend violate their intellectual property rights. The USTR's Special 301 process, in which the state applies coercive pressure on behalf of rights holders, demonstrates the history (since 1988) of state-facilitated regulation in relation to the global protection of intellectual property.

The United States found the Special 301 process useful in stimulating discussions internationally among countries reluctant to adopt new rules to protect intellectual property. When the GATT Uruguay Round discussions stalled between 1986 and 1989, frustrated industry actors used the “new weapons in its arsenal – swift retaliation and a more credible threat” (Sell 2003:108) to target countries, like Brazil, that failed to protect intellectual property in a manner considered adequate by U.S. industry. After an aggressive barrage of 301 complaints, leading developing countries grudgingly admitted in 1989 that they would participate in negotiations on all trade-related aspects of intellectual property rights, which became the TRIPS agreement (Sell 2003).

iv) *Rights Holders' Authority to Set Rules*

To draw together the ideas discussed so far, U.S.-based rights holders and trade associations played a central role in crafting and establishing consensus around the agreement that became TRIPS, along with their industry allies in Europe and Japan (Sell 2003). The most influential corporate actors, who sat on the Intellectual Property Committee, represented the interests of the largest and most powerful pharmaceutical, software, automotive, entertainment and

⁹⁴ The Alibaba marketplace, a business-to-business trading platform also owned by the Alibaba Group, was on the Notorious Markets List from 2008 to 2011.

chemical companies (see Drahos and Braithwaite 2002).⁹⁵ Alongside these actors were the leading trade associations representing the music, movie and software industries, as well as the International Anti-Counterfeiting Coalition, which represents well-known brands like Nike and Levi Strauss.

In addition to their standing as powerful, multi-national corporations, these actors achieved their objectives of stronger trademark laws and enforcement because of several, inter-related factors. They had expertise on the legal and technical aspects of intellectual property at the time when most others around the negotiating table lacked this knowledge, and they provided valuable information on infringement and countries' inadequate intellectual property laws (Sell 2003).⁹⁶ Importantly, they also had a remarkable aptitude to frame intellectual property as an issue integral to trade and a serious, compelling problem at the global level. These actors cannily employed forum shifting by moving among negotiations at WIPO, various GATT meetings and informal meetings with government officials and industry actors to create strategic alliances and pressure reluctant states and actors to embrace intellectual property reform (Drahos and Braithwaite 2002; Matthews 2002). These skills—specialised technical and legal knowledge, the capacity to constructive persuasive frames, and the ability (and resources) to shift among fora—are also evident in the private anti-counterfeiting regime.

Underlying corporate actors' success in crafting agreements at the global level are close, inter-dependent ties between U.S. industry and the U.S. government. In relation to intellectual property, the U.S. government is a non-neutral arbitrator: its interests are aligned toward the ever-increasing protection intellectual property (Drahos and Braithwaite 2002; Sell 2003). The role of major U.S. corporations as trade policy advisors to the United States was institutionalised in the USTR 301 processes and the USTR Advisory Committee for Trade Negotiations. The 301 processes gave industry actors a valuable,

⁹⁵ In 1986, the members of the Intellectual Property Committee, an offshoot of the Advisory Committee for Trade Negotiations were Bristol-Myers, Pfizer, Merck, Monsanto, CBS, Du Pont, General Electric, General Motors, Hewlett-Packard, IBM and Johnson and Johnson (Sell 2003:12).

⁹⁶ Drahos (1995:15) notes that many developing countries had no tradition of intellectual property as understood and practiced by industrialised countries and therefore lacked "consciousness" and "doctrinal knowledge" that accompanied industrialised countries' understanding of intellectual property.

state-sanctioned coercive tool to persuade other countries of the importance of intellectual property and its rightful place at the heart of trade policies. As explained in chapter 2, this is an example of the state legitimising corporate authority and empowering corporate actors (Büthe 2010; Levi-Faur 2013).

The U.S. government was sympathetic to corporate actors' framing of intellectual property as a trade issue because it offered a nationalistic solution to U.S. economic woes (foreign theft) that emphasised a continuation of U.S. economic dominance (see Drahos 1995). The U.S. government and its prominent industries in these trade negotiations represented a state-market condominium (Underhill 2003) as corporate interests shaped the government's policies on intellectual property and the government influenced the development of the market by setting standards through TRIPS. However, TRIPS, is not simply a narrative of U.S. corporate and government interests. Key business interests in Europe and Japan also pushed for strengthened measures for intellectual property. While U.S. corporate actors play an important role, the international effort to increase the protection of intellectual property rights can be understood as one of global corporate actors representing a diverse array of multinational corporations and trade associations (Matthews 2002).

II) From TRIPS to Regulation of Online Infringement

Intellectual property actors' campaign against online infringement is a continuation of their battle to create TRIPS. Even though TRIPS advocates claimed "we got 95% of what we wanted" in the agreement (Sell 2011:448), it was never intended as an end goal but rather a beginning point for tough new global standards. In this battle for intellectual property protection, each new agreement or standard merely establishes a global baseline or "floor," which proponents of intellectual property seek to "raise" in subsequent efforts to strengthen enforcement mechanisms (Sell 2003). The corporations and trade associations that successfully created and achieved consensus over TRIPS began in the late 1990s and early 2000s to apply their considerable lobbying and policymaking acumen to the online realm.

i) *Challenges and Advantages of Online Enforcement*

Following the implementation of TRIPS in 1995, U.S. intellectual property actors increased their push for legislation to deal with online infringement. TRIPS was created at a time when counterfeit goods were smuggled in container loads into ports from foreign manufacturing sites and then distributed through flea markets and low-end retail outlets. That world, in part, still exists. Counterfeit goods must still be manufactured and physically shipped to consumers, unlike music, movies, books and software which can be created and disseminated in an electronic format. E-commerce enables businesses, whether licit or illicit, to communicate with customers, advertise their wares, and establish markets globally for their products. Sellers of counterfeit goods can offer their wares through platforms like eBay or the China-based Taobao marketplace. They can also set up their own website to sell counterfeits openly to willing consumers or try to deceive individuals who want to buy genuine products.

At the same time, the Internet brings distinct enforcement challenges as a space for transnational policing (Bowling and Sheptycki 2012; Sheptycki 2007). The International Anti-Counterfeiting Coalition argues that its members face difficulties in protecting their intellectual property online because of the “relative anonymity, minimal cost of entry, and decreased overhead of the online retail market, compared to traditional brick-and-mortar” stores (Johnson 2013:2). Addressing wrongdoing on the Internet also commonly involves jurisdictional challenges, as countries may not have the capacity or interest in addressing online infringement (Mann and Belzley 2005). Further, targeting infringing sites can be challenging as site operators may shift from one jurisdiction or service provider to another in response to enforcement pressure. Internet law scholar Peter Swire refers to this type of illicitly operating sites as “mice” (Swire 2005). Such mice are small, nimble and breed annoyingly quickly, which makes traditional enforcement operations difficult (Swire 2005:1979). Those in the intellectual property protection sphere refer to this challenge as “whack a mole,” in a reference to the popular arcade and carnival game. Bob Barchiesi, president of the IACC explains that rights holders

Would take websites down and they'd pop right back up. Within twenty seconds, they'd knock a site down and it would pop back up with a number one or a dot, just something a little bit different [in the domain name]. It just wasn't doing anything. It didn't have any effect at all.⁹⁷

Intellectual property actors argue that because of the pervasiveness of online infringement and the difficulties in policing it, the problem is too large and complex for rights holders to address alone. Further, they claim that Internet intermediaries bear a certain degree of responsibility for policing infringement and ensuring that they do not facilitate infringing activities. Internet intermediaries, as defined in chapter 1, are firms that facilitate a wide range of technical and commercial interactions, transactions and services on the Internet, such as search, payment or advertising (OECD 2011). When states or private actors persuade intermediaries to monitor or control certain activities, intermediaries became gatekeepers or enforcers. Any Internet intermediary can be persuaded to act as a gatekeeper, given the right motivation.

Intermediaries are generally perceived to be more cost-effective and efficient regulators than if government (or corporations) were to undertake the regulation alone.⁹⁸ Not all intermediaries have an equal regulatory capacity. Their capability in controlling different types of wrongdoing depends on how they operate, their scope, and the services they offer. Internet intermediaries range from micro-intermediaries, which have relatively small operations in terms of their market share, users and transactions and scope, to macro-intermediaries.⁹⁹ The term macro-intermediary refers to a small group of Internet firms and payment providers that operate vast, global platforms and command significant market share in their industry sectors.

While the Internet brings enforcement challenges, it also offers considerable advantages. A London-based investigator with a firm specialising in intellectual property protection explains:

⁹⁷ Interview with Bob Barchiesi, President, International Anti-Counterfeiting Coalition, 24 April 2012, Washington.

⁹⁸ For discussions on the perceived cost-effectiveness of Internet intermediaries, particularly payment providers, see MacCarthy (2010).

⁹⁹ For a discussion of macro- and micro-gatekeepers in the online environment, see Laidlaw (2010).

Actually, being online, to some extent, makes it easier because you do have cutting points. Online people have a trail. They do have these merchant accounts. [...] It leads directly to their bank account. It will lead to details of where these individuals are and who they are.¹⁰⁰

Macro-intermediaries can enable rights holders to detect and exploit “cutting points” (or chokepoints, for example, bank accounts) and track down wrongdoers. Intellectual property actors recognised the role that macro-intermediaries could play in controlling infringement and mounted high-pressure campaigns to convince the Internet actors to assist them. Macro-intermediaries use technology as a regulatory instrument—a characteristic of techno-regulation. These Internet actors operate massive surveillance and enforcement programs and have the capacity to monitor and control hundreds of millions of transactions across and users of their systems. Macro-intermediaries regulate their users’ behaviour through their internal terms-of-service agreements, which enables them to institute rules swiftly and easily and govern their platforms and services globally. These firms are industry leaders, meaning that once they adopt certain rules, others in their industry tend to follow, particularly if they have contractual relationships with the macro-intermediaries. Further, by virtue of their size, these macro-intermediaries can enact chokepoints that, to varying degrees, control the flow of transactions, users or information across their vast systems. These macro-intermediaries, then, can exert considerable regulatory authority and shape the use of essential Internet services, like payment, search and domain name services.

Before examining efforts by states and rights holders to enlist these macro-intermediaries, this chapter briefly outlines how the 1998 U.S. *Digital Millennium Copyright Act* (DMCA) and similar legislation in the European Union set the standard for anti-counterfeiting efforts.

ii) ***The DMCA: Setting the Standard for Online Enforcement***

The *Digital Millennium Copyright Act* (DMCA) was the first major piece of legislation to address the online infringement of intellectual property rights. The

¹⁰⁰ Interview with Gavin Hyde-Blake, Director of Research and Investigation, Eccora, 19 September 2012, London.

DMCA was born out of rights holders' growing concerns in the United States about digital-copyright infringement in the early 1990s (see Zittrain 2006). This legislation focuses exclusively on copyright infringement. However, two elements are important because the DMCA influenced the regulation of trademark infringement in the United States and internationally. First, the DMCA struck a balance between the interests of rights holders and intermediaries. In particular, it granted specific intermediaries conditional immunity from liability for the infringement if, among other criteria, they removed the allegedly infringing content.¹⁰¹ Second, the DMCA instituted a response to infringement that was echoed internationally and adopted in relation to trademark infringement—the notice-and-takedown regime.¹⁰² This refers to intermediaries' practice of removing content (i.e., takedown) upon receiving a complaint from the relevant rights holders (i.e., notice).

Once the United States passed the DMCA, it pushed other countries to adopt similar notice-and-takedown legislation to establish a new, global baseline for the protection of copyright. In the following years, other countries slowly implemented their own legislation (de Beer and Clemmer 2009). Like the DMCA, these laws established some sort of compromise between intermediaries and rights holders and provided limited immunity for certain intermediaries in exchange for their prompt action upon receipt of a notice of infringement (Weatherall 2012). In 2000, the European Parliament introduced the *Electronic Commerce Directive (E-Commerce Directive)*,¹⁰³ which harmonised the conditions under which intermediaries could be held liable for third-party infringement throughout the Europe Union.¹⁰⁴ It employs a notice-and-takedown scheme for infringing content similar to that of the DMCA.¹⁰⁵

While the DMCA focuses solely on copyright infringement, the *E-Commerce Directive* takes a broader approach. It applies to a range of activities, including

¹⁰¹ DMCA Sec. 512 (b)(1).

¹⁰² DMCA Sec. 512 (b)(1)(E).

¹⁰³ The United Kingdom implemented the Electronic Commerce (EC Directive) Regulation 2002, SI 2002/2013, a mirror of the ECD, as all member states of the European Union must do with EC Directives.

¹⁰⁴ This is not a harmonization of liability but rather of "limitations of liability" (see Sparas (2013:10).

¹⁰⁵ For example, ECD Article 14 (b): "the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."

copyright and trademark infringement, as well as defamation. The Directive does not provide a legal definition of “intermediaries,” although it describes the intermediaries that it considers “information society service providers,” which includes those that sell goods online, like eBay and Amazon.¹⁰⁶ The *E-Commerce Directive* is echoed, to varying degrees, in legislation of the European Union member states and thus governs how those countries address infringing sites.

The DMCA and *E-Commerce Directive* establish a baseline for rights holders to address the online distribution of counterfeit goods, albeit unintentionally in the case of the DMCA. They provide a framework for Internet firms not designated as intermediaries within these acts to deal with online infringement. For example, in 1998 eBay created a notice-and-takedown program called VeRO (Verified Rights Owner Program) modelled on the DMCA as part of its efforts to respond to rights holders’ complaints of the sale of counterfeit goods, threats of legal action and lawsuits (see Dougherty 2011). Further, the DMCA and the *E-Commerce Directive* illustrate how states arbitrate among competing (in these cases, corporate) interests and, in doing so, align themselves more closely with certain interests, specifically rights holders, rather than others. In the DMCA, the U.S. government continued its long-held tradition of seeking ever-increasing protection for intellectual property (see Haggart 2014), a practice it maintained with the introduction of the *Stop Online Piracy Act* in 2011. With the DMCA and SOPA, the U.S. government further demonstrates that it is non-neutral arbitrator on the issue of intellectual property as its interests are closely inter-twined with prominent rights holders and trade associations.

III) Expansion of Online Enforcement Efforts Against Infringement

With the maturation of e-commerce, intellectual property actors in the United States argued that legislation dealing with online infringement needed to be updated. Notice-and-takedown schemes, spurred into being by the 1998

¹⁰⁶ In Article 18, the Directive describes intermediaries that provide mere conduit services (e.g., that provide access to the Internet, like Virgin Media), caching services (e.g., as undertaken by web browsers), and hosting services (e.g., like Facebook or eBay).

DMCA, had not evolved alongside Internet technologies and Internet intermediaries. Since the late 1990s, there has been a dramatic expansion in Internet services with the creation of entities like PayPal (created in 1999), Facebook (2004), YouTube (2005) and Twitter (2006). Given this range of new types of intermediaries, proponents of tougher intellectual property protection began arguing in the mid-2000s that new legislation was needed in the United States to update the DMCA (Castro, Bennett, and Andes 2009). They contended that more types of Internet intermediaries should be obliged to assume gatekeeping duties, particularly payment and advertising intermediaries, in addition to those proscribed in the DMCA (Castro, Bennett, and Andes 2009).

i) ***Emergence of “Voluntary” Enforcement Initiatives***

Voluntary (non-legally binding) enforcement efforts against online infringement emerged in the European Union and United States in 2009. In the European Union, there is a history of official support for non-binding enforcement agreements among private actors. The 2000 *E-Commerce Directive*, which also sets out enforcement provisions against online trademark infringement that were discussed earlier, grants Internet service providers permission to form non-binding agreements to develop “rapid and reliable procedures for removing and disabling access to illegal information.”¹⁰⁷ In 2004, the European Commission called upon industry to take an active role in anti-infringement efforts and promoted the development of codes of conduct as “a supplementary means of bolstering the regulatory framework” (European Commission 2004:4).

It was in 2009, however, when negotiations began on the first non-binding agreement for the enforcement of intellectual property rights. In that year, the European Commission announced it had “organised a structured dialogue between stakeholders to facilitate mutual understanding” in relation to the sale of counterfeit goods through online marketplaces (European Commission 2009:10). The resulting agreement, which will be examined in greater detail

¹⁰⁷ *E-Commerce Directive* Art. 40 also states that provisions in this Directive “should not preclude the development and effective operation, by the different interested parties, of technical systems protection and identification and of technical surveillance made possible by digital technology.”

later in chapter 6, established a set of non-binding general principles among marketplaces, rights holders and their trade associations to guide enforcement efforts against counterfeit goods.

In the United States, the idea of voluntary industry initiatives also began to gain traction in 2009. The International Trademark Association (INTA), an influential New York City-based trade body, recommended that more intermediaries needed to assume greater enforcement responsibility for the online sale of counterfeit goods. INTA released recommendations that online marketplaces, search engines, and payment providers should adopt voluntary measures to address the online sale of counterfeit goods (INTA 2009). Prominent firms agreed to the measures, including Visa, MasterCard, American Express, and Paypal, as well as eBay, Yahoo and Google. The recommendations largely focus on educating consumers and encouraging intermediaries to work with rights holders and establishing clear processes to deal with infringement.

Also in 2009, the Information Technology and Innovation Foundation (ITIF), a Washington, D.C.-based think tank, released a white paper. In the paper, ITIF analysts recommended that the U.S. government should “encourage stakeholders to develop best practices and collaborative self-regulation regimes” (Castro, Bennett, and Andes 2009:23). Daniel Castro, lead author on the paper, acknowledged that there is no “silver bullet” or “single technical or legislative proposal will completely solve such a complex issue” as online infringement but “there are many “lead bullets”” (Castro, Bennett, and Andes 2009:1). In this bullet metaphor, many intermediaries have important roles to play in the regulation of online infringement, particularly search engines, payment providers and advertising platforms. ITIF analysts recommended that the U.S. government work with rights holders and intermediaries to identify infringing sites. Once infringing sites are identified, “ad networks and other companies can refuse to place ads with them, and banks and credit card companies can refuse to process payments to them” (Castro, Bennett, and Andes 2009:23).¹⁰⁸

¹⁰⁸ ITIF’s white paper also recommends search engines and Internet service providers block infringing sites in a manner similar to that used against sites distributing child pornography (see Bennett, and Andes 2009).

The proposals by the International Trademark Association and the Information Technology and Innovation Foundation recommended a significant departure from the traditional conception of Internet intermediaries. First, these groups argued that more types of Internet intermediaries should be enlisted as gatekeepers to address online infringement on behalf of rights holders, like payment providers and advertising platforms. Second, INTA and ITIF advocated an expansion of intermediaries' traditional notice-and-takedown roles (as described in relation to the *E-Commerce Directive*) to include notice-and-termination programs. In notice-and-termination programs, Internet intermediaries withdraw or terminate services to sites upon receiving a complaint (i.e., notice) from rights holders of infringing activity. Intermediaries can withdraw payment processing services, for example, that disable a website's capacity to process payments. Third, these programs would be voluntary.

In their recommendations, INTA and the ITIF advocated a shift from the removal of infringing content, in which sites remain functional, to the disabling of sites through the termination of their essential technical and commercial services. Proponents of this strategy view Internet intermediaries as the most appropriate regulators and argue that they have technological capacities to detect and address online infringement (Castro, Bennett, and Andes 2009). In this strategy of regulation through technology, advocates argued that the focus of enforcement should move from the removal of specific infringing content to the termination of entire sites. Rights holders and intermediaries would work together with minimal government involvement to determine what constitutes infringement and how best to address it (Castro, Bennett, and Andes 2009). The state, however, would remain in the background to provide coercive pressure to stimulate or direct regulatory activities, a situation that is clearly evident in the private regulatory arrangements examined in chapters 4 to 6.

Neither the INTA proposal nor the ITIF proposal considered the involvement of consumers or civil-advocacy groups in relation to the voluntary initiatives. Moreover, ITIF's report acknowledged that encouraging Internet firms and payment providers to act voluntarily against infringing sites could raise the possibility of anti-competitive behaviour. Macro-intermediaries hold

considerable market share in their industry sectors, such as Google for search engines and Visa, PayPal and MasterCard for payment providers. To address problems of potential anti-competitive behaviour, ITIF suggests, “the government should also consider providing anti-trust exemptions for collaborative industry action” (Castro, Bennett, and Andes 2009:23). Such collaborative industry action against infringement, ITIF argues, is more important than deterring potential anti-competitive behaviour among Internet giants. It is evident in ITIF’s strategy, and argued throughout the dissertation, that the interests of consumers and the public are secondary to the protection of intellectual property on behalf of rights holders.

ii) ***Four Doomed Intellectual Property Bills in the United States***

While intellectual property actors were pushing macro-intermediaries in 2009 to adopt non-binding enforcement measures, they were also forcefully lobbying U.S. legislators and policymakers for legislation to update the DMCA. As discussed in chapter 2, there are advantages and disadvantages of voluntary regulation by industry actors. Non-binding measures can be created and altered rapidly, according to the situation and participants’ needs (Büthe 2010; Cafaggi 2011). Legislation, meanwhile, has judicial safeguards, punitive sanctions and a binding force that, in the case of intermediaries, would require them to police infringing sites. Proponents of legislation framed online infringement as a problem best solved by Internet intermediaries, as is evident in the proposals from the Information Technology and Innovation Foundation. Regulation by intermediaries gained public prominence when they became the centrepiece of four U.S. federal bills on intellectual property enforcement introduced in 2010 and 2012.

a) **Combating Online Infringements and Counterfeits Act**

When Senator Patrick Leahy, a Democratic senator from Vermont, introduced an intellectual property bill in September 2010, there was no indication that intellectual property would captivate millions of people less than two years later and spark a massive online protest. At that time, intellectual property was a largely considered an arcane subject of interest only to large corporations and

attorneys. The bill, *Combating Online Infringements and Counterfeits Act* (COICA)¹⁰⁹ would have allowed the Attorney General to seek court orders against domestic and foreign infringing domain names (see Table 3.1).¹¹⁰ Internet intermediaries, specifically domain name registrars, payment providers and advertising platforms, would be required to withdraw their services from targeted sites.¹¹¹ The bill also would have granted these intermediaries the right to act voluntarily against domain names they reasonably believed was “dedicated to infringing activities.”¹¹²

Civil-society groups like Electronic Frontier Foundation contended the bill would result in inadvertent takedowns of legitimate sites and would censor the Internet (Timm 2012). More surprising, however, was fierce opposition from Senator Ron Wyden, a Democrat from Oregon. Intellectual property is a long-standing, non-partisan issue in the United States (Drahos and Braithwaite 2002). Wyden broke ranks with his Senate colleagues and announced he would vote against the bill in a full Senate vote because he said, as written, it was “almost like using a bunker-busting cluster bomb when what you really need is a precision-guided missile” (Anderson 2010).

b) Protect Intellectual Property Act

Given Wyden’s opposition, Senator Leahy withdrew the bill and in May 2011 introduced a revised version of the bill into the Senate Judiciary Committee. The *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act* (PIPA) had several similarities with its predecessor (see Table

¹⁰⁹ *Combating Online Infringements and Counterfeits Act* of 2010, 111th Cong., 2nd Sess., September 20, 2010, S. 3804.

¹¹⁰ COICA would have targeted domain names, which are the names given to Internet Protocol addresses, such as ThePirateBay.se. One domain name may have multiple websites. For example, in 2011 the U.S. Department of Homeland Security’s Immigration and Customs Enforcement seized a domain—mo00.com—that was a domain name service provider. As a result, 84,000 subdomains were wrongfully seized as well and associated with the child pornography charges that resulted in the seizure of mo00.com (Kopel 2013). In contrast, the *Stop Online Piracy Act* would have targeted particular infringing websites, which are sets of related webpages.

¹¹¹ COICA, Sec. 2(e)(2) (non-domestic names) and COICA Sec. 2(e)(1) for domestic domain names.

¹¹² COICA, Sec. 2(e)(B).

3.1).¹¹³ PIPA allowed the Attorney General to seek court orders to be served on intermediaries requiring them to withdraw their services from infringing sites.¹¹⁴ It also granted intermediaries a voluntary right of action against sites selling or dispensing pharmaceuticals without a valid prescription and for “medication that is adulterated or misbranded”.¹¹⁵ However, PIPA went a step further than COICA when it proposed to grant rights holders a private right of action (see Tables 3.2 and 3.3). This provision would have enabled rights holders to seek a court order to compel payment providers and Internet advertising networks to suspend their services to infringing sites.¹¹⁶

Table 3.1: Comparison of Intermediaries – Private Right of Action

	COICA	PIPA	SOPA	OPEN
Actors	Domain registries & registrars, payment providers & advertising platforms	Domain registrars & registries, payment providers, advertising platforms, information location tools	Advertising platforms, search engines, domain registrars, & registries, payment & providers	Advertising platforms & payment providers
Private right of action	No	Yes - Payment providers & advertising platforms (Sec. 4)	Yes - Advertising platforms & payment providers against foreign infringing sites (Sec. 103).	No

c) Stop Online Piracy Act

While PIPA was under discussion in the Senate Judiciary Committee and critics were raising mounting concerns about its provisions, another intellectual property bill was introduced in October 2011. Representative Lamar Smith, a Republican from Texas, introduced the *Stop Online Piracy Act* (SOPA) into the

¹¹³ *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act* of 2011. 112th Cong., 1st sess., May 12, 2011, S. 968.

¹¹⁴ PIPA Sec. 3(2).

¹¹⁵ The provision defined ‘misbranded’ as that within *Section 502 of the Federal Food, Drug, and Cosmetic Act* (21 U.S.C. 352). This section refers to false or misleading labels, packages, or contents on labels. See PIPA, Sec. 5(b) in relation to voluntary action against infringing sites threatening public health.

¹¹⁶ PIPA Sec. 4.

House Judiciary Committee. Like PIPA, SOPA allowed the Attorney General to seek court orders to require a range of intermediaries to disable their services to infringing sites. SOPA also granted a private right of action to rights holders.¹¹⁷ It granted voluntary right of action to intermediaries to withdraw their services from sites they reasonably contend are infringing sites and to sites endangering the public health by distributing counterfeit pharmaceuticals (see Tables 3.1 and 3.2).¹¹⁸ SOPA took a tougher line against Internet intermediaries than PIPA: it introduced a timeframe of five days for intermediaries to take action or face penalties.¹¹⁹

Table 3.2: Comparison of Intermediaries – Voluntary Actions

COICA	PIPA	SOPA	OPEN
Domain registries & registrars, payment providers & advertising platforms (Sec. 2(e)(B).	Payment provider & advertising platforms against foreign infringing sites (Sec. 5a). Domain registrars & registries, payment provider, advertising platforms, information location tools against sites endangering public health (Sec. 5b).	Payment providers, advertising platforms, search engines, domain registries & registrars against sites reasonably believed to be foreign infringing sites (Sec. 104). Payment providers, advertising platforms, search engines, domain registries & registrars against sites endangering public health (Sec. 105).	Advertising platforms & payment providers against sites endangering public health (337A(8)(13)(k)

¹¹⁷ SOPA Sec. 103.

¹¹⁸ SOPA Sec. 104 granted immunity for voluntary action against non-U.S.-based infringing sites and SOPA Sec. 105. granted voluntary right of action against sites endangering public health.

¹¹⁹ SOPA Sec. 102 and 103.

d) **Online Protection and Enforcement of Digital Trade Act**

As protests grew over SOPA and PIPA, two politicians who were critical of the bills introduced an alternative, the *Online Protection and Enforcement of Digital Trade Act* (OPEN Act) in December 2011.¹²⁰ Senator Wyden introduced it into the Senate Finance Committee and Representative Darryll Issa, a Republican from California, introduced the Act into the House Judiciary Committee. OPEN differed substantially from the previous bills. It did not offer a private right of action nor did it propose that the Attorney General could seek court orders against infringing sites. Instead, it proposed to situate the regulatory authority for foreign infringing sites in the U.S. International Trade Commission (ITC).¹²¹ The ITC could grant rights holders orders to compel payment service providers and advertising intermediaries to withdraw their services from infringing sites.¹²² Like SOPA and PIPA, however, even OPEN would granted voluntary right of action to payment providers and Internet advertising networks against infringing sites endangering the public health through the unauthorised distribution of pharmaceuticals (see Table 3.3).¹²³

e) **Protests over PIPA and SOPA**

Soon after the introduction of COICA, civil-advocacy groups like Electronic Frontier Foundation and Public Citizen criticised the bill, along with cyber law scholars and technologists who track regulation on and of the Internet (Benkler 2011). With the introduction of PIPA and SOPA, the protest gathered momentum as critics wrote about it in blogs, spread the word through social media, circulated petitions, and on November 16, 2011, declared “America censorship day” to protest the bills, which gathered four million signatures on its first day (Moon, Ruffini, Segal 2013; Sell 2013). The campaign accelerated in

¹²⁰ *Online Protection and Enforcement of Digital Trade Act*. H.R. 3782 (112th Congress, 2011–2013). Introduced Jan 18, 2012; *Online Protection and Enforcement of Digital Trade Act*. S.2029 (112th Congress, 2011-2012). Introduced 17 December 2011.

¹²¹ In contrast to COICA, PIPA, and SOPA, which would have operated through the Attorney General at the Department of Justice, OPEN proposed to work through the ITC, an independent, quasi-judicial federal agency with an investigative mandate for trade-related issues. The OPEN Act would have only considered foreign infringing sites and referred domestic infringing sites to the Attorney General for investigation.

¹²² SOPA Sec. (8)(13)(g).

¹²³ OPEN 337A(8)(13)(k).

late 2011 as anti-SOPA activists planned an Internet blackout for January 18, 2012 in which thousands of websites agreed to block their home webpages partially or completely in solidarity with the protest (Sell 2013). These sites, like Google and Wikipedia, urged concerned individuals to contact their elected representatives in the United States. Following an unprecedented outpouring of anger against PIPA and SOPA, the U.S. Congress withdrew them on January 20, 2012. The OPEN Act languished after the SOPA protests and has not progressed since then.

f) Legitimising Intermediaries as Gatekeepers

Although these bills failed to become law—and, in the case of PIPA and SOPA, spectacularly so—they served an important purpose for intellectual property actors. There are commonalities across the four bills, even though the OPEN Act was introduced as an alternative to PIPA and SOPA. All the bills focused on disabling infringing sites by using intermediaries to withdraw commercial and business services instead of removing infringing content. They all proposed to grant intermediaries a voluntary right of action against sites that unlawfully distribute pharmaceuticals. Finally, they all expanded the concept of Internet intermediaries that should bear responsibility for policing online infringement from the 1998 DMCA and 2000 European *E-Commerce Directive*. Each bill references payment providers and advertising platforms.

Although there are differences among these bills, their similarities indicate a degree of consensus among U.S. policymakers and legislators in terms of enforcement strategies that are considered suitable. The bills legitimised ideas of disabling sites, at least in the eyes of the bills' proponents. They also legitimised the concept of voluntary right of action for intermediaries against certain types of infringing sites. Even the OPEN Act incorporated ideas of voluntary rights of action and targeting entire sites instead of proposing policies to address specific problematic content or activities. The differences between OPEN and the other bills are therefore not absolute but a matter of degrees.

The Electronic Frontier Foundation referred to the bills' voluntary measures as the "vigilante provision" because intermediaries could act without any judicial

oversight, “the standard for immunity is incredibly low and the potential for abuse is off the charts” (Timm 2012). To qualify for immunity, these intermediaries need only act “in good faith” and “on credible evidence,”¹²⁴ which raises significant concerns given the number of complaints of inaccurate or abusive enforcement by intermediaries in the area of digital-copyright enforcement (see Urban and Quilter 2006).¹²⁵ The recasting of Internet intermediaries as gatekeepers fundamentally shifts intermediaries’ burden of responsibility for policing third-party infringement on their platforms. While these bills clearly recognise that these intermediaries have specialised, technical knowledge and their capacity to regulate certain activities, their determination of why Internet intermediaries should bear responsibility for infringement is less compelling. The reasoning appears to be that intermediaries have a technical capacity to monitor and block certain transactions and a global reach. Therefore, intermediary-facilitated regulation would enable rights holders—and, by extension, the U.S. government—to expand their regulatory efforts globally. Despite the death of these bills, their ideas live on in non-binding agreements adopted by an elite group of macro-intermediaries, as the next section explores.

IV) Framing the Debate over Online Enforcement

The acrimonious debate over the *Stop Online Piracy Act* provides a valuable opportunity to examine how intellectual property actors and macro-intermediaries frame ideas around the online regulation of intellectual property rights. By examining actors’ competing narratives regarding online infringement, the researcher can focus upon how they try to legitimise their positions and, in turn, influence policymaking in the United States. As discussed in chapter 2, actors may draw upon different sources of legitimacy consecutively or simultaneously. They can also construct, shape, meld or manipulate legitimacy claims depending on the community to whom they are speaking. Actors may look to various sources for authority but corporate actors commonly draw upon their power in the market (often termed structural authority) (see Avant,

¹²⁴ SOPA Sec. 105.

¹²⁵ For example, in a study of takedown notice in relation to copyright infringement, Urban and Quilter (2006) found a large proportion (55% of notices they examined related to Google’s search results) were from businesses trying to remove search results of their competitors (see Urban and Quilter 2006).

Finnemore, and, Sell 2010). Corporate actors also draw upon discursive authority, which refers to their capacity to construct and communicate persuasive narratives about particular problems and appropriate solutions (Fuchs 2007).

i) ***Framing the Concept of Intellectual Property***

Underlying the concept of framing is the understanding that ideas are influenced by the social milieu in which actors operate and are thus subject to shift and change (Odell and Sell 2006). Perceptions of the material world are “mediated through ideational processes” (Béland 2010:148), which means that actors give meaning to and make sense of the world in which they live. Actors can use ideas and metaphors as discursive frames to present events or behaviour in certain ways and suggest alternatives (see Odell and Sell 2006). In relation to policymaking, actors employ frames to persuade others of the seriousness of particular problems and the necessity of reform. Effective framing is vitally important. “One must convince people that one’s arguments are good, one’s institutional innovations necessary, and one’s horror stories disturbing” (Boyle 2007:18 in Sell 2003:3).

Just as actors construct and interpret particular policy responses as appropriate, they also define and shape the perceived problems. As discussed earlier in this chapter, rights holders strategically constructed an association between intellectual property and international trade. Similarly, they have proven remarkably apt at framing infringement as a serious criminal offence. This strategic construction of crime (Lacey and Zedner 2012) enables rights holders to shift attention away from any role that their corporate processes may play in creating opportunities for counterfeiters, like out-sourcing production to China (Mackenzie 2010). There is a common misconception “that there’s some kind of boogeyman counterfeiter or evil empire,” explains a Hong Kong-based attorney, “Nine times out of ten it’s their own suppliers.”¹²⁶ Thus, instead of interpreting the problem as one of parallel trade or contractual dispute between rights holders and manufacturers, counterfeiting is framed as a criminal

¹²⁶ Interview with lawyer at Hong Kong law firm, 7 May 2012, Washington.

offense.¹²⁷ Intellectual property actors' framing of infringement as a harmful crime has remarkable staying power. It is a frame that simplifies complex issues. What is often defined as a problem of "counterfeit pharmaceuticals," for example, can be much more complicated. Intellectual property actors sometimes conflate issues of generic medication, counterfeit pharmaceuticals, parallel trade medication, and substandard medication.¹²⁸ Such slippage among different issues can enable actors to portray a problem as larger or more serious than it is in reality.

Before protests over the bill made supporting it politically unpalatable, SOPA (and its sister bill the *Protect IP Act*) commanded wide, though not universal support in the U.S. Congress. Industry supporters were largely multinational rights holders and their affiliated trade associations like the Motion Picture Association of America, the Recording Industry Association of America, and the Entertainment Software Association. Opponents of the bills were an eclectic group ranging from non-governmental organizations, librarians, civil-society groups and technologists to Internet giants. These latter actors included Google, Yahoo, Amazon, eBay, Facebook, and Twitter, as well as the industry associations like the Consumer Electronics Association (Sell 2013).

ii) ***Advocates for SOPA***

Proponents of tougher enforcement against online infringement draw upon arguments they have successfully employed since the 1980s: counterfeit goods cost jobs, threaten innovation and endanger public health (Halbert 1997). For the online realm, they also emphasise what they see as the inherently deceptive nature of infringing sites that lure unsuspecting consumers because they accept popular credit cards. Such sites threaten "our collective confidence in the Internet ecosystem," argued Representative Bob Goodlatte, a Republican from

¹²⁷ Parallel trade refers to the distribution of legitimate, non-counterfeited goods from one country or region to another without the authorization of the intellectual property rights owner. Rights holders generally object to this practice because they may practice differential pricing in which an identical product is assigned higher prices in certain country or regions.

¹²⁸ Generic pharmaceuticals refers to genuine drugs that are no longer covered by a patent and that are identical in terms of active medicinal ingredients but typically cheaper than brand-name versions of the same drug. Counterfeit pharmaceuticals refer to medication that is deliberately and fraudulently mislabelled and may have the wrong or incorrect quantities of active ingredients. Substandard medication, which describes problems with or flaws in the medication, can refer to genuine or counterfeit medication.

Virginia, in his remarks to the House Judiciary Committee on SOPA in 2011 (Goodlatte 2011:38). Elements of the SOPA debate echoed concerns from the late 1970s about a flood of counterfeit goods from Asia. Advocates directed heated accusations at China, demonstrating that the rhetoric of the 'foreign counterfeiter' has remarkable staying power.¹²⁹ Metaphors of lawlessness and ungoverned spaces are used in relation to infringement to lend urgency to enforcement efforts and justify action from both the state and the private sector (Loughlan 2006).

SOPA advocates worked to recast opposition by Google, Yahoo and others to the bill as being fundamentally concerned with furthering their business interests rather than protecting American businesses and consumers. By arguing that Internet intermediaries were part of the problem, intellectual property actors sought to shift the burden of regulatory responsibility onto those intermediaries. Representative Lamar Smith, a Texas Republican, underlined this point when he argued that if Google made "the right decision" (i.e., strengthened its enforcement efforts) then it would have to give up revenue from "ads that are actually on the infringing websites" (Smith 2011:129).

iii) *Opponents of SOPA*

Opponents of the proposed legislation argued that they supported the bill's intention to address copyright infringement and the online distribution of counterfeit goods but criticised the proposed measures as flawed and problematic. "Believing that a free and open Internet is worth fighting to protect," Senator Wyden argued, "does not mean that we aren't concerned about copyright infringement" (Wyden 2011). To underline their legitimacy as guardians of the Internet, Internet firms emphasised the important roles they played in facilitating a healthy and vibrant Internet, social and cultural interactions, and fertile environment for e-commerce. These firms pointed to their considerable economic contribution to the U.S. economy. Google, for

¹²⁹ The narrative that constructs counterfeiting as a serious, transnational crime also conceptualises the 'counterfeiter' as the foreign 'other,' a process that is common to many other narratives explaining crime (e.g., see Woodiwiss (2001) for a critique of 'foreign' organised crime).

example, stressed that the firm generated \$64 billion in economic activity in 2010 for American businesses (Oyama 2011).

These firms also grounded their objections in appeals to protect basic rights and freedoms, particularly freedom of speech (Sell 2013). Randall Rothenberg, president of the Interactive Advertising Bureau, the trade association for digital advertisers, emphasised that his industry was “greatly concerned about the broad, potentially unconstitutional, constraints on the freedom to advertise,” which is protected by the First Amendment in the United States (Rothenberg 2011). Kent Walker, vice president and general counsel at Google, said that any measures must not undermine the principle of “Internet freedom [as] a cornerstone of U.S. foreign policy” (Walker 2011:7-8). Nor, he argued, should they endanger “legitimate technologies, innovative businesses, and lawful speech” (Walker 2011:7-8).

In testimony to Congress, Google, MasterCard and GoDaddy all expressed support for some form of voluntary regulation that would give them the flexibility to address infringement in their own way (for MasterCard, see Kirkpatrick 2011). These firms warned, however, that the burden for enforcement could not fall on intermediaries alone. In a statement that all intermediaries echoed, to varying degrees, Google argued, “no intermediary will be able to prevent all abuse of its systems” (Oyama 2011:7).

iv) *Inter-Play of Interests*

By examining the competing frames employed by advocates and opponents of SOPA, one can also study the varying interests and power dynamics at play in relation to the regulation of online infringement. Both camps drew upon considerable resources of structural and discursive authority. Each created a compelling narrative that spoke to their respective constituencies. Proponents of the bill represented the Goliath in this battle because of their decades of successful intellectual property policymaking in the United States and on the global stage (Sell 2003). The anti-SOPA coalition expertly roused public opposition and achieved a surprise upset over the powerful, institutionalised interests of intellectual property actors. This clash of multi-national corporations

over intellectual property enforcement is unusual. More unusual was the legislative defeat of rights holders, which was the first such occasion in 30 years in the United States (Sell 2013).

Despite the remarkable achievement of the SOPA protest, it is important to recognise that it was a temporary alliance among a broad coalition of interests. Internet firms flexed their growing lobbying power but their interests may not necessarily align again with others in the anti-SOPA movement (Sell 2013). The coalition successfully created a narrative to defeat the bill—Stop Censorship and Don't Break the Internet—but even with the death of the bill the dominant frame—Copying is Theft—remains intact. Activists won the skirmish against the bill but lost the larger battle as intellectual property actors merely instituted SOPA-like measures into private non-binding agreements.

V) Creation of Private Enforcement Agreements

Given their opposition to SOPA's provisions, what explains macro-intermediaries' decisions to adopt private enforcement agreements that institute SOPA-like practices? There are several reasons, which will be explored further in the following chapters. First, macro-intermediaries face an uneven playing field, as explored earlier in this chapter. There is strong bipartisan support for greater protection for intellectual property rights in the United States. This sentiment is also evident in the European Union, as demonstrated by the actions of the European Commission and U.K. government in compelling macro-intermediaries to enter private enforcement agreements by threatening legislation or legal action. In addition, rights holders have an institutional advantage in terms of influencing states from their decades of shaping intellectual property policymaking in the United States and internationally. These states, this dissertation argues, are non-neutral actors that have strong preferences for macro-intermediary-facilitated regulation of intellectual property on the Internet.

There are two other important reasons that macro-intermediaries adopted the private enforcement agreements examined in this dissertation, as will be

examined further below. There are inter-dependent interests among macro-intermediaries, intellectual property actors, and states. Macro-intermediaries share common financial and reputational concerns with rights holders. More importantly, macro-intermediaries and the U.S. government, in particular, share overlapping interests in online surveillance.

i) *Inter-dependent Interests*

Macro-intermediaries, like rights holders, have financial interests in protecting intellectual property (trademarks, copyright and patents) related to their products and services. Internet firms and payment providers also have reputational interests in ensuring that they maintain the confidence of their users and preserve the reputation of their brands. As discussed in chapter 1, the European Union, and particularly, the United States perceive intellectual property as integral to their economies (Drahos and Braithwaite 2002; Sell 2003). Rights holders and trade associations constructed a conceptual linkage between intellectual property and international trade and, as a result, prioritise highly the protection of intellectual property rights (Sell 2003). Critics of this linkage argue that, in many cases, intellectual property does not boost economic growth but instead stifles innovation and rewards rent-seeking behaviour by large corporate interests (e.g., Drahos and Braithwaite 2002; Mazzone 2011; Raustiala and Sprigman 2012). This dissertation does not engage that debate but notes that the United States, United Kingdom and European Union accord intellectual property importance based, in part, on rights holders' persuasive narrative of its significance to their economies (Sell 2003).

In addition to common interests in intellectual property, states involved in the private regulatory regime (the United States, United Kingdom and the European Union) can capitalise upon macro-intermediaries' regulatory capacity to exert influence online in their areas of interest. The United Kingdom and the European Union, for example, are interested in working with Internet intermediaries, often in voluntary regulatory arrangements, to take down child pornography sites and extremism sites (Fae 2014; Laidlaw 2012). There are also complex, inter-dependent relationships between the macro-intermediaries and the U.S. government in relation to online surveillance. The U.S.

government, through its National Security Agency (NSA) and along with its allies, particularly the United Kingdom, is reliant upon macro-intermediaries' big-data-oriented business models.¹³⁰ These firms are ideally suited to facilitate mass surveillance as many of their applications and services are premised upon collecting, storing and mining vast amounts of personal and commercial data from their users.

Information from Edward Snowden's leaked files demonstrates the degree to which the NSA relies upon data from Google, Yahoo and Microsoft, which enables the United States and its allies to protect their national security and economic interests.¹³¹ These firms are economically motivated to work with the U.S. government to ensure that lucrative government contracts flow unimpeded. An executive for a top technology firm in the U.S. explained the difficulty of resisting the U.S. government in relation to the NSA's surveillance while courting its business. "We're fighting you on this," the unnamed executive exclaims, "oh, and can I have that \$400 million contract" (Levy 2014). State reliance upon information from macro-intermediaries provides a degree of legitimization of and protection for their corporate surveillance programs, which have regularly attracted criticism and charges of breach of privacy.

By agreeing to work with rights holders on intellectual property, an issue of significant importance to the United States and European Union, macro-intermediaries are in a valuable position to influence government policymaking and standard setting in areas of importance to them. This includes shaping regulations on digital privacy, intellectual property and anti-trust measures.¹³² Governments are also interested in shaping standards on the Internet to

¹³⁰ Big data can be understood as massive volumes of information that companies must process in order to identify patterns, infer probabilities and make connections. Firms like Twitter, Google and Facebook provide "free" services, such as search, email and social networking, in exchange for amassing and tracking users' data, which they sell to advertisers to generate the bulk of their revenue (Mayer-Schönberger and Cukier 2013).

¹³¹ The Snowden files reveal accounts of the NSA spying on allies of the United States to strengthen its economic bargaining position in trade talks. For example, the NSA monitored communications among European Union officials in New York and Brussels and also conducted surveillance of U.S. law firms representing foreign governments in U.S. trade disputes (Glanz and Lehen 2013).

¹³² Google, for example, is now one of the top five lobbying corporations in the United States along with companies like General Electric and AT&T. Its two main areas of lobbying are the topics of intellectual property (trademarks, copyright and patents) and labour and anti-trust issues, according to the Center for Responsive Politics' project OpenSecrets.org that tracks corporate lobbying amounts.

facilitate state influence over Internet infrastructure and services. The Snowden files, for example, reveal how the U.S. government strategically weakens encryption standard-setting processes to ensure it has a back door into companies using that encryption.¹³³ In doing so, the U.S. government signals its intention to remain a principal actor within the digital economy and the evolution of the Internet.

ii) *Uncertain Regulatory Landscape*

Macro-intermediaries face an uncertain legal climate in relation to the enforcement of intellectual property rights for several reasons. States threatened each of the macro-intermediaries examined in this dissertation with legislation or legal action. Rights holders and their trade associations have also sued or threatened legal action against macro-intermediaries. In relation to these lawsuits, U.S. and European courts have delivered starkly divergent rulings in relation to intermediaries' enforcement responsibilities, particularly in relation to online marketplaces (Mac Síthigh 2013; Rimmer 2011). More broadly, Internet-related intellectual property law is evolving with the maturation of e-commerce, shifts in business models, and with the growing industry awareness of online infringement (Mac Síthigh 2013). As a result, there is a lack of clarity on the nature of an appropriate notification of infringement from rights holders, which makes it difficult for intermediaries to determine what constitutes compliance and how to implement appropriate enforcement measures (McNamee 2011).

Intermediaries that face varying degrees of legal uncertainty about their enforcement responsibilities, have a greater motivation to adopt additional or informal regulatory measures (McNamee 2011). The threat of future legal proceedings against intermediaries for contributory liability is "the pressure that gets everyone to agree to the arrangements," explains Robert Guthrie, an associate at SJ Berwin LLP in London.¹³⁴ Thus, intermediaries' adoption of voluntary measures is partly "defensive" (Lindenbaum and Ewen 2012) as

¹³³ Snowden's files revealed that the NSA was deliberately weakening and introducing flaws into international encryption standards developed by industry, something long suspected by cryptographers (see Perlroth, Larson, and Shane 2013).

¹³⁴ Interview with Robert Guthrie, Associate, SJ Berwin, 5 October 2012, London.

compliant intermediaries presumably have a lower risk of being sued by rights holders or targeted by states for legal action.

iii) ***Limitations of Private Authority***

As will be explored throughout this dissertation, rights holders have some capacity to shape macro-intermediaries' enforcement practices by pressuring the firms and employing threats of legal action. However, they did not have the authority to force macro-intermediaries to adopt enforcement practices that were as coordinated, streamlined and comprehensive as rights holders desired. Rights holders, for example, were unable to persuade Visa and MasterCard to amend their enforcement practices to facilitate the rapid, mass termination of payment services to infringing sites.

Rights holders' private authority is limited: they do not have the ability to persuade other actors to adopt their rules in all circumstances. Intellectual property actors faced several critical impediments in their efforts to persuade macro-intermediaries to adopt strengthened enforcement measures voluntarily. Private actors' rule production and enforcement works best among "small exclusive clubs of participants" who lack important conflicts of interest (Peters, Förster, and Koechlin 2009:500). This is not the case in relation to the private regulation of online infringement. In this private regulatory regime, there are a range of industries, including apparel, sporting goods, electronics and pharmaceuticals. The macro-intermediaries involved represent multiple industry sectors, from advertising, search and domain name services to payment and marketplaces. In addition, these macro-intermediaries have considerable resources to defend themselves against threats of legal action and material interests in resisting greater responsibility for policing their platforms.

More importantly, rights holders and their trade associations have little leverage over these firms outside pressuring them and threatening legal action. Rights holders do not have a financial or contractual relationship with the macro-intermediaries, as is the case in some types of private regulation. Moreover, rights holders wanted the macro-intermediaries to adopt rules that would substantially alter their enforcement practices and generally exceed what the

firms are obliged to do under law or most court rulings. Give the impasse between rights holders and the macro-intermediaries, rights holders petitioned the state to intervene and to compel the firms to accept private non-binding enforcement agreements.

iv) ***Office of the U.S. Intellectual Property “Czar”***

Against the backdrop of increasingly heated debates over COICA, PIPA and SOPA, Internet firms and payment providers were quietly meeting with U.S. government officials to negotiate “voluntary, best practices” agreements. The office behind these efforts—the Office of the U.S. Intellectual Property Enforcement Coordinator (IPEC)—is small and almost entirely unknown to the general public. IPEC was created in the *Prioritising Resources and Organization for Intellectual Property Act (PRO-IP Act) of 2008* and is located within the Office of Management and Budget. Its mission is singular: coordinate and enhance federal enforcement efforts solely in relation to intellectual property rights.¹³⁵

Victoria Espinel served as the first head of IPEC, after the Senate confirmed her nomination in December 2009 until August 2013.¹³⁶ (Note: In an indication of the tight ties between this office and rights holders, in August 2013, Espinel left IPEC to work for Business Software Alliance, a trade association that represents the interests of software companies (BSA 2013).) During her tenure, Espinel was popularly referred to as the “IP czar.” This is a fitting title for Espinel who announced that her goal was to “change the enforcement paradigm” (IPEC 2012:44) in relation to online infringement by working “to encourage practical and effective voluntary actions to address repeated acts of infringement” (Espinel 2012). The term, “IP czar,” again reveals the priority that the U.S. government accords the protection of intellectual property.

¹³⁵ IPEC, for example, coordinates the Joint Strategic Plan on Intellectual Property Enforcement Report, prepares legislative recommendations on intellectual property enforcement, and develops strategies on certain topics, like counterfeit pharmaceuticals.

¹³⁶ Espinel had extensive experience working on intellectual property policy as senior counsel at the Office of the U.S. Trade Representative (USTR) and as the Assistant U.S. Trade Representative for Intellectual Property and Innovation at the USTR and the chief U.S. trade negotiator for intellectual property and innovation.

For such a small department, IPEC has had an out-sized influence on shaping U.S. enforcement strategies against online infringement. In 2010, one year after her appointment to lead IPEC, Espinel coordinated a series of meetings among Internet firms and payment providers to create sets of industry-generated best practices to address online infringement. Between 2010 and 2013, she announced a series of informal agreements covering a wide range of Internet services, involving search, payment, advertising, and domain name services (see Table 3.4). Signatories included Google, Microsoft, Visa, PayPal, MasterCard, GoDaddy, Yahoo and American Express.

v) *Agreements in the United Kingdom and European Union*

Around the same time, government officials in the United Kingdom and at the European Commission were also quietly coordinating non-binding agreements. The United Kingdom and the European Commission, along with the United States, are the key state actors in the private anti-counterfeiting regime. They are all strong proponents of intellectual property protection and advocates of informal regulation by industry. The eight private enforcement agreements examined in this dissertation all (except one) emerge from the United States, United Kingdom or by the European Commission.¹³⁷

In the United Kingdom, responsibility for intellectual property is divided between two departments. The first is the Department for Business, Innovation and Skills in which Viscount Younger of Leckie, House of Lords, is the Parliamentary Under Secretary of State for Intellectual Property. The other, which is primarily involved in coordinating the agreements, is the Department of Culture, Media and Sport (DCMS).¹³⁸ Ed Vaizey, Parliamentary Under Secretary of State for Culture, Communications and Creative Industries, within DCMS has responsibility for Internet and creative industries, culture, and broadband spectrum and telecommunications, among other duties. Vaizey began organizing a series of closed-door roundtables with rights holders, trade associations and technology firms in late February 2011.

¹³⁷ The exception is the private enforcement agreement established between the Canadian Anti-Fraud Centre and Visa, which is examined in Chapter. 4.

¹³⁸ The Department for Culture, Media and Sport is known colloquially as the Ministry of Fun.

Chaired by Vaizey, the roundtables discuss a range of issues, including non-binding agreements for payment, advertising and search intermediaries to control infringing sites. Participants include major trade associations: the Federation Against Copyright Theft, British Recorded Music Industry, Motion Picture Association of America, and the Internet Advertising Bureau, which represents the digital-advertising industry in the United Kingdom. Major Internet and telecom firms also participate in the roundtables, including Google, Yahoo, Microsoft, Facebook, Virgin Media and British Telecom. Between 2011 and 2013, Vaizey helped coordinate a code of conduct for search engines and pushed forward a new self-regulatory program for the U.K. digital advertising industry (see Table 3.3).

Table: 3.3: Private Enforcement Agreements

Initiative	Government	Macro-intermediaries
Ad Networks' Statement of Best Practices	U.S. Office of Intellectual Property Enforcement Coordinator	Google, Yahoo, AOL, Bing (Microsoft)
Digital Standards Trading Group (advertising)	U.K. Dept. for Culture, Media & Sport	Google, Yahoo, Bing
Centre for Safe Internet Pharmacies	U.S. Office of Intellectual Property Enforcement Coordinator	American Express, Visa, MasterCard, PayPal, Google, GoDaddy, Yahoo, Microsoft
Payment Account Termination Program	U.S. Office of Intellectual Property Enforcement Coordinator	MasterCard, Visa PayPal, American Express
Payment Account Termination Program	Canadian Anti-Fraud Centre	Visa
Search Engine Code of Conduct	U.K. Dept. for Culture, Media & Sport	Google, Yahoo, Bing
Memorandum of Understanding	European Commission	eBay
Memorandum of Understanding	U.S. Office of Trade Representative	Taobao

In 2009, the European Commission began holding a series of closed-door, industry-only meetings to discuss the online sale of counterfeit goods (see Table 3.3). The Commission argued that voluntary arrangements aimed at counterfeiting and piracy can give industry stakeholders “the flexibility to adapt quickly to new technological developments” (European Commission 2009:10). The Commission offered to act as a facilitator for these meetings, which involved providing administrative and logistical support and “safeguarding, where necessary, a fair balance between all the different interests at stake, including the legitimate rights and expectations of EU citizens” (European Commission 2009:10). By May 2011, signatories had hammered out a deal that was quietly posted online. The agreement sets out general principles for marketplaces and rights holders to work together in cracking down on the sale of counterfeit goods in the European Economic Area (European Commission 2011).

There are commonalities among the eight private enforcement agreements examined in this dissertation. Government officials from the European Commission and in United States and United Kingdom shaped all the private agreements, except one.¹³⁹ Industry stakeholders and government officials created the agreements in closed-door meetings. Consumers were neither consulted nor were their interests fully represented. Government officials used varying degrees of coercion to compel cooperation from the macro-intermediaries. In general, the agreements focus on making enforcement practices more streamlined, more rapid, and more proactive.

vi) *Global Private Regulatory Regime*

To summarise, this chapter demonstrates that multinational rights holders and their trade associations, particularly from the United States, have considerable private authority to shape policymaking in the United States and internationally in relation to the protection of intellectual property rights. These corporate actors also created a compelling narrative of infringement as a serious and economically harmful problem that remains ingrained despite the SOPA

¹³⁹ Note: The Canadian agreement was created by a government agency, the Canadian Anti-Fraud Centre.

protests. Rights holders have an institutional advantage over macro-intermediaries in convincing governments in the United States or European Union to intervene on their behalf and compel cooperation from macro-intermediaries. The states involved in this private regulatory regime play a central role in employing coercive means—threats of legislation and legal action—to secure macro-intermediaries' participation as gatekeepers on behalf of rights holders. These states do so because they have longstanding, socially constructed interests in protecting intellectual property (Drahos and Braithwaite 2002), as well as the economic interests discussed in chapter 1. Further, these states also have strategic security interests in tapping into macro-intermediaries' global regulatory capacity.

As will be explored in the next three chapters, the private anti-counterfeiting regime also demonstrates the complex dynamics of corporate regulation on the Internet. There is a distinct spatial patterning in this regulatory regime with its small group of U.S.-based multinational corporations that dominate the provision of key Internet services. In this environment, it is corporations not governments that have the global reach, technological capabilities and vast data-mining capacity necessary to police infringement in the manner desired by rights holders.

The following chapters examine the eight private enforcement agreements. Chapter 4 analyses private agreements involving payment and advertising macro-intermediaries, while chapter 5 concentrates on search and domain name macro-intermediaries. The *Stop Online Piracy Act* targeted these actors and the private agreements in these chapters incorporate SOPA-like provisions. Chapter 6 examines private agreements among online marketplaces, specifically eBay and Taobao. These actors were not targeted in SOPA but their agreements, which set out informal measures for strengthened, streamlined, and proactive enforcement practices that go beyond what is required by law or judicial rulings, are in the spirit of SOPA.

Chapter 4: Revenue Chokepoints using Payment and Advertising Intermediaries

Payment processing and digital advertising are the lifeblood of commercial websites. By impairing access to these essential services, intellectual property actors have the capacity to “starve” infringing sites of revenue. In the anti-counterfeiting strategies, payment providers endeavour to prevent these sites from receiving illicit revenue from the sale of counterfeit goods. Similarly, advertising platforms work to deter infringing sites from receiving legitimate revenue from advertisements. Proponents of this enforcement strategy approvingly refer to it as establishing revenue “chokepoints” in the online environment that “throttle” unwanted behaviour.¹⁴⁰ This regulatory approach will be familiar to anyone who has examined the U.S. *Stop Online Piracy Act* (SOPA) and *Protect Intellectual Property Act* (PIPA). These bills would have allowed rights holders to obtain court orders requiring payment and advertising intermediaries to withdraw their services from infringing sites and for these intermediaries to take action voluntarily against sites that endangered public health.¹⁴¹ Although the U.S. public soundly rejected SOPA and PIPA, supporters of the bills have quietly introduced similar provisions into private enforcement agreements with payment and advertising macro-intermediaries. These macro-intermediaries, such as PayPal and Google, agreed to withdraw their services voluntarily from infringing sites upon the request of rights holders. The private agreements pertaining to payment and advertising macro-intermediaries, based on non-binding “best practices,”¹⁴² lack the legislative and judicial oversight mechanisms contained within SOPA and PIPA.¹⁴³

¹⁴⁰ Interview with David Wood, Director of Anti-Piracy, British Recorded Music Industry (BPI) Ltd., 12 September 2012, London.

¹⁴¹ PIPA and SOPA, along with the other two failed U.S. intellectual property bills, COICA and OPEN, all proposed that payment providers and advertising platforms should be used to target infringing sites. The bills all proposed voluntary rights of action against sites endangering public health, such as those that sold pharmaceuticals without a valid prescription or pharmaceuticals that are adulterated or misbranded.

¹⁴² These “best practices” are identified and designated as such by industry and do not represent objectively evaluated measures.

¹⁴³ For example, SOPA would have required qualifying plaintiffs to inform the Intellectual Property Enforcement Coordinator of any court orders in which payment or advertising intermediaries fail to comply with a court order requiring them to withdraw services from infringing sites, see: SOPA Sec. 103 (c).

Payment and advertising macro-intermediaries are, as Siân Croxon, a London-based attorney with DLA Piper, observes, “an important part of the armoury in the fight against counterfeits.”¹⁴⁴ Visa, MasterCard, American Express and PayPal dominate the online payment industry. This chapter focuses on Google because it is the most popular search engine globally (with the exception of a few regions) and is also the largest digital advertising platform.¹⁴⁵ Other smaller digital advertising actors that have signed onto these agreements are Yahoo and Bing, Microsoft’s search engine. From the perspective of techno-regulation, these macro-intermediaries control their platforms and services by deploying monitoring technologies to protect their services from violations of their internal policies, including the infringement of intellectual property rights. They have massive, sophisticated programs to detect and remove content (advertising platforms) or sanction users (payment providers). Given their global scope and significant market share, these macro-intermediaries have a tremendous regulatory capacity that state and industry actors can endeavour to tap into.

Rights holders and trade associations working on their own lacked the authority to persuade or compel macro-intermediaries to strengthen their enforcement policies and successfully appealed to government to intervene. Payment and advertising actors have faced various pressures to adopt informal private agreements to regulate online infringement. Chief among these were threats of legislation and legal action from the U.S. and U.K governments. The U.S. Office of the Intellectual Property Enforcement Coordinator (IPEC) and the U.K. Department of Culture, Media and Sport (DCMS), two prominent state actors within the private regulatory regime, directly facilitated the creation of the private agreements. In addition to government coercion, payment and advertising actors faced pressure from rights holders to strengthen their enforcement practices. These macro-intermediaries also have financial and reputational interests in protecting their corporate brands and ensuring that their customers retain confidence in their services.

To explore why and under what conditions payment and advertising macro-intermediaries adopted private enforcement agreements, this chapter examines

¹⁴⁴ Interview with Siân Croxon, Partner, DLA Piper, 14 September 2012, London.

¹⁴⁵ Baidu, for example, is the largest search engine in China.

programs in the United States, the United Kingdom, and Canada. The United States, which is the headquarters of all the macro-intermediaries, hosts the largest number of private anti-infringement agreements because of the work of Victoria Espinel, the former head of IPEC.¹⁴⁶ The U.S. payment-termination program is the largest in the world. Similarly, the United Kingdom's digital advertising industry operates the largest and most comprehensive program worldwide to prevent the placement of advertisements on infringing sites. Finally, the Canadian payment-termination program offers a useful counterpoint to the U.S. program because the former differs markedly in its origins and structure from the U.S. program.

This chapter proceeds as follows. First, it briefly introduces the payment and digital advertising industries before explaining how online payment processing and digital advertising work. Then the chapter explores how these macro-intermediaries became gatekeepers targeting online infringement and describes the creation of the non-binding enforcement agreements that underpin the private regulatory regime. Third, it examines four programs to regulate the online distribution of counterfeit goods. The first two—one in Canada and one in the United States—involve payment providers terminating their services to infringing sites. The others—one in the United States and one in the United Kingdom—are designed to deter the placement of advertisements onto infringing sites. Fourth, the chapter then analyses these programs and, in the fifth section, examines the role of the state and actors' interests. It then offers a brief conclusion.

I) Online Payment and Advertising Industries

Payment providers and advertising intermediaries provide services essential to the functioning and growth of the digital economy. Websites can generate revenue by selling goods and services or selling advertising space on their webpages. Any site interested in generating revenue or donations must have a functional payment processing capacity and offer trusted, well-known payment options. Visa, MasterCard, American Express and PayPal are dominant players

¹⁴⁶ As discussed in Chapter 1, Espinel facilitated five informal agreements between 2010 and 2013 that involve advertising, domain name, payment, and search macro-intermediaries.

within the global online payment industry. While other online payment options exist, most commercial websites depend on at least one of the big four providers to enable their customers to purchase their goods and services.

Visa is the globally dominant payment provider. It controls 72.7% of the debit market and 49.6% of the credit market globally, and processed 92.7 billion transactions in 2012 (Suchman 2013). It is also the most commonly accepted payment method for infringing sites, according to a U.S. law firm's examination of 3,000 websites that U.S. federal courts ordered closed for selling counterfeit goods (RogueFinder 2012). MasterCard and PayPal are also commonly accepted forms of payment on infringing sites, according to the law firm's report. Behind Visa, MasterCard and American Express are large players in the online payment industry, generating 40.1 billion transactions and 5.8 billion transactions respectively in 2012, compared with 9 billion transactions through China's UnionPay, which is another major payment provider (Suchman 2013).¹⁴⁷ PayPal is a major online payment processor with 137 million accounts in 2012 (eBay 2013).

The digital advertising industry is growing rapidly. Online or digital advertising refers to a wide range of ads on social media platforms (e.g., Facebook, Twitter and LinkedIn), mobile devices (e.g., smart phones and tablets), through email and search engine results, and on websites. Rights holders are keenly interested in digital advertising because it is an increasingly important forum in which to advertise their brands. In 2012, spending in the industry reached (in U.S. dollars) \$99 billion globally and the industry predicts that 2013 global spending will reach just over \$113 billion (WPP 2013). Online advertising made up nearly 20% of all advertising globally in 2012 and is experiencing double-digit annual growth (WPP 2013).

The United States and the United Kingdom are both large and fast-growing markets for online advertising. In 2012, spending in the United States accounted for just over \$36.8 billion, with the market in the United Kingdom reaching £5.4 billion (eMarketer 2013). While people think of Google primarily

¹⁴⁷ UnionPay is a network of China-based banks and its credit cards, which are affiliated with Visa, MasterCard or America Express, can be used in most countries worldwide.

as a search engine, it is also the giant of online advertising. It controls about 33% of digital ads globally (eMarketer 2013). Google is also highly dependent on advertising for its revenue and, in 2012, received 95% of its \$50 billion revenue from advertising (Google 2012:12). Far behind Google are other familiar Internet firms: Facebook, with 5% of digital ad revenue; Yahoo with 3%; Microsoft at 1.7%; AOL at 0.9%; and Twitter at 0.5% (Efrati 2013). Facebook and Twitter, which are recent entrants into digital advertising, are rapidly expanding their market share.

The payment and advertising industries are dominated by a handful of U.S.-based firms: Visa, MasterCard, PayPal, American Express and Google. These macro-intermediaries have a considerable capacity to institute and enforce rules governing their networks and platforms. Equally importantly, they also have a significant ability to set rules and standards, which, by virtue of their market share, can influence regulatory practices throughout their industry sectors. When the largest payment providers enact rules prohibiting certain activities, they shape e-commerce activities globally and affect what Internet users can purchase and how they can use payment systems, even with respect to situations where the goods or services in question are legal. PayPal, for example, withdrew its services in 2012 from online publishers that offered what PayPal argued was unacceptable types of erotic content (Charman-Anderson 2012).¹⁴⁸ In situations where payment macro-intermediaries collectively remove their services from sites they contend are engaging in unacceptable activities, the affected sites have few commercial alternatives. Payment macro-intermediaries can essentially cut off actors deemed “bad” from the global online payment system, crippling, possibly fatally, their means of conducting business.¹⁴⁹ This is the essence of governing through revenue chokepoints.

¹⁴⁸ In this case, PayPal withdrew its services from self-publishing and small publishing outlets that offered erotic content including incest, under-age sex, and bestiality. Following an outcry over censorship, in which protesters pointed out that famous works of literature would have been banned under these rules (including Vladimir Nabakov’s *Lolita* and Sophocles’ *Oedipus*), PayPal relented and restored the services (see Charman-Anderson 2012). Unlike the online publishers that regained PayPal’s services after a public protest, other sites may not have the resources or public-interest angle to mount a successful challenge.

¹⁴⁹ There are alternatives to these big payment providers, such as MoneyGram and Western Union. However, both MoneyGram and Western Union have joined the global private regulatory regime targeting infringing sites. These companies are part of the payment-termination program operated by the International Anti-Counterfeiting Coalition, which is discussed later in the chapter (see Montanaro 2012).

Google—as the world’s most popular search engine and the global giant of digital advertising—has a tremendous capacity to shape how individuals access information. As will be discussed in chapter 5, like all search engines Google indexes information from webpages and ranks it according to proprietary algorithms. This means Google selects and prioritises some types and sources of information over others based on a set of closely guarded criteria (Singhal 2012). As a search engine, Google has significant power to filter and control access to information, thus constructing meaning and shaping choices (Elkin-Koren 2001:185; see also, Introna and Nissenbaum 2000; Kohl 2013). As a digital advertiser, Google sells specific terms to advertising intermediaries, which result in relevant advertisements being listed alongside search results. For example, a search on hotels in Bangkok may be accompanied by ads for flights to Thailand. Google can therefore play a key role in structuring the online market of goods and services (see Elkin-Koren 2001:185) as it determines the content and advertisements that users see. Further, critics of Google argue that it prioritises its own services over those of competitors, thus using its power to skew competition in its favour (Kohl 2013:233). Given the sheer scope and commercial power of Google’s services—unprecedented in the Internet age—those who can regulate Google can regulate the Internet (Kohl 2013:233).

i) *How Online Payment Processing Works*

Given the complexity of the online payment and advertising industries, it is necessary to give a brief outline of how sites process payments and how intermediaries deliver ads to sites. For the consumer, Visa, MasterCard and American Express all function in a similar manner. However, there is an important difference that affects how payment providers terminate merchant accounts. Visa and MasterCard operate what is termed an “open-loop” payment system, while American Express operates a “closed-loop” payment system, at least in the United States. An open-loop payment system means that Visa and MasterCard do not issue cards to users or grant merchant accounts to individuals wishing to process commercial payments. “We allow the cardholder sitting in Turkey to do business with a merchant in Germany within a nano-second,” explains Martin Elliott, director of corporate risk management at Visa

International. “What we don’t do is we don’t issue the cards. We don’t sign the merchants. We don’t lend money to folks” (Elliott 2012).

Visa and MasterCard are card associations, which means that they each operate through a network of tens of thousands of formally affiliated and licensed financial institutions globally. Each financial institution affiliated to Visa or MasterCard must adhere to the card association’s rules when offering payment services. Institutions that issue branded payment cards (i.e., a credit/debit card with a Visa or MasterCard logo) are called issuing institutions. Financial institutions that grant merchant accounts that can accept payment by Visa or MasterCard are known as acquiring institutions. Transactions through open-loop payment systems involve multiple intermediaries to process transactions among the cardholder, issuers and acquirers, the card association and the merchant. Visa and MasterCard do not have direct contractual relationships with merchants (i.e., individuals selling goods online). Instead, merchants have contractual relationships with the issuing and acquiring institutions, which, in turn, have direct contractual relationships with Visa and MasterCard.

The closed-loop system, in contrast, is much simpler. These systems are popular among department stores where payment cards are limited to use within a particular store. American Express operates a closed-loop system in which it directly issues payment cards to users and has a contractual relationship with merchants. It processes payments made between cardholders and merchants without a network of financial institutions. To make matters more complex, however, American Express primarily operates its closed-loop system in the United States but outside the United States, it establishes agreements with third-party financial institutions in the American Express network in a manner similar to that of Visa and MasterCard (*Forbes* 2013).

PayPal, meanwhile, operates quite differently from Visa, MasterCard or American Express. It is an online payment system that allows users to transfer funds from various sources, such as bank accounts, credit cards or PayPal accounts to recipients. Users must sign up for a PayPal account. They can then

use PayPal by transferring money into that account or by linking their PayPal account to their bank account or credit card.

Anyone who has purchased goods from a legitimate online retailer has an idea of how online payments work at the consumer's end but there are complex and highly technical transactions behind the checkout page. Imagine purchasing something from your favourite online retailer. You click to the checkout page and enter your payment and shipping information. The site then lists various payment options, Visa, MasterCard, PayPal and American Express. Each of these is called a financial or payment channel. On legitimate sites, each of these payment channels is functional. On infringing sites not all channels may function but may be used to give the appearance of legitimacy.

Table 4.1: Processing Payments Online

Open-loop Process	Closed-loop Process
Cardholder submits card to merchant's system	
1. Merchant's bank asks card association (Visa or MasterCard) to determine issuing bank. 2. Card association's authorization system validates card's security features and forwards to issuing bank for purchase approval. 3. Issuing bank approves purchase. Card association sends approval to acquiring bank. 4. Acquiring bank sends approval to merchant.	1. The merchant's system sends the transaction to American Express. 2. American Express verifies the card and authorises the transaction. 3. American Express sends approval to merchant.
Cardholder completes purchase and receives receipt	

The transaction process varies according to the type of payment you choose (see Table 4.1). If you decide to pay with an American Express card (assuming a closed-loop process), then you enter your payment details and the merchant's system sends the transaction directly to American Express. American Express verifies the card, authorises the transaction and sends approval to merchant. If you pay with Visa or MasterCard, the transaction goes between the

cardholder's issuing bank and the merchant's acquiring bank for approvals before it is processed.

ii) ***How Online Advertising Works***

Even casual Internet users will have encountered multiple types of digital advertising. Ads can be static (simple images or text), animated, or interactive in which the user is invited to play a game or watch a video. Some ads “pop-up” above the webpage that you are viewing, while banner ads that sit within a webpage may be static, or may incorporate video, audio and other interactive elements. Understanding digital advertising can be difficult as the purchase and placement of ads involves transactions through multiple intermediaries. There can be as many as nine different intermediaries depending on the nature of the firms involved in creating, selling and placing advertisements. The industry also increasingly relies upon automated and real-time bidding to purchase and deliver ads to sites in microseconds, similar to the operation of stock exchanges. The complexity of the industry means that it can be difficult to track the distribution of ads and determine how some end up in the wrong place, like a site selling counterfeit goods.¹⁵⁰ Amit Kotecha, a senior mobile and networks manager for the U.K. branch of the Internet Advertising Bureau, the digital advertising trade association, has spent many hours explaining the complexity of digital advertising to rights holders. Most thought “it was a one-to-one relationship between the advertiser and the publisher,” Kotecha says, “when in fact most of the time there are over five relationships or five transactions before it ends up on the site.”¹⁵¹

The most common advertising intermediaries are the advertiser, ad network, ad exchange and publisher.¹⁵² The advertiser (referred to here as the rights holder)

¹⁵⁰ Interview with Amit Kotecha, Senior Mobile & Networks Manager, Internet Advertising Bureau, 8 October 2012, London.

¹⁵¹ Ibid.

¹⁵² There are also several other advertising intermediaries, which are less relevant to the discussion here: agency, demand-side platform, supply-side platform, and agency trading desk. A demand-side platform is a technology platform that facilitates real-time bidding for buyers to purchase space on desirable webpages from multiple ad exchanges and ad networks. Demand-side platforms serve those purchasing ad space, while supply-side platforms help publishers (i.e., websites) manage and sell their available ad space and facilitate their interaction with ad exchanges that, in turn, interact with a demand-side platform. An agency-trading desk is

purchases ads to sell its products. Rights holders generally work with an advertising agency that plans and produces advertising campaigns and advertisements. Ad networks serve as brokers between rights holders producing ads and websites selling space on their platforms. These ad networks determine how much advertising they can sell to sites, contract with rights holders to buy that space and then deliver the ads. Ad networks may represent sites in a particular sector (e.g., health or electronics) or buy access to sites meeting certain criteria (e.g., with certain demographics or recreational interests). Among the largest ad networks are Google AdSense, Yahoo Publisher Network, and AOL Advertising. An ad exchange is a technology platform that facilitates automated, auction-based pricing and real-time buying. Sellers put ads on the exchange and buyers bid for ads similar to “eBay or the stock market.”¹⁵³ Google, Yahoo and Microsoft operate some of the largest ad exchanges in addition to operating large ad networks. Finally, the publisher is the individual website that delivers and disseminates the advertisement. One publisher may deal with thousands or tens of thousands of webpages that end users end up seeing.

II) Pressure on Marketplaces from State and Industry

For proponents of stronger online anti-counterfeiting efforts, the *Stop Online Piracy Act* and its sister bills were essential because the United States does not have a statutory measure to address online trademark infringement. As discussed in chapter 3, Internet intermediaries have adapted notice-and-takedown programs required under the U.S. *Digital Millennium Copyright Act* to deal with rights holders’ complaints related to the trade in counterfeit goods. SOPA would have required advertising and payment macro-intermediaries to act against the online distribution of counterfeit goods and, with the death of SOPA, proponents of stronger enforcement redoubled their focus on private, informal enforcement efforts. In the United Kingdom, neither payment nor advertising intermediaries are required by statute to remove content or disable

software that enables ad networks and advertising agencies to connect to ad exchanges and manages buying.

¹⁵³ Interview with Amit Kotecha, Senior Mobile & Networks Manager, Internet Advertising Bureau, 8 October 2012, London.

services in relation to online trademark infringement.¹⁵⁴ Given this absence of statutory measures, proponents of strong protection for intellectual property emphasised informal, non-legally binding measures and thereby created a private regulatory regime.

Payment and advertising intermediaries have internal policies that prohibit providing services to sites trading in counterfeit goods, as will be discussed in further detail in this and the following sections. Many of these policies predate the private enforcement agreements that payment and advertising providers implemented in 2011 and 2013 respectively. Similar to other industries, companies in the online payment and advertising sectors are subject to an array of domestic laws in countries in which they operate, as well as certain industry-created rules, standards and codes that guide their operations. The ways in which macro-intermediaries regulate infringement depends on the type of revenue stream they facilitate and their degree of interaction with infringing sites. Payment providers facilitate the direct flow of funds to infringing sites by enabling sites to process customers' payments. Payment actors have a direct contractual relationship either with the merchant or with the financial institution that granted the merchant an account. Advertising intermediaries, in contrast, facilitate the indirect flow of revenue through ads placed on sites. Advertising actors may not have a direct relationship as the online placement of advertisements typically involves multiple transactions and intermediaries.

Before discussing how payment and advertising macro-intermediaries regulate infringing sites, the following section explains how they were enlisted as gatekeepers to address infringing sites. The chapter then examines four private regulatory programs: two that terminate payment services to infringing sites and then two that prevent the placement of advertisements on such sites.

¹⁵⁴ In a January 2014 speech during the discussion of an intellectual property bill in the U.K. House of Commons, MP Mike Weatherley recommended that payment and advertising intermediaries should be included in the bill and required to act as gatekeepers to remove illegal content. Prime Minister David Cameron appointed Weatherley as the U.K. intellectual property advisor in September 2013 (Weatherley 2014).

i) ***Regulating Payment Providers***

Prior to their adoption of private enforcement agreements, payment providers governed violations of their policies, including the trade in counterfeit goods, through their internal policies. These policies generally incorporate state laws and industry rules within their terms-of-use contracts that lay out the conditions under which individuals and companies can use their services. These terms-of-use agreements stipulate that individuals cannot engage in any activities while using the services that violate the laws of their country. Visa and MasterCard, for example, state that any transactions "must be legal in both the Cardholder's jurisdiction and the Merchant Outlet's jurisdiction" (Visa 2013). The terms-of-use agreements also outline company- or industry-specific policies regarding the use of their services and penalties for violation, which generally include restricted access to services or termination of services (Visa 2013).

Payment macro-intermediaries have a history of working for states against a range of wrongdoing since at least the early 2000s. In the United States, for example, Visa, MasterCard, PayPal and American Express have worked with federal and state authorities to track and block online payments in relation to commercial child pornography sites, Internet gambling sites, and the distribution of illicit drugs (MacCarthy 2010). A 2005 agreement among payment providers and U.S. state attorneys general to tackle online sales of tobacco aptly illustrates how governments can use non-binding agreements with the private sector to further public policy goals. In 2005, state authorities complained of online tobacco retailers selling tobacco without verification of the buyer's age and without reporting tax (see Ribisl et al. 2011). Enforcement of these violations, however, was difficult and unsuccessful (see MacCarthy 2010; Ribisl et al. 2011). To address this problem, federal and state authorities requested Visa, MasterCard, PayPal and American Express to prohibit payment processing for sites that did not meet state requirements, and the providers agreed (MacCarthy 2010).

Public health researchers lauded the resulting non-binding agreement among payment providers as "landmark" and an official from the Bureau of Alcohol, Tobacco and Firearms observed that industry "cooperation" was "completely

voluntary” (Green Sheet 2005). By shifting enforcement responsibility to intermediaries, federal and state officials effectively extended their regulatory reach to undertake the first national effort to address the illicit online distribution of tobacco (Ribisl et al. 2011).¹⁵⁵ To encourage cooperation from payment providers, for example, forty-two state attorneys general warned the providers that they believed federal and state laws on tobacco were being violated and requested they take measures to address these violations (MacCarthy 2010:1084). By pointing to the violation of laws and urging specific action, these attorneys general emphasised the potential of payment providers being held accountable for facilitating criminal activity. Thus, the tobacco agreements clearly illustrate the inherently coercive nature of this type of “voluntary” industry initiative. This case also demonstrates how states can extend their regulatory reach by working through Internet intermediaries, as well as capitalizing upon their specialised technological expertise to monitor and control massive numbers of financial transactions.

ii) ***Payment Providers’ Informal Agreements***

Payment providers drafted and adopted their informal agreements in closed-door meetings. As a result, it is difficult to determine with any precision when intellectual property actors first proposed that payment macro-intermediaries should regulate infringing sites voluntarily. In September 2009, however, the International Trademark Association (INTA), an influential New-York-based lobbying body for rights holders,¹⁵⁶ released what it termed “voluntary best practices” for Internet intermediaries to address online infringement (see INTA 2009).¹⁵⁷ INTA’s practices represent “a middle ground as to how to deal with this problem that was acceptable to everybody,” recalls Candice Li, external relations manager dealing with anti-counterfeiting policies at INTA.¹⁵⁸ “We

¹⁵⁵ Separate non-binding agreements were also struck in 2005 between the federal government and private shipping firms, specifically United Parcel Service, FedEx and DHL (Ribisl et al. 2010).

¹⁵⁶ INTA performs what it calls “policy-advocacy” work, which involves lobbying, awareness raising and policy development, and making recommendations on legislation and trade agreements, including the the Anti-Counterfeiting Trade Agreement. Interview with Candice Li, External Relations Manager, Anti-counterfeiting, International Trademark Association, 3 April 2012, New York City.

¹⁵⁷ INTA also proposed best practices for search engines and marketplaces (see INTA 2009).

¹⁵⁸ Interview with Candice Li, External Relations Manager, Anti-counterfeiting, International Trademark Association, 3 April 2012, New York.

couldn't just go ahead and say companies like eBay are fully responsible for doing everything." For payment providers, one of INTA's key recommendations was that they consider merchant-account terminations.¹⁵⁹ Visa, MasterCard, PayPal and American Express all agreed to these practices, which were the first to outline how rights holders should work with payment providers to deal with online infringement. In contrast to the 2011 private agreement, INTA's practices focused on creating awareness of the problem of counterfeit goods and establishing lines of communication between rights holders and intermediaries (INTA 2009).

In terms of intellectual property enforcement, payment providers have worked with law enforcement agencies and rights holders since the early 2000s in relation to sites that provide copyright-infringing versions of music and movies. However, rights holders were unable to convince payment providers to adopt tougher enforcement measures to deal with infringing sites, as the next section explores. Prior to payment providers' agreements in 2011, their enforcement efforts were relatively uncoordinated and unstructured. Linda Kirkpatrick, a senior executive with MasterCard, recalls that before the U.S. government-facilitated enforcement agreement, payment providers had a "different fragmented approach to attacking the problem" and "no formal process for addressing inquiries" (Kirkpatrick 2012). For payment providers, it took direct pressure from the U.S. and U.K. governments for them to implement formalised, systematic processes to terminate infringing sites' merchant accounts on behalf of rights holders.

The first instance of an informal private agreement in relation to intellectual property was around 2009 with the City of London Police in the United Kingdom. The City of London Police, which undertakes law enforcement duties within the three-kilometre square area covering London's financial district, has responsibility to addressing financial crime, including intellectual property rights crime. At the time, officers with the City of London Police and rights holders were working together to stop multiple Ukraine-based sites that allowed users to

¹⁵⁹ INTA suggested that payment providers may "choose" to terminate services to infringing sites or issue other sanctions, which suggests a flexibility in sanctions that is not evident in private agreements agreed to by payment providers in 2011 (see INTA 2009).

download copyright-infringing music for a small fee.¹⁶⁰ The U.K. police had no jurisdiction over the sites and so rights holders asked Visa and MasterCard to terminate the sites' merchant accounts voluntarily. The payment providers, however, were somewhat reluctant as they can face legal liability for removing payment services without cause. Visa, in particular, was understandably hesitant as, in 2006, Visa withdrew its services from an allegedly infringing site that then successfully sued Visa in a Russian court (Yee 2011).¹⁶¹ In response to the providers' resistance to voluntary action, officers from the City of London Police sought legal advice and informed the providers they could lay criminal charges against the providers if cooperation were not forthcoming. Det./Supt. Bob Wishart, who worked on the case, said he told the payment providers:

Look, you are effectively supporting these sites. We're telling you that they are illegal. [...] We're telling you that from here on in everything that you earn out of these sites is potentially proceeds of crime. We're putting you on notice.¹⁶²

Given that incentive, "MasterCard stepped up to the plate straight away," Wishart recounts but Visa was "slightly more reluctant."¹⁶³

In the United States, the private regulatory regime was created in an environment where the threat of legislation hung over meetings between macro-intermediaries and Victoria Espinel, head of the U.S. Office of the Intellectual Property Enforcement Coordinator (IPEC). Beginning around November 2010, Espinel facilitated a series of meetings among Internet firms and payment providers. The purpose of these meetings was to create a series of informal private agreements to address online infringement. Espinel learned of the City of London's arrangement with payment providers when she was appointed as head of IPEC in 2009.¹⁶⁴ At the same time that Espinel was in negotiations with the payment macro-intermediaries, the U.S. Congress was debating two intellectual property bills: the *Combating Online Infringement and Counterfeits*

¹⁶⁰ Interview with Det./Supt. Bob Wishart, Head of National Operational Delivery, Regional Fraud Project, City of London Police, 6 September 2012, London.

¹⁶¹ The Russian court ordered the payment provider to restore the site's payment services (see Yee 2011).

¹⁶² Interview with Det./Supt. Bob Wishart, Head of National Operational Delivery, Regional Fraud Project, City of London Police, 6 September 2012, London.

¹⁶³ Ibid.

¹⁶⁴ Ibid.

Act (COICA) and the *Protecting Intellectual Property Act* (PIPA). The U.S. Senate introduced COICA in September 2010 and then replaced it with PIPA in May 2011.

Just one month after the introduction of PIPA, in June 2011, Espinel announced that MasterCard, PayPal, Visa and American Express agreed to non-binding principles to terminate the merchant accounts of infringing sites (IPEC 2011). The agreements, which were not released publicly, outline a series of guidelines to make payment providers' enforcement measures more coordinated and streamlined (see Appendices B and C).¹⁶⁵ Provisions in the agreements echo COICA and PIPA as they encourage payment providers to remove their services voluntarily from infringing sites.¹⁶⁶ These private enforcement agreements form the basis of the private anti-counterfeiting regime. As will be discussed later in the chapter, the International Anti-Counterfeiting Coalition drew upon these best practices when it worked with IPEC to create its payment termination program.

iii) ***Regulating Advertising Platforms***

Advertising intermediaries' adoption of private enforcement agreements to regulate infringing sites has similarities with the experiences of payment providers. The U.K. government warned the digital advertising industry to implement its regulatory program quickly or face legislation.¹⁶⁷ In addition to government pressure, rights holders pushed the advertising industry to strengthen its enforcement practices. In advertising, rights holders play a key role in demanding and shaping regulation as they spend considerable sums to craft a certain image of their brand. They not only want their brands to end up

¹⁶⁵ The agreements negotiated by IPEC are not widely available. A law professor in the United States unsuccessfully filed a freedom of information request to IPEC to obtain information about the informal agreements with the payment providers. The Office of Management and Budget, which includes IPEC, denied the request citing trade secrets, privileged or confidential information. Fortunately the International Anti-Counterfeiting Coalition provided the information to the lawyer who shared the two best practices documents with me.

¹⁶⁶ Although the payment providers' agreement preceded the introduction of SOPA, which came in October 2011, I argue that the agreements are "SOPA-like" because of the agreements' similarity to provisions in PIPA, which strongly resembles SOPA.

¹⁶⁷ This is according to minutes from the Search Roundtable Discussion with Rights Holders and Search Engines in November 2011 between trade associations, Internet intermediaries and the U.K. Department for Culture, Media and Sport obtained by the U.K. Open Rights Group through a freedom of information request (Bradwell 2011).

on legitimate, non-infringing sites, but rights holders also want their brands to be represented on sites that meet certain criteria. The Interactive Advertising Bureau, for example, sets out guidelines for rights holders to avoid placing advertisements on sites with content relating to pornography, tobacco, illicit drugs or violence (see IAB 2013). Rights holders campaign strongly against misplaced advertisements because the public relations from “one bad story could ruin a brand for a very long time,” says Amit Kotecha at the Internet Advertising Bureau.¹⁶⁸

In fact, rights holders’ fear of damage to their brands was the impetus for regulation of the digital ad industry in the United Kingdom in 2005. In that year, the U.K. television program *Panorama* ran a documentary that exposed how the advertising industry inadvertently placed advertisements on some websites with illegal and controversial content.¹⁶⁹ “We are talking about some pretty grim websites,” recounts David Ellison, marketing services manager for the advertising trade association, Incorporated Society of British Advertisers (Ellison 2012).¹⁷⁰ The sites were “at best distasteful and on the wrong end of the morality scale, and at worst highly illegal” (Ellison 2012). While the documentary outraged rights holders, “it was really good for the industry because all of the legitimate ad networks got together,” explains Kotecha. They “said what are we going to do about this? Our business is at threat because we don’t want all this money to go away.”¹⁷¹ The result was a voluntary code called the Internet Advertising Sales House (IASH), which certified ad networks as ‘brand safe’.¹⁷² Ad networks vetted every website they represented and allowed rights holders to choose whether or not they would place their ads on sites that have content dealing with sexual content, alcohol or violence.¹⁷³ Rights holders could select the types of sites they approved for their advertisements:

They were given this blue box on their order form and they could tick whatever classification – adult, etc. They could also tick whether they wanted ‘vetted’ or ‘non-vetted.’ Vetted means that it was totally brand

¹⁶⁸ Ibid.

¹⁶⁹ Ibid.

¹⁷⁰ Some of these sites contained videos of illegal boxing or street-fighting matches. Ibid.

¹⁷¹ Ibid.

¹⁷² Ibid.

¹⁷³ Ibid.

safe. Non-vetted would mean that it would not be on a porn site where there is a list of stuff but the content hasn't been checked in advance.¹⁷⁴

The industry code was popular with rights holders. Those with the biggest accounts, like British Airways decided that they “only want[ed] to buy from the ad networks that have been certified by the industry.”¹⁷⁵

As the digital advertising industry evolved, other types of intermediaries emerged, particularly ad exchanges. Ad networks, which serve as brokers between rights holders and sites, were covered by the IASH industry code. Ad exchanges, which are technology platforms that buy and sell ads in real time, were not. The underlying purpose of the regulatory regime—and a key demand of rights holders—was to expand the Internet Advertising Sales House to cover the whole industry. Rights holders “fund the whole industry and everyone has to meet those demands,” Kotecha explains.¹⁷⁶ The new non-binding agreement—the subject of one of this chapter's advertising case studies—is the Digital Trading Standards Group (DTSG). The digital advertising industry, as described earlier, began creating the DTSG in 2011 to adjust for evolution in the industry. Government pressure forced the industry to rapidly develop and implement the DTSG in late 2013. The important difference between the previous IASH program and the DTSG is that the latter covers all intermediaries involved in the online placement of advertisements. In addition, as will be explored later in the chapter, the DTSG uses an industry-generated blacklist that helps advertisers avoid placing ads on infringing sites.

The process of creating the Digital Trading Standards Group was complex as it involves multiple advertising exchanges, as well as trade associations representing the advertising industry and those for rights holders, particularly the Federation Against Copyright Theft and the British Recorded Music Industry.¹⁷⁷ These latter trade associations, along with the Internet Advertising Bureau, repeatedly met with Ed Vaizey, the U.K. Parliamentary Under-Secretary for Culture, Communications and Creative Industries, at the Department of Culture, Media and Sport, to update the government on the

¹⁷⁴ Ibid.

¹⁷⁵ Third-party auditors certified participating ad networks. Ibid.

¹⁷⁶ Ibid.

¹⁷⁷ Ibid.

progress of the DTSG. On behalf of rights holders' trade associations, Minister Vaizey pushed the advertising industry to "fast-track" the agreement while in meetings with industry stakeholders.¹⁷⁸ This pressure forced the industry to develop the agreement "really quickly" because the government wanted a process in place in 2013.¹⁷⁹ While government pressure was not responsible for the creation of the DTSG, direct pressure from government officials hastened its implementation and the threat of legislation hung over the industry if it did not make sufficient progress. Kotecha explains:

They really believe in self-regulation. [...] The last thing they want to do is legislate. We definitely don't want that. It just leads to this black hole. We don't know when they are going to legislate again. They could just push something through. If they do it once, they can do it again.¹⁸⁰

iv) *Advertising Platforms' Informal Agreements*

In the United States, the digital advertising industry also faced the threat of legislation in the form of COICA, PIPA and the *Stop Online Piracy Act*. In addition to these bills, the largest digital advertising actor—Google—faced criminal charges from the U.S. Department of Justice for facilitating infringement in relation to so-called "illegal" online pharmacies, as will be discussed later in this section (DOJ 2011). Even before the introduction of COICA in 2010, the U.S. digital advertising industry had policies in place that prohibited the placement of ads on sites with illegal or what the industry determined to be "inappropriate" content (see IAB 2013). Despite these measures, advocates of tougher enforcement measures argued that legislation was necessary to address the problem of legitimate advertisements on infringing sites (Espinel 2011a).

U.S. legislators and policymakers made their preferences clear for more action from the digital advertising industry. Ads "hel[p] these sites obtain legitimacy

¹⁷⁸ This is according to minutes from the Online Infringement of Copyright Roundtable in February 2012 between trade associations, Internet intermediaries and the U.K. Department for Culture, Media and Sport obtained by the U.K. Open Rights Group through a freedom of information request (Bradwell 2012).

¹⁷⁹ Interview with Amit Kotecha, Senior Mobile & Networks Manager, Internet Advertising Bureau, 8 October 2012, London.

¹⁸⁰ Ibid.

and confuse the public,” argued Victoria Espinel, head of IPEC in testimony to a Judiciary Subcommittee in the U.S. House of Representatives in 2011, and also provide sites “a source of revenue” (Espinel 2011a:48). The U.S. Congressional International Anti-Piracy Caucus went a step further. In letters to the top three U.S. advertising associations in October 2011, members called upon the digital advertising industry to choke off revenue to sites involved in distributing infringing goods (Sandoval 2011).¹⁸¹ Direct state pressure, similar to the situation of the payment providers and U.K. advertising actors, underlies the private agreements with the U.S. advertising (see Table 4.2).

Between 2010 and 2013, Espinel held a series of meetings with Google, Yahoo and Bing about how they could better regulate their advertising services (IPEC 2013). In the background to these discussions, the U.S. Congress introduced COICA, PIPA and SOPA, which, as discussed in chapter 3, would have required advertising intermediaries to withdraw their services from infringing sites. The result of Espinel’s negotiations was three best practices-based agreements: one that focuses on so-called illegal online pharmacies and two that address advertisements on infringing sites in general (see Table 4.2).

Table 4.2: U.S. Informal Agreements with Advertising Actors

Agreement	Actors
Centre for Safe Internet Pharmacies (2010)	Google, Yahoo, Bing (American Express, MasterCard, PayPal, Visa, GoDaddy)
Advertising associations’ best practices (2012)	American Association of Advertising Agencies, the Association of National Advertisers, Interactive Advertising Bureau
Ad networks’ best practices (2013)	Google, Yahoo, Bing

The first agreement, announced in December 2010, three months after the introduction of COICA, brought together multiple actors to create the Centre for

¹⁸¹ Members of the Congressional International Anti-Piracy Caucus called for action from the American Association of Advertising Agencies, the Association of National Advertisers, and the Interactive Advertising Bureau (Sandoval 2011).

Safe Internet Pharmacies.¹⁸² In this agreement, advertising actors would remove advertisements from and prevent advertising from being placed on sites that sold pharmaceuticals in violation of U.S. federal and state laws (IPEC 2011). For reasons of space, this dissertation does not examine the role of advertising macro-intermediaries in relation to the Centre for Safe Internet Pharmacies but instead focuses in chapter 5 on the domain registrar GoDaddy's regulatory efforts in regards to this agreement.

The other two informal agreements relate specifically to advertising associations and advertising networks. In May 2012, the largest advertising associations in the United States announced a shared statement of best practices that would guide their members' policies. The Association of National Advertisers, the American Association of Advertising Agencies and the Interactive Advertising Bureau set out best practices to urge their members to avoid placing advertisements on infringing sites (ANA 2012). This agreement set the tone for the U.S. digital advertising industry as these associations represent the majority of U.S. firms involved in advertising.

Just over a year later in July 2013, a group of U.S.-based ad networks announced a similar set of best practices (Ad Networks 2013). Signatories to the agreement were Google, Bing, AOL and Yahoo and prominent advertising firms 24/7 Media and Condé Nast. It is this latter agreement—the ad networks' agreement—that is the chapter's second advertising case study. While the ad networks' agreement introduced guidelines to direct how advertising intermediaries addressed infringing sites, Google, Bing and Yahoo already had enforcement policies in place. The private agreements formalised but did not substantially alter their enforcement practices, as is discussed in the next section.

Like the payment macro-intermediaries, the advertising actors—Google, Yahoo and Bing—adopted informal agreements with provisions similar to those proposed in PIPA and SOPA. In both the United States and the United

¹⁸² Discussions between IPEC and these actors began in the autumn of 2010, with a cross-industry meeting in November 2010 and the agreement in December 2010. The Centre achieved non-profit status in 2012 (IPEC 2011; Clifton 2012).

Kingdom, advertising macro-intermediaries negotiated private agreements in the shadow of legislation. Google, however, faced additional coercive pressure in the form of criminal charges from the U.S. Department of Justice. While Google was in talks with Victoria Espinel about strengthening its advertising policies, Google was under investigation that it accepted ads from so-called “illegal” online pharmacies (see DOJ 2011).¹⁸³ In 2011, Google settled the case by forfeiting \$500 million, one of the largest forfeitures in the United States (DOJ 2011). This case indicates the importance of digital advertising and the concern with which the U.S. pharmaceutical industry and, more broadly, the U.S. government, views the protection of intellectual property relating to pharmaceuticals, as is explored in greater detail in chapter 5.

To summarise, the U.S. and U.K. governments exerted direct coercive pressure on payment and advertising macro-intermediaries to compel their involvement in private enforcement agreements. These agreements are the basis of a global private regulatory regime that relies upon state authority. The coercive conditions under which these states created the agreements, and therefore the regime, demonstrate the mutually aligned interests of rights holders and the U.S. and U.K. governments. As the next section explores, the regime’s mode of regulation is through technology: macro-intermediaries are responsible for monitoring their platforms and removing content and services related to the distribution of counterfeit goods. Macro-intermediaries’ ability to shape compliance by withdrawing services or altering how individuals can use their platforms makes them valuable gatekeepers.

III) Intermediaries’ Enforcement Programs

Having established how key payment and advertising actors signed onto private enforcement agreements, the chapter turns to explain the ways in which they police infringing sites. Advertising and payment intermediaries facilitate different

¹⁸³ The issue of online pharmacies is complex and controversial, as will be discussed in chapter 5. Federal and state authorities in the United States impose strict conditions on the types of online pharmacies that can legally serve U.S. consumers and how they can operate. As a result, cheaper medication from foreign, often Canadian-based online pharmacies may violate these rules but supply genuine branded or generic medication. Thus, not all online pharmacies operate in accordance with U.S. laws but they do not all supply counterfeit or misbranded pharmaceuticals.

types of revenue for their clients: advertisements allow infringing sites to generate legitimate revenue, while selling counterfeit goods produces illicit funds. These intermediaries also have different relationships with rights holders. The advertising industry exists to promote products and services while payment providers, in contrast, enable financial transactions among all parties.

i) ***Payment Intermediaries' Enforcement Policies***

Payment providers operate through a series of contractual agreements (different from the non-binding private enforcement agreements). These agreements involve cardholders, acquirers, issuers, card associations, and merchants. The policies lay out how users and merchants can use the services, what activities are unacceptable, the responsibilities of issuing and acquiring financial institutions and the penalties for violating policies. Rights holders and their trade associations refer to these contractual agreements as a “legal lynchpin” (Montanaro 2012a) because they provide the authority for providers to terminate the merchant accounts of infringing sites anywhere in the world.

Violation of these policies can result in a range of sanctions. Payment providers may suspend or terminate a user's account and levy fines on acquiring banks that fail to detect or deal adequately with merchants operating infringing sites (American Express 2013). These fines are incentives for acquiring banks to ensure they do not grant merchant accounts to individuals involved in selling illegal goods. Bob Barchiesi, president of the International Anti-Counterfeiting Coalition, comments that fines are “the hammer that the credit cards have over” their network of licensed financial institutions (Barchiesi 2012).

Payment providers have notice-and-termination policies that predate their participation in private enforcement agreements. The process for terminating merchant accounts is relatively straightforward. Visa, MasterCard and American Express have similar procedures (American Express 2011; MasterCard N.d.):

- 1) Rights holders (or their authorised agents) provide contact information and evidence of ownership of the trademark/s in question.¹⁸⁴
- 2) Rights holders describe the alleged infringement and capture a screenshot of the site showing the product/s for sale.
- 3) They note the web address of the site selling infringing products.
- 4) They provide evidence of payment methods by capturing a screenshot of the site's checkout page.
- 5) They attest that the merchant is not authorized to sell the products in question (e.g., the merchant is not an authorized re-seller).
- 6) They provide evidence that they have notified the website operator of the infringement, for example cease-and-desist letters.
- 7) They attest that the information is accurate and complete with statements made in good faith.

Once the payment providers receive the complaint, they identify the acquiring bank that granted the merchant account. Visa and MasterCard require the acquiring bank to respond within two business days if law enforcement has initiated the complaint and within five business days for rights holder-generated complaints (MasterCard N.d.). Acquiring banks must conduct an investigation and terminate the merchant agreement and account if warranted. If the bank decides termination is not necessary, Visa and MasterCard demand, in the words of MasterCard, that acquirers provide "provide compelling, written evidence disproving the violation" (MasterCard N.d.).

PayPal's process for account termination is simpler as it does not operate through a network of acquiring financial institutions. PayPal's internal security unit and third-party online monitoring firms "crawl the Internet looking for key words, indicators and PayPal brands and references."¹⁸⁵ If violations of PayPal's policies are identified, PayPal conducts an investigation. "[I]f we detect behaviour in violation of our terms the PayPal account is restricted," says Julie Bainbridge, senior brand protection manager with PayPal.¹⁸⁶ PayPal then sends

¹⁸⁴ Authorised agents include trade associations that undertake enforcement efforts, attorneys or private investigative or brand-monitoring firms.

¹⁸⁵ Personal interview Julie Bainbridge, Senior Brand Protection Manager, PayPal, 1 July 2012, by Skype.

¹⁸⁶ Ibid

an email to the user saying the account is restricted because of a violation and that the merchant can no longer accept payment by PayPal.

ii) ***Payment Providers' Private Enforcement Agreements***

Payment providers' enforcement agreements set out broadly worded principles for working with rights holders and terminating merchant accounts. Although these agreements have not been publicly released, I obtained copies (see Appendices B and C).¹⁸⁷ The agreements require rights holders to coordinate their complaints of infringement by working through associations like the International Anti-Counterfeiting Coalition (see Appendix C). According to the agreements, rights holders should also develop, in cooperation with payment providers, "a common form or system" and standardized coding to categorize types of infringement (see Appendix C). The agreements also contain references to safeguards. The guidelines recommend that payment providers have a clearly identified complaint mechanism and point of contact for complainants. Importantly, they should also have a process to allow a "prompt review" if merchants dispute the allegations and allows providers flexibility in issuing sanctions (see Appendix B).

Overall, these enforcement agreements are intended to transform payment providers into gatekeepers with the technological capacity to process mass numbers of complaints in a rapid, streamlined manner for rights holders. These agreements form the basis of how Visa, MasterCard and PayPal work with the International Anti-Counterfeiting Coalition, which is explored in greater detail below.

iii) ***Account Termination Programs***

Beginning in 2011, rights holders, trade associations and government actors in the United Kingdom, the United States, and Canada, working in cooperation with payment providers separately created several merchant-account

¹⁸⁷ As discussed earlier, the International Anti-Counterfeiting Coalition shared these two agreements (one four-page agreement, dated May 2011, and one two-page agreement, dated July 2011) with a U.S. lawyer who shared them with me (see Appendices B and C).

termination programs. These programs vary in scope, degree of law enforcement involvement, and payment actors but have broadly similar operations. In the United Kingdom, several music trade associations work with the City of London Police in a partnership that began with a threat of criminal charges, as discussed earlier.¹⁸⁸ There are also several other smaller programs run by brand-monitoring firms and trade associations as merchant-account termination is a growing area of interest for brand-protection firms.¹⁸⁹

In addition to these programs, there are also two, well established programs operating in North America, one in the United States and the other in Canada, which form this chapter's payment case studies. The U.S. program targets sites distributing counterfeit and copyright-infringing goods. The Canadian program concentrates solely on counterfeit goods. The principal difference between the programs is the U.S. program has no direct participation from law enforcement or government agencies while the other is operated by a law enforcement agency on behalf of Canadian rights holders. Studying these programs provides an ideal opportunity to examine the role of government in the creation of each.

a) International Anti-Counterfeiting Coalition Program

The International Anti-Counterfeiting Coalition (IACC), based in Washington D.C., launched its program in January 2012. The program directly emerged from the best practices agreement that Victoria Espinel, the head of IPEC, coordinated among payment providers (IPEC 2012). Building upon this agreement, the IACC signed memoranda of understanding with multiple payment providers, including Visa, MasterCard, PayPal and American Express. Rights holders participating in the program can make complaints in three

¹⁸⁸ In mid-2011, the International Federation of the Phonographic Industry (IFPI), the British Recorded Music Industry (BPI) and the City of London Police joined forces with MasterCard, Visa and PayPal (IFPI 2013). Investigators from IFPI and BPI identify sites they allege are offering copyright-infringing content and forward the information to the police, which request that the payment providers withdraw their services (IFPI 2013).

¹⁸⁹ In my interviews, I identified a similar merchant-account termination program operated by a U.K. trade association and one operated by a U.K. brand monitoring firm.

categories: 1) counterfeit goods; 2) digital-copyright infringement; and 3) circumvention devices (Montanaro 2012).¹⁹⁰

Bob Barchiesi, IACC president, explains the program's goal is to "create a streamlined, simplified procedure" for rights holders to submit complaints "to credit card networks across multiple platforms" (Barchiesi 2011). The IACC's program, called "RogueBlock," allows IACC members to submit complaints electronically to the IACC. The IACC reviews all complaints, employs analysts to conduct trace messaging¹⁹¹ to determine the relevant acquiring bank, and then sends complaints directly to the relevant payment providers for account termination (Montanaro 2012). The program is available to any member of the IACC or its affiliated members who pay the program's annual fee. Participants can submit a maximum of 25 URLs per calendar month, which "limits the brand owner to really pick the cream of the crop cases," explains Kristina Montanaro, director of special programs for the IACC and manager of the program.¹⁹²

b) Canadian Anti-Fraud Centre Program

The Canadian Anti-Fraud Centre (CAFC) is a law enforcement agency in North Bay, Ontario that works with the public, law enforcement agencies, and the private sector to address and deter fraud.¹⁹³ Its merchant-account termination program is the creation of Barry Elliott, who is head of the analysis section of the CAFC and a retired member of the Ontario Provincial Police's Anti-Rackets Branch. Elliott launched the program in 2011—it predates the IACC's program—and says that it is based upon his long-time professional relationship with Visa through their partnership in fraud investigations. Elliott explains that the program's strategy is "to go for the throat and to take away the ability of the

¹⁹⁰ Circumvention devices refer to hardware or software that breaks rights holder-imposed digital locks, such as those that confine an e-book to a particular e-reader or a video game to a particular device.

¹⁹¹ Trace messaging involves tracking a payment transaction to identify the merchant account's acquiring bank so that the payment provider (e.g., Visa) can request that the relevant bank investigate the merchant account.

¹⁹² Interview with Kristina Montanaro, Associate Counsel, Director of Special Programs, International Anti-Counterfeiting Coalition, 24 April 2012, Washington.

¹⁹³ The Canadian Anti-Fraud Centre is jointly managed by the Royal Canadian Mounted Police (federal law enforcement), Ontario Provincial Police, and the Competition Bureau Canada (federal regulatory agency). Visa is a key partner.

merchants to make money.”¹⁹⁴ There are several important differences between the CAFC and IACC programs. The CAFC works exclusively with Visa and solely targets sites selling counterfeit versions of Canadian rights holders’ products.¹⁹⁵ “If you target Canada, we’ll take your merchant account,” Elliott says.¹⁹⁶ The CAFC acts upon complaints received from rights holders and, in contrast with the IACC program, the CAFC also receives complaints from consumers. Rights holders can also pay to submit a thousand sites annually to the CAFC rather than the 300 permitted by the IACC.¹⁹⁷

Although the CAFC operates the merchant-account program, it does not verify that the sites are selling counterfeit goods but instead relies upon rights holders to make that determination. “If the company says that the site is unauthorized, we cut the merchant account,” explains Elliott. “Civil liability falls on the company.”¹⁹⁸ The CAFC’s program is rather unusual as it operates by employing undergraduate criminology students from the local university, Nipissing University. The CAFC supervises the students and trains them to process complaints and conduct trace messaging.¹⁹⁹ Nipissing University administers rights holders’ fees and pays the students’ wages because the CAFC cannot charge or receive money for its services as a non-profit association.²⁰⁰

iii) ***Advertising Intermediaries’ Enforcement Policies***

Regulating the placement of ads in the digital advertising industry is even more complex than identifying and targeting infringing sites’ merchant accounts. Underlying the digital ads we see everyday are technical and highly complex systems that classify content. Some topics are highly regulated—or outright

¹⁹⁴ Interview with Barry Elliott, Criminal Intelligence Analytical Unit, Canadian Anti-Fraud Centre, North Bay, Ontario, 27 June 2012, by telephone.

¹⁹⁵ In contrast, the IACC program works with multiple payment providers and operates on behalf of rights holders anywhere worldwide.

¹⁹⁶ Interview with Barry Elliott, Criminal Intelligence Analytical Unit, Canadian Anti-Fraud Centre, North Bay, Ontario, 27 June 2012, by telephone.

¹⁹⁷ Interview with Barry Elliott, Criminal Intelligence Analytical Unit, Canadian Anti-Fraud Centre, North Bay, Ontario, 27 June 2012, by telephone.

¹⁹⁸ Ibid.

¹⁹⁹ The students’ trace-messaging analysis identifies the acquiring bank in a transaction that Visa can trace but as the students do not have access to payment providers’ data like the IACC program, Visa must identify the acquiring bank.

²⁰⁰ Interview with representative from Nipissing University, 12 July 2012, by Skype.

prohibited—on many advertising platforms, such as pornography, weapons, hate speech, tobacco and illicit drugs. Other topics may vary according to a particular country's policy on the subject, such as alcohol, abortion and gambling. Some taboo topics are surprising and idiosyncratic to the company. Google, for example, forbids ads for 'secret' paternity tests.²⁰¹ Advertising intermediaries institute these policies because rights holders have repeatedly expressed their concern that their ads could be placed on sites that offer illegal or inappropriate content that may negatively affect their brands. For example, an industry-run survey of marketing managers in the U.K. found that they are most concerned about their ads ending upon on pornographic sites (Digital Strategy Consulting 2013).²⁰² After pornography, marketing managers were most concerned about sites linked to terrorism and then those offering infringing content.

The online advertising industry regulates the content and placement of ads through a series of best practices agreements and internal policies. Some of these rules echo state regulations that limit advertising, for example, on tobacco products or alcohol, while others reflect rights holders' demands to avoid controversial or unwanted content (IAB 2013). The major advertising trade associations in the United States and the United Kingdom all have policies that recommend advertising intermediaries not place ads on infringing sites (ANA 2012; IAB 2013). Advertising actors like Google, AOL, Yahoo and Bing explicitly prohibit ads for counterfeit goods (Bing N.d).

iv) *Advertising Intermediaries' Enforcement Programs*

As introduced earlier, there are two non-legally binding regulatory programs in which advertising macro-intermediaries work to control advertising practices in relation to infringing sites—one in the United States and the second in the United Kingdom. Depending on the services they offer, advertising intermediaries are responsible for both preventing the placement of legitimate

²⁰¹ For a list of Google's AdWords Restricted Products and Services, see: <http://support.google.com/adwordspolicy/bin/topic.py?hl=en&topic=1308252>.

²⁰² The survey, conducted on behalf of Project Sunblock, a company that offers brand-protection services, was of 268 senior marketing decisions makers at mid-sized (50-500 people) UK brands (Digital Strategy Consulting 2013).

ads on infringing sites and removing ads for counterfeit goods (i.e., ads that direct consumers to sites selling counterfeit products). For the latter effort, Google, Yahoo and Bing operate notice-and-takedown programs that allow rights holders (or their authorized representatives) to complain about specific ads. These notice-and-takedown provisions, however, are only for ads. If rights holders want to complain about a search result (e.g., from Google or Yahoo) that links to an infringing site, they can file a notice of infringement to the relevant search engine to have that link de-indexed from the search results, as will be discussed in chapter 5.

a) Ad Networks' Private Enforcement Agreement

In July 2013, a group of U.S.-based ad networks announced it would follow a private enforcement agreement established after several years of negotiation with the Office of the Intellectual Property Enforcement Coordinator (Ad Networks 2013). Google, the largest digital advertising actor, signed the agreement. So did AOL, and Yahoo-Bing, which operate a combined advertising network. In addition to these actors, the prominent ad networks 24/7 Media, Adtegrity, and Condé Nast agreed to the agreement. The guidelines that comprise the agreement have three components.

1. Members agree to institute policies prohibiting advertising on infringing sites and agree to an “ongoing dialogue” with all interested parties including consumer organizations and free speech advocates.
2. Members agree to be certified, either through the Interactive Advertising Bureau, the trade association for online advertising, or an independent process.
3. Members agree to institute a notice-and-takedown process to deal with complaints from rights holders.

These private agreements coordinate regulatory practices among the largest advertising actors. However, they largely reiterate policies and practices that participants already had in place. For example, Google and Yahoo-Bing operated notice-and-takedown programs before they joined the agreement. In addition, the Interactive Advertising Bureau had already certified Google and Yahoo's ad networks prior to their adoption of the private agreement (see IAB

2013). As is argued later in this chapter, the similarity between the ad networks' established policies and the private enforcement agreements is because of the ad networks' economic dependence on rights holders.

b) Digital Trading Standards Group

In 2011, the digital advertising industry in the United Kingdom began updating its voluntary industry certification program, the Internet Advertising Sales House (IASH) code of conduct. As discussed earlier, this was because new actors had joined the industry, specifically ad exchanges, which buy and sell advertisements in real time. In late 2013, the industry introduced the Digital Trading Standards Group (DTSG), which is based on a set of non-binding guidelines. Signatories to the DTSG include Google, Bing and Yahoo UK. The DTSG has two main components:

1. A process to govern where advertisements can be placed; and
2. A third-party verification process that certifies firms that have adopted processes to "minimize the risk of ad misplacement" (JICWEBS 2013:4).²⁰³

To comply with the first element, advertising intermediaries can employ automated "content-verification tools." These tools check the contents of any webpage where an ad will be delivered using, for example, keyword identification to search for common terms used on pornographic sites. If these tools detect problematic terms, they block the real-time delivery of advertisements to inappropriate sites (IAB 2013). Advertising networks and exchanges may also develop lists of pre-verified sites (called "whitelists" or, in industry jargon, "appropriate schedules"). They can also compile lists of prohibited sites (known as "blacklists" or "inappropriate schedules"). Ad networks and exchanges then use these blacklists and whitelists to govern where they place advertisements (JICWEBS 2013).²⁰⁴ Buyers and sellers of advertising agree on placement restrictions prior to selling ads and incorporate those terms into their sales contracts.

²⁰³ JICWEBS, which refers to the Joint Industry Committee for Web Standards in the U.K. and Ireland, approved the DTSG and recommends the program as an industry standard.

²⁰⁴ Interview with Amit Kotecha, Senior Mobile & Networks Manager, Internet Advertising Bureau, 8 October 2012, London.

To comply with the auditing component of the DTSG, signatories agree to allow independent, industry-approved firms verify their ad misplacement-minimization policies within six months and then thereafter annually (JICWEBS 2013:4).²⁰⁵ “No other country in the world has got this far,” says Amit Kotecha, whose industry group, the Internet Advertising Bureau, facilitated the creation of the DTSG. “It’s a massive step forward.”²⁰⁶

The City of London Police plays an unusual role in relation to the Digital Trading Standards Group. The Police Intellectual Property Crime Unit (PIPCU), which is part of the City of London Police, hosts an “infringing website list” (or blacklist). Trade associations like the Federation Against Copyright Theft and the British Recorded Music Industry populate the list of infringing sites based on their rights holder members’ complaints (Police 2013). Both trade associations had strongly pushed the digital advertising industry to crack down harder on infringing sites.²⁰⁷ Police say that all sites on the blacklist, which will not be publicly available, “are identified and evidenced as infringing by rights holders and then verified by PIPCU” (Ernesto 2014). Advertising intermediaries that belong to the DTSG will use this blacklist to ensure that the listed sites do not receive advertisements.

IV) Analysis of Intermediaries’ Enforcement Measures

The four enforcement programs analysed in this chapter from the United States, the United Kingdom and Canada outline a private regulatory regime that, while rooted in specific geographical locations, stretches globally by virtue of macro-intermediaries’ vast operations. By tapping into macro-intermediaries’ sophisticated monitoring and enforcement capabilities, the regime has the technological capacity to shape the provision of payment and advertising services across the Internet.

²⁰⁵ The industry body JICSWEB, a media industry trade association, must approve independent, third-party verification firms and content verification tools.

²⁰⁶ Interview with Amit Kotecha, Senior Mobile & Networks Manager, Internet Advertising Bureau, 8 October 2012, London.

²⁰⁷ Interview with Kieron Sharp, Director General, Federation Against Copyright Theft, 9 October 2012, by Skype.

Payment and advertising macro-intermediaries not only facilitate different types of revenue streams but they also have different regulatory capabilities in relation to infringing sites. Payment providers supply an essential service. All commercial sites and even those that operate through donations require payment processing that is reliable, trusted and popular enough to attract consumers. When the largest payment providers—PayPal, Visa, MasterCard and American Express—terminate their services, finding viable commercial replacements can be more difficult than replacing advertising revenue. Payment providers can therefore cripple websites that rely upon processing donations or payments from customers. This means that the wrongful targeting of legitimate sites can render sites commercially non-viable.

Advertising intermediaries, depending on their specific roles, can remove bad ads for counterfeit goods and deter infringing sites from accessing legitimate sources of advertising revenue. Both strategies have weaknesses. Those advertising counterfeit goods can seek alternate fora for their ads, such as social networks. Operators of infringing sites can sell space on their webpages to less reputable, non-mainstream advertisers. In contrast to payment services, commercial sites can exist without ads or can rely upon less-reputable ads from, for example, the sex industry.

i) *Payment Macro-Intermediaries*

Regulation of the online payment and advertising industries is challenging because both industries have complicated, real-time and automated enforcement processes, global operations, and an intricate ecosystem of firms providing a range of facilitative services. Merchant-account terminations are complex because each infringing site may offer multiple payment methods, termed “payment channels,” such as PayPal, Visa and Western Union. Not all these channels may be functional but the logos may be present to attract consumers. Each payment channel may support multiple webpages meaning if “you attack the single checkout page, you can make a difference,” says Robert Caldwell, founder of G2 Web Services, the company that built and does data analysis for the IACC merchant-account program (Caldwell 2012).

Detailed information on the merchant-account termination programs is not publicly available. However, snapshots released by each program give some indication of the scale of enforcement (see Table 4.3). Two years after its launch, the International Anti-Counterfeiting Coalition's program reported in January 2014 that it had referred over 8,400 sites for investigation and terminated over 2,800 merchant accounts (IACC 2014). The difference between the payment channels identified and merchant accounts terminated refers to sites that may still be under investigation, those with inactive payment channels, or already-terminated payment channels. The Canadian Anti-Fraud Centre reported that between April 2011 and March 5, 2012 it terminated 484 Visa merchant accounts.²⁰⁸ In a presentation at the IACC's anti-counterfeiting conference in May 2012, a representative from MasterCard said that it and Visa have had "hundreds and hundreds, even thousands over the last few years of merchants terminated as a result of our collective efforts" (Kirkpatrick 2012).

Table 4.3: Merchant-Account Termination Programs

Program	Intermediaries	Scope	Offences	Terminations
IACC	MasterCard, Visa PayPal, American Express, (also: Money Gram, Western Union, and Discover (Diners Club & PULSE)	Global	Counterfeit, copyright infringement, & circumvention devices	Jan. 2012 to Jan. 2014: 8,400 sites submitted and 2,800 accounts terminated
CAFC	Visa	Global (Canadian rights holders only)	Counterfeit	April 2011-5 March 2012: 484 accounts terminated

Created by author

Payment macro-intermediaries have considerable regulatory authority to control infringing sites by withdrawing their payment processing capacities. This finding corroborates recent scholarly research, which examines websites selling unauthorized pharmaceuticals, that concludes that "reliable merchant banking is

²⁰⁸ Interview with Barry Elliott, Criminal Intelligence Analytical Unit, Canadian Anti-Fraud Centre, North Bay, Ontario, 27 June 2012, by telephone.

a scarce and critical resource that, when targeted carefully, is highly fragile to disruption” (McCoy et al. 2012:1). In fact, the stated goal of the IACC’s program is to “shrink the universe” of Internet firms that provide services to infringing sites (Johnson 2013). By partnering with macro-intermediaries, intellectual property actors shift infringing sites to alternative payment methods or less-reputable payment providers whose services would not be as popularly accepted as the major payment firms.

ii) ***Advertising Macro-Intermediaries***

Enforcement efforts against online infringement within the digital advertising industry are more complex than those of the online payment industry. This is because of the number of actors involved and the dual role that some advertising intermediaries must play in removing bad ads and preventing the placement of legitimate ads on infringing site. As the ad networks’ agreement and the Digital Trading Standards Group launched in July 2013 and late 2013 respectively, it is too soon to analyse enforcement results from these programs. It is clear, however, that Google, the largest online-advertising actor, is active in its removal of ads from its services that violate its policies. In 2013, for example, Google reported removing more than 350 million bad ads, not all of which were for counterfeit goods, and banning about 14,000 advertisers for trying to sell counterfeit goods, a decline of 80% from 2012 (Google 2014). Google also reported disabling more than two million ads for “illegal online pharmacies” in 2013 (Google 2014). Despite Google’s prolific efforts, removing this content does not prevent those responsible from shifting to another, less-reputable advertising provider.

From all indications, the amount of legitimate advertising mistakenly placed on infringing sites is relatively small. Despite rights holders’ concerns, it appears to comprise a single-digit percentage of overall digital advertising. Project Sunblock, a U.K. firm providing brand-protection services, found in its survey of U.K. marketing managers that 1% of all ads were placed on sites with inappropriate content (Digital Strategy Consulting 2013). This content included phishing scams, malware, illegal drugs, violence and pornography. A senior manager for Hewlett Packard, the information technology company, echoed

these findings at the May 2012 conference hosted by the IACC. He said less than 1% of Hewlett Packard's digital advertising campaign had gone astray and 98.6% of its advertising partners were compliant with the company's rules (Linggo 2012).

More importantly, infringing sites do not appear to rely extensively on mainstream advertising. Two scholarly analyses of ads on infringing sites directed toward Canada and Singapore demonstrate that so-called high-risk advertising dominates these sites, particularly ads for the sex industry (see Watters 2014; Watters 2013). Two other studies, which focus on copyright-infringing sites, also conclude that these sites generally do not rely upon mainstream advertising to support their services.²⁰⁹ Advertising intermediaries candidly admit that a small proportion of ads will continue to be inadvertently placed on inappropriate sites. "I know after years of doing this stuff," explains Kotecha at the Internet Advertising Bureau, "everything flies around really fast and sometimes it's impossible to figure out the culprit."²¹⁰

There will always be some advertising intermediaries who will facilitate the placement of less-reputable ads to less-reputable sites. However, as critics pointed out during protests of the *Stop Online Piracy Act*, ads for "escort services and high-interest lenders" do not pay as much as "the Chevys and Coca-Colas of the world" (Healy 2013). Infringing sites, if they receive revenue from advertisements, are more likely to rely upon advertising that is unwanted by more mainstream sites, such as ads for escort services. These ads generate far less revenue than mainstream, premium brands, like Apple or Nike.

V) State Pressure and Actors' Interests

State pressure and coercion were central to the creation of payment and advertising macro-intermediaries' private enforcement agreements. The U.S.

²⁰⁹ A study jointly commissioned by Google and PRS for Music, a UK association of composers and music publishers, concluded the majority of sites analysed used ads from non-mainstream advertising firms (BAE Systems Detica 2012). The American Assembly, a non-partisan public affairs forum based in Columbia University, surveyed unauthorised downloading sites and found they were low-cost operations that rely upon donations in some cases (Karaganis 2012).

²¹⁰ Interview with Amit Kotecha, Senior Mobile & Networks Manager, Internet Advertising Bureau, 8 October 2012, London.

and U.K. governments both employed threats of legislation and legal action to convince the macro-intermediaries to adopt and implement non-binding enforcement practices. Advertising and payment actors, in addition to facing coercive measures, have varying financial and reputational interests in adopting private agreements. Interests of industry and states, however, largely overshadow consumers' interests and the private enforcement agreements raise serious concerns of anti-competitive behaviour.

i) ***Role of the State***

Governments in the United Kingdom and United States played key roles in pushing payment and advertising macro-intermediaries into negotiations and guiding the creation of non-binding regulatory arrangements. In the United Kingdom, senior officers from the City of London Police used the threat of criminal charges against Visa and MasterCard to “leverage” their cooperation.²¹¹ In the United States, the Department of Justice cracked down on Google's acceptance of advertisements for illegal online pharmacies. Google not only settled with the government for \$500 million but it also agreed to institute compliance mechanisms to prevent a reoccurrence of the problem (DOJ 2011). The action by the Department of Justice shows the seriousness that the U.S. government accords infringing sites, particularly those that are involved in the unauthorized distribution of pharmaceuticals. Pressure from the U.S. pharmaceutical industry, a powerful voice for strong intellectual property laws (see Drahos and Braithwaite 2002), likely influenced the U.S. government's crack down on Google.²¹²

In contrast, the Canadian program was created with any apparent threats or pressure on Visa as it developed from a longstanding partnership with the Canadian Anti-Fraud Centre. However, the CAFC, as a law enforcement agency, has authority to pressure Visa to cooperate should that have been necessary and, as explored earlier, a U.K. law enforcement agency had already

²¹¹ Interview with Det./Supt. Bob Wishart, Head of National Operational Delivery, Regional Fraud Project, City of London Police, 6 September 2012, London.

²¹² The influence of the U.S. pharmaceutical industry in shaping online enforcement efforts against infringing sites is explored in Chapter 5.

threatened Visa's European operations with criminal charges to compel the payment provider to work voluntarily with rights holders and law enforcement.

Negotiations in both the United States and the United Kingdom took place against pending legislation or threats of legislation. In the U.S., discussions with Victoria Espinel, Intellectual Property Enforcement Coordinator (IPEC), took place while the U.S. Congress was considering multiple intellectual property bills, including the controversial *Stop Online Piracy Act*. The U.K. digital advertising industry feared that the government could step in with legislation and "push something through," explains Kotecha, a manager at the Internet Advertising Bureau, although he contends that the last thing they want to do is legislate.²¹³

IPEC directly shaped the private agreements. Fred Humphries, vice-president of U.S. government affairs at Microsoft, acknowledges Espinel's work when he comments that the agreement with the U.S. ad networks came after a "multi-year effort with the White House to develop these best practices" (Humphries 2013). Similarly, payment providers credit Espinel for pushing them to strengthen their enforcement practices. Julie Bainbridge, a senior brand protection manager at PayPal, recalls that Espinel said to PayPal, "We know you're at the table being proactive but you need to do more."²¹⁴ Linda Kirkpatrick, an executive at MasterCard, recognizes Espinel's role in coordinating negotiations that shaped the payment industry's approach to online infringement:

We have, thanks to Ms. Espinel, an established best practices policy that all of us have signed up for, a set of minimum standards that many of us far exceed but it certainly sets the ground work and framework for what's appropriate (Kirkpatrick 2012).

In the United Kingdom, the government also made clear its preference that the digital advertising industry develop and implement the Digital Trading Standards Group quickly. In an industry-only roundtable group hosted by Minister Ed

²¹³ Interview with Amit Kotecha, Senior Mobile & Networks Manager, Internet Advertising Bureau, 8 October 2012, London.

²¹⁴ Interview with Julie Bainbridge, Senior Brand Protection Manager, PayPal, 1 July 2012, by Skype.

Vaizey, Parliamentary Under-Secretary for the Department for Culture, Media and Sport, he urged the advertising industry to “fast-track” the DTSG.²¹⁵ The digital advertising industry recognizes the role of government in shaping its regulatory measures. “[P]olitical imperatives from government have really pushed things forward,” says Kotecha.

ii) ***State and Corporate Interests in Informal Private Regulation***

The private enforcement agreements struck among payment and advertising macro-intermediaries primarily serve state and corporate interests. These agreements, drafted and implemented quietly, enable states to bypass problematic legislation and achieve similar regulatory outcomes through non-binding enforcement measures.

Payment and advertising macro-intermediaries have multiple financial and reputational interests in joining private enforcement agreements, as well as the motivation of lessening the risk of litigation from rights holders. For example, Bob Barchiesi, president of the International Anti-Counterfeiting Coalition, explains that several rights holders told him that the only reason payment providers were working with the IACC was because “they don’t want to be litigated or legislated into it.”²¹⁶ By strengthening their regulatory efforts against online infringement, macro-intermediaries can demonstrate to government that they are responsible corporate actors. Payment providers want to be able to go to “the White House and say ‘we don’t really have as big an issue as folks thought,’” explains Barchiesi.²¹⁷ Advertising actors in the United Kingdom hope that a more comprehensive regulatory program will deliver some peace in the industry. “It will be great to work with them instead of against them,” Kotecha says, as his association, the Internet Advertising Bureau, had been pressured to improve industry practices by trade associations. “There was a lot of lobbying and fighting before.”²¹⁸

²¹⁵ Minutes from February 2012 roundtable meeting chaired by Ed Vaizey (Bradwell 2012).

²¹⁶ Interview with Bob Barchiesi, President, IACC, 24 April 2012, Washington.

²¹⁷ Ibid.

²¹⁸ Interview with Amit Kotecha, Senior Mobile & Networks Manager, Internet Advertising Bureau, 8 October 2012, London.

Macro-intermediaries, like rights holders, have valuable brands that they want to protect from negative association with criminal activity. Barchiesi recounts that he used this argument when he lobbied payment providers to work with the IACC and terminate their services to infringing sites. “[Y]ou have a brand and your brand is getting damaged,” he recalls telling the providers, “because your brand lends credibility to these sites. Consumers trust your brand.”²¹⁹ Macro-intermediaries are also financially motivated to address online infringement on behalf of rights holders. Advertising actors have a strong economic self-interest in adopting measures that encourage rights holders to continue expanding their digital advertising presence. Google, for example, received 95% of its annual revenue from advertising in 2012 (Google 2013). Rights holders have tremendous power to shape rules and standards in the advertising industry because they supply the product—well-known, sought-after brands. “They fund the whole industry and everyone has to meet those demands,” says Kotecha.²²⁰ Payment providers also have financial interests in protecting their corporate brands and ensuring that the online payment industry is safe and reliable.

iii) *Consumers’ Interests*

Consumers, meanwhile, were shut out of the negotiations. Consumers’ interests are threatened by the potential of anti-competitive behaviour by macro-intermediaries that can determine the legality of content and websites in ways that may unfairly constrain the goods and services available to individuals. For proponents of stronger enforcement, private agreements that encourage coordinated or standardized regulatory practices within Internet sectors provide a useful consistency in anti-counterfeiting activities. However, the practice of macro-intermediaries working together raises the problem of anti-competitive behaviour. State pressure on payment providers, for example, has resulted these macro-intermediaries working together collaboratively for the first time. Linda Kirkpatrick at MasterCard, made this point during a presentation at the May 2012 IACC conference on counterfeiting:

²¹⁹ Interview with Bob Barchiesi, President, IACC, 24 April 2012, Washington.

²²⁰ Interview with Amit Kotecha, Senior Mobile & Networks Manager, Internet Advertising Bureau, 8 October 2012, London.

Some of us are competitors in our space. But on this particular topic, I think we've unified and rallied against the common goal of follow the money. It's not often that you get MasterCard, PayPal and Visa on the same panel. Our lawyers don't let us. But again, on this topic, there's no question that we need to be unified (Kirkpatrick 2012).

Kirkpatrick's statement highlights the problem of anti-competitive behaviour that can result when companies with dominant market shares in an industry work together to set rules and standards. There are real concerns that multinational corporations may set rules that benefit their interests and those of other powerful companies over consumers' interests and those of the general public. PayPal, for example, has withdrawn its services from technology companies that offer virtual private networks and online file storage services, which are legal technologies, because of concerns that these companies facilitate unauthorized downloads of music, movies and software (Enigmax 2013; Ernesto 2012). Payment providers' withdrawal of services from a company, on behalf of rights holders, because of suspected wrongdoing of some users is an unfairly broad regulatory approach.

There are similar concerns of anti-competitive behaviour in relation to the Digital Trading Standards Group because of its use of an industry-generated blacklist of infringing sites. Advertising intermediaries will use this list to avoid placing legitimate advertisements on infringing sites. The Police Intellectual Property Crime Unit at the City of London Police hosts and reports that it will verify sites on the list. However, the list is not publicly available for scrutiny, nor are the criteria used to designate sites as infringing. It is unclear how site operators can challenge their inclusion on the list and whether inclusion on this blacklist brings other sanctions, such as termination of payment processing facilities.

VI) Conclusion

This chapter's analysis of four anti-counterfeiting enforcement programs involving payment and advertising macro-intermediaries reveals a private regulatory regime that is rooted in the United States and the United Kingdom and extends outward globally, with a branch in Canada. Except for the Canadian case, direct state pressure was essential in compelling these macro-

intermediaries to adopt and implement regulatory arrangements based on non-binding enforcement measures. Rights holders were particularly influential in pushing advertising intermediaries, both in the United States and United Kingdom, to adopt informal regulatory arrangements because of rights holders' capacity to make rules governing the use of their brands in the advertising industry. In contrast, state pressure was necessary to stimulate cooperation from payment providers, as rights holders' lacked the authority to force payment providers to accede to their rules. State actors thus play a central, though often hidden role, within the regulatory regime but macro-intermediaries involved in the regime credit state pressure for their participation.

Payment and advertising macro-intermediaries comprise an integral part of the private anti-counterfeiting regime because, particularly in regards to payment providers, they can enact revenue chokepoints to disable infringing sites. By using the provision of payment services as an enforcement tool—a form of techno-regulation—payment macro-intermediaries are highly effective regulators that can disable sites that rely upon sales or donations. Given the market dominance of a handful of U.S.-based payment companies, they have the capacity to act as private arbiters of the legality of technologies, services and applications on the Internet and shape how individuals may access and use them. A similar challenge is evident in relation to the U.K. advertising industry's use of industry-generated blacklists to ensure advertisements are not placed on infringing sites. There is a danger that such blacklists, which are drafted in secret by powerful trade associations, will further entrench established industry interests and hinder the development of new technologies and services.²²¹

²²¹ Industry-generated blacklists of sites have a troubled history. The U.S.-based GroupM, for example, which is one of the world's largest advertising firms created a blacklist that mistakenly included many legitimate sites, including a digital library (Archive.org), technology company (BitTorrent Inc.) and video and music-sharing sites (SoundCloud and Vimeo) (Ernesto 2011).

Chapter 5: Access Chokepoints: Search and Domain Intermediaries

Search engines and domain registrars facilitate access to the web²²² and both provide critical Internet services. Search engines enable Internet users to search for and access information from among billions of webpages. Domain registrars are part of the domain name system, which is an essential part of the Internet infrastructure that translates easy-to-remember domain names (bbc.co.uk) into numerical addresses and allows users to access websites anywhere in the world. Advocates of using enforcement strategies of “access chokepoints” contend that search engines and domain registrars can deter users from accessing sites that distribute counterfeit goods or copyright infringing content.²²³ By throttling access to customers, the reasoning goes, infringing sites will cease to be profitable and individuals who seek legitimate goods will not be deceived by counterfeits.²²⁴

Similar to the strategy of revenue chokepoints discussed in chapter 4, using search and domain intermediaries to deter access to infringing sites was a key part of PIPA and SOPA. These bills would have required search and domain intermediaries to withdraw their services from infringing sites.²²⁵ Further, they would have permitted domain intermediaries to act voluntarily against sites that endangered public health.²²⁶ Despite the failure of PIPA and SOPA, search and domain macro-intermediaries adopted provisions similar to those contained within these bills in non-binding enforcement initiatives. GoDaddy, the world’s largest domain registrar, signed an agreement to withdraw its services from online pharmacies that violate U.S. laws on the distribution of pharmaceuticals.

²²² While the “Internet” and “World Wide Web” (or web) are often used inter-changeably they refer to different entities. The Internet is a series of interconnected computers and the web, a system of hypertext-linked webpages, is one of the services that operates on the Internet.

²²³ Interview with Dave Wood, Director of Anti-Piracy, British Recorded Music Industry (BPI), Ltd., 12 September 2012, London.

²²⁴ This dissertation does not address the regulatory role of Internet service providers (ISPs), such as Verizon, which enable users to access the Internet. They play a significant role in the control of digital-copyright infringement but not the regulation of counterfeit goods. For the role of ISPs in regulating copyright infringement, see McIntyre and Scott (2008) and de Beer and Clemmer (2009).

²²⁵ SOPA Sec. 103 and PIPA Sec. 4.

²²⁶ Google would have been permitted to act voluntarily against sites endangering public health through its role as an advertising intermediary, see: SOPA Sec 104 and PIPA Sec 5(b).

Google, the largest global search engine, adopted a U.K.-based code of conduct to guide its regulation of search results.

Examining search engines and domain registrars together makes sense because both types of intermediaries facilitate access to sites. In addition, intellectual property actors argue both should assume greater responsibility for blocking or deterring access to infringing sites. Search and domain macro-intermediaries are key components of the global private regulatory regime, as are the payment and advertising macro-intermediaries examined in chapter 4. Google and GoDaddy—the focus of this chapter’s case studies—are classic examples of gatekeepers that regulate through technology. They each operate massive operations with global reach and have highly sophisticated surveillance and enforcement programs to protect their platforms from all kinds of threats, including infringement by third parties. As they each dominate their respective industries, rights holders and states are keen to recruit them as private enforcers to crack down voluntarily on infringing sites.

Search and domain macro-intermediaries negotiated their private enforcement agreements in the shadow of legislation, similar to the experience of the intermediaries discussed in chapter 4. Google and GoDaddy—this chapter’s two case studies—have varying interests in agreeing to strengthen their enforcement efforts voluntarily against infringing sites. Both Google and GoDaddy are motivated to protect their corporate reputations from association with wrongdoing and mitigate the risk of legislation or legal action from rights holders or states for facilitating infringement. Google, in particular, has been subject to intense pressure from governments in the United States and United Kingdom, as well as from rights holders and their trade associations. Google also faced the threat of criminal charges from the U.S. Department of Justice for accepting ads from unauthorized online pharmacies, a matter it settled by forfeiting \$500 million (DOJ 2011).

This chapter explores how and why Google and GoDaddy, the leading search and domain macro-intermediaries, agreed to adopt a tougher approach against infringing sites voluntarily. First, the chapter briefly introduces the search and domain name industries before explaining how search engines and domain

registrars operate. Third, it explores how these macro-intermediaries became gatekeepers and the creation of the private regulatory regime. To illustrate how these macro-intermediaries regulate infringing sites, this chapter examines two cases of informal private regulation. In the first case, the chapter analyses the first-ever search engine-created voluntary code of conduct drafted in the United Kingdom by Google, Yahoo and Bing. The chapter then discusses GoDaddy's participation in a White House-negotiated informal agreement to crack down on online pharmacies that violate U.S. laws on the distribution of pharmaceuticals (commonly termed "illegal online pharmacies"). In the fifth section, the chapter provides analytical findings on these programs and then examines the role of the state and actors' interests. The chapter then offers a brief conclusion.

I) Search and Domain Names Service Industries

Search engines and domain registrars provide essential Internet services that are integral to the effective functioning of the Internet and the growth of e-commerce. Search engines provide the vital link between users and the billions of webpages comprising the World Wide Web. They enable individuals to access knowledge and ideas from around the world and to tap into previously difficult-to-access sources of information. They also help consumers locate goods and services from vendors ranging from boutique neighbourhood outlets to global multinational corporations. Domain registrars, for their part, deliver essential Internet infrastructure. The domain name system (DNS), which is explained in greater detail in the next section, is commonly described as the phone book of the Internet. It enables anyone to connect to websites around the world by resolving (i.e., translating) easy-to-remember domain names (e.g., www.slate.com) to the corresponding unique numeric Internet Protocol address. The DNS enables universality: anyone can reach the same website by entering its domain name. Domain registrars are one of several actors that facilitate the operation of the domain name system and enable individuals and companies to operate their own sites. Two U.S.-based companies—Google and GoDaddy—dominate the search and domain name markets, although there are many smaller search engines and domain registrars that offer services.

Google's dominance on the Internet is difficult to overstate. Created in 1997, Google is the most popular search engine globally and the largest digital advertising platform. Google is outranked in some markets by local search engines, such as by Baidu in China and by Yandex in Russia. Google dominates the search markets in the United States (67%) and in the European Union (over 80%) (Goodwin 2014). Alongside Google are other, much smaller search engines. Yahoo, created in 1994, has around 10% of the U.S. market (Goodwin 2014). Bing, which is owned by Microsoft and was created in 2009, has about 16% of the U.S. market (Goodwin 2014). The number of searches these companies facilitate is staggering. In December 2013, Google conducted 18 billion searches, Bing conducted 3.3 billion, and Yahoo 2 billion (Goodwin 2014).

The collection and organization of information, whether in libraries or through search engines, is never neutral but always privileges certain ideas and voices over others (Kohl 2013). Search engines effectively construct meaning by defining the information that is available for search queries and therefore they shape choices (Elkin-Koren 2001:185). Critics have long argued that search engines deliberately or inadvertently exclude certain types of sites (Introna and Nissenbaum 2000).²²⁷ In the online environment where the amount of information is overwhelming, search engines play a vital role in amassing and sorting information. In doing so, however, they can be understood as powerful chokepoints (Kohl 2013) and gatekeepers that filter information in a deliberate and strategic manner (Elkin-Koren 2001).

As a search and advertising giant, Google has a tremendous capacity to shape the types of information users access and, because of its reliance upon advertising revenue, it has strong commercial interests in doing so. Google thus generates significant social anxiety. In a January 2014 debate on an intellectual property bill before the House of Commons in the United Kingdom, Pete Wishart, a Member of Parliament for the Scottish National Party, expressed concerns about Google's influence:

²²⁷ Introna and Nissenbaum (2000) argue that search markets that are slanted toward large, commercial, popular sites and risk silencing certain voices and content.

It is digital behemoth—there is nothing bigger in the digital world—and the gatekeeper for all our content industries. Nothing happens without Google, and nothing can go through its prism without satisfying it in some way (Wishart 2014:24).

States and corporate actors have successfully tapped into Google’s surveillance and enforcement apparatuses to try to exert control over the types of search queries that are “acceptable” and to regulate “objectionable” content—the definitions of which vary widely and are not always set out in legislation (see Elkin-Koren 2001; Kohl 2013). In terms of intellectual property, rights holders and their trade associations have for years lobbied Google to take ever-greater responsibility to ensure its service does not facilitate access to illegal content. As a result, Google has become—at times unwillingly—one of the major online regulators of infringing content.

Domain registrars, in contrast, have attracted much less political attention. In contrast to Internet services like search engines or marketplaces, users generally do not directly encounter domain registrars. Instead they use Internet services that themselves rely upon the domain name system. The average Internet user likely has little familiarity with the operation of the domain name system. This is because the domain name system is technical, complex and challenging to comprehend fully. The DNS operates as good infrastructure should—unobtrusively, effectively and without requiring its users to comprehend its operations. Even those in intellectual property rights enforcement are more familiar with traditional regulatory actors, such as search engines or online marketplaces. Domain registrars are relatively new regulatory actors in the realm of anti-counterfeiting in contrast with search engines.

GoDaddy, created in 1997 and based in Phoenix, Arizona, is the largest domain registrar globally with approximately 30% of market share and it claims on its website to have over 57 million domains.²²⁸ As a registrar, it registers domain names on behalf of individuals or companies wanting to create websites. GoDaddy registers multiple types of domain names, known as generic top-level domains, including .com, .net, .org, info, .biz., .travel and .xxx. Individuals wanting to create sites with one of these domain extensions register domain

²²⁸ For information on GoDaddy’s services, see: <http://au.godaddy.com/>.

names with the company. GoDaddy is also one of the world's largest web hosting companies. This means that it provides content storage or hosting services to individuals or companies wanting to establish sites. GoDaddy is a privately held company and financial analysts estimated its 2013 revenue at \$1.43 billion (Kharif 2013).

i) *How Search Engines Work*

To “exist is to be indexed by a search engine,” argue Professors Lucas Introna and Helen Nissenbaum (2000:171) in their analysis of the political importance of search engines, in which they argue search engines shape the information users can access. This observation aptly captures how users fundamentally rely upon search engines to navigate effectively among billions of webpages. Google has entered our common vernacular (‘to Google’ something) and the term is often used to refer to any kind of online search. One could thus say to “exist is to be indexed by Google.” Given the scale of Google’s search platform, any exclusion from its search results represents a broader exclusion from society and from full participation in commercial, social and cultural life. Despite the common usage of the term ‘Google,’ the average Internet user may regularly rely upon search engines but have little understanding of how they operate.

Other programs can perform search functions but this dissertation focuses exclusively on search engines. This is because rights holders and governments argue search engines are the main culprits furthering infringement (MPAA 2013).²²⁹ Search engines are complex software programs that use algorithms to scan the web, extract billions of items of information and deliver it to users organized in a fashion that is relevant to users’ search queries. Retrieved information may be in a wide variety of formats, including text, images, maps, audio and video, products and geographical locations (Gasser 2006:206). Although search engines are highly complex, they are essentially software systems that look for information on the web and, sometimes, in databases, in

²²⁹ The Motion Picture Association of America, the main lobbying body for the movie industry, released a report in 2013 in which it argued that Google facilitated users’ searches for copyright-infringing content and thus facilitated illicit downloads of movies (MPAA 2013).

response to users' inputted keywords. In order to identify and catalogue the web's billions of webpages, search engines use software called 'web crawling bots' or 'spiders' to crawl the web and build indices of what is found on hundreds of millions of sites. Search engines must continually crawl the Internet because new sites are added and existing sites change.

Once a search engine retrieves information based on a user's keywords, it must present the information in a manner that is useful and relevant to the user, although the search results may number in the tens of millions. Search engines use complex proprietary algorithms to rank search results and they closely guard the details of those algorithms. Google, for example, only discloses that its algorithm uses 200 variables to rank webpages, including the frequency and location of keywords on that page and the number of other pages linking to the page in question (Singhal 2012). Search engines then present those ranked results in listings called "search engine results pages." Each search result contains a hyperlink to the webpage where the search terms appear and a brief snippet of text. From that text snippet and the hyperlink, the user can choose the desired search result. Highly ranked search results receive the most traffic and Google's top search results are the most valuable as it is the dominant search engine. As search ranking is proprietary, search results differ among search engines and search engines also produce different results in different countries (Spink et al. 2006). Search engines generally sell ad space alongside search results that correspond to the search terms.

ii) ***How the Domain Name System Works***

In contrast to search engines, the domain name system is more complicated. The domain name system refers to the complex process that translates ("resolves") a site's domain name into its corresponding, unique Internet Protocol address and, in doing so, locates the site in question and enables the user to access it. Simply put, the domain name system matches names (e.g., a website's address) to numbers (its IP address). Users do not have to remember or even know a site's specific numerical Internet Protocol address.

Although it is easy to take the effective functioning of the DNS for granted, it is

important to outline how the system functions in order to explain how registrars can disable infringing sites. Imagine that you wish to create a website. To do so you have to purchase server space from a web hosting service for a small fee. You can choose from one of thousands of companies, including from many Internet service providers that enable you to access the Internet, like Virgin Media. You also have to register for a domain name from a domain registrar so people will be able to find your site easily. Domains are not sold outright: one must register them for fixed periods of time and they can be automatically renewed.

Domain registrars manage and register domain names. They may, like GoDaddy, offer retail-level services to register names on behalf of individuals and companies. They may also offer wholesale-level services to companies that are re-sellers of domain names, such as the U.S.-based company eNom. Many of these companies offer both web hosting and registrar services. Imagine you choose GoDaddy, which is the largest registrar globally and also offers web hosting. You select a simple and catchy domain name and use the registrars' automated process to register your name. GoDaddy registers domain names "at a rate of more than one per second," which makes it "virtually impossible for a human being to verify the legitimate use of every domain name," explains Christine Jones, former executive vice president and general counsel for GoDaddy in testimony before the U.S. Congress in 2011 (Jones 2011:4). GoDaddy approves your registration and issues the name to you for a specified period of time as long as you abide by GoDaddy's terms and conditions regarding your use of the domain name (GoDaddy 2013).

Your new domain name fits neatly into a global, hierarchal domain name system. The system is organized into various types of domain names extensions. There are 250 unique country-code designations (country-code top-level domains), such as .us (United States), .ca (Canada), .uk (United Kingdom) and .jp (Japan). There are generic designations (generic top-level domains), of which .com, .net, and .org are commonly recognized. The .com designation is the most popular code for commercial sites. Codes that refer to specific agencies or institutions are called sponsored designations (sponsored top-level

domains), such as the commonly used .edu (education) and .gov (U.S. government).

Once your new site is ready to be viewed, you type its domain name into your web browser and, in a fraction of a second that it takes to load, a series of transactions occur. This process, which translates a domain name into its corresponding numeric IP address and enables the user to view a specific site, is called resolution. To resolve the domain name, the individual's computer (or handheld computing device) works to resolve the query by using cached information from previous views of the site in question. The process may also involve the Internet service provider (e.g., Verizon) sending a series of queries to different domain name servers. These are massive databases that map domain names to their Internet Protocol (IP) addresses. The Internet service provider sends queries until the address is found. Simplifying somewhat, the following process occurs:

1. Someone types your domain name into a web browser. This generates a request by your Internet service provider to match the domain name to its IP address known as a DNS query.
2. The query travels to an authoritative name server, sometimes going through other name servers in the process, which translates the domain name into its IP address, known as DNS resolution.
3. The Internet service provider, now with the IP address, contacts the site in question and it loads in the user's browser.

II) Pressure on Marketplaces from State and Industry

As explained in chapters 3 and 4, the United States does not have a statutory measure to address online trademark infringement. As a result, in the United States, search and domain intermediaries are not required by statute to remove content or disable services in relation to rights holders' complaints of online trademark infringement. They can, however, do so voluntarily. In the European Union, in contrast, search engines are required to remove search results linking to webpages that offer counterfeit goods under the *E-Commerce Directive*,

which is echoed in member states' laws.²³⁰ For proponents of tougher measures to address online infringement, informal private regulatory arrangements are useful in situations where there are legislative gaps (e.g., domain intermediaries in the United States) or where parties consider the statutory requirements insufficient (e.g., search engines' regulation in the United Kingdom).²³¹

Rights holders and their trade associations recognize the regulatory capacity that search and domain macro-intermediaries can bring to the policing on online infringement. Google, in particular, has been a target of pressure because intellectual property owners, particularly the large movie, music and software industries, argue that Google facilitates digital-copyright infringement by displaying search results that link to infringing webpages.²³² Government officials in the United States and United Kingdom have likewise harshly criticized Google and demanded that the search giant crack down on search results that link to webpages with illegal content.²³³ Domain intermediaries, in contrast, have attracted much less political attention. This is largely because the domain name system is technical and complex, particularly for those accustomed to working with web hosts, Internet service providers or marketplaces. As well, domain intermediaries are relatively new to policing online infringement.

Search and domain intermediaries both facilitate access to the web, although they differ in the ways they function and their degree of interaction with Internet users. Individuals have direct contact with search engines as they choose a specific search engine, type search terms and receive a list of search results from their query. In contrast, domain registrars do not have direct contact with

²³⁰ Domain intermediaries are not included within the *E-Commerce Directive*. This chapter focuses on the operation of the domain registrar GoDaddy in relation to its U.S.-based operations.

²³¹ There were legislative gaps in the United States because, at the time the Office of the Intellectual Property Enforcement Coordinator was coordinating negotiations that led to the Centre for Safe Internet Pharmacies, the U.S. Congress was considering COICA. With the deaths of COICA, PIPA and SOPA, the private agreement that created CSIP survived.

²³² As mentioned earlier in this chapter, in 2013, the Motion Picture Association of America released a report that accuses Google of facilitating users' access to copyright-infringing content (MPAA 2013).

²³³ For example, the U.K. House of Commons' Culture Media and Sport Committee criticised Google harshly in its 2013 report, entitled "Supporting the creative economy." In their report, members "condemn[ed] the failure of Google" to address illegal content on its platform (2013:3).

users. They play a role in operating the domain name system, which ensures users can access the webpages they select from their list of search results. Domain registrars have a contractual relationship with the site operators for which they provide domain names (such as the .com or .net extensions) but not individuals visiting those sites. Search engines do not have a contractual relationship with either users of their systems or the sites that they index to produce their search results.

i) **Regulating Search Engines**

Domestic laws, judicial rulings, internal policies and informal agreements govern the type of information search engines are permitted to display in their search results page.²³⁴ Search engines argue that they merely deliver information relevant to users' search queries. Google, for example, says that it "is a provider of information, not a mediator" and does not "make any claims about the content" of the webpages relating to search requests.²³⁵ Despite this claim, search engines mediate search and shape search results in many ways, as the next section will explore in greater detail. In many countries, search engines are legally required to remove search results that link to webpages with copyright-infringing content once appropriately alerted by rights holders or their authorized representatives. As discussed in chapter 3, search engines fall under the 1998 *Digital Millennium Copyright Act* (DMCA) in the United States and the European Commission's 2000 *E-Commerce Directive* in the European Union.²³⁶ Both the DMCA and the *E-Commerce Directive* contain provisions that require search engines to remove infringing search results in notice-and-takedown programs in

²³⁴ For example, a court in France ordered Yahoo in 2000 to disable access to auctions of Nazi memorabilia for individuals in France as indicated by their Internet Protocol addresses (Goldsmith and Wu 2006).

²³⁵ Google makes this statement on its webpage describing how content can be removed from Google, see: <https://support.google.com/legal/troubleshooter/1114905?rd=2#ts=1115655,1282899>

²³⁶ Search engines are classified under "informational locational tools" in the DMCA, see Sec. 512 (d). In the E-Commerce Directive, search engines fall under hosting providers, see Article 18. European Commission Electronic Commerce Directive (ECD), 2000/31/EC, passed 8 June 2000. The United Kingdom implemented the Electronic Commerce (EC Directive) Regulation 2002, SI 2002/2013, a mirror of the ECD.

response to notifications of infringement.²³⁷ These rules formalized search engines' role in controlling online infringement.

Search engines also have internal policies that govern the types of search terms they display. Google, for instance, removes or blocks images in search results that involve pornography, bodily functions or fluids, vulgar words, or animal cruelty.²³⁸ In addition, search engines will remove certain types of results. They generally remove results relating to child sexual abuse and some types of personal information, such as social insurance numbers or credit cards that could make individuals susceptible to crime. To protect users' safety, Google will also remove search results that link to sites, for example, that install or distribute viruses. However, search engines generally refuse to remove search results that link to content that individuals may allege is embarrassing, inaccurate or offensive, unless ordered to do so by the courts.²³⁹

It is important to clarify search engines' capacity to regulate. Search engines index and rank webpages. They can de-index (i.e., remove) specific hyperlinks from search results that link to problematic webpages but they cannot remove content from those webpages. Complainants who want webpages removed must contact site operators or web hosts. Complainants must also distinguish between search engines results (i.e., the list of hyperlinks for webpages) and search engine-related ads that appear alongside those results. Search intermediaries have separate policies and notice-and-takedown systems to deal with each (for the removal of ads, see chapter 4).

Nonetheless, search engines' capacity to access, index and rank hyperlinks to vast amounts of information, mark them as powerful regulators. Governments around the world and corporate actors are increasingly demanding that search engines deliver only "acceptable" search results, although concepts of

²³⁷ See DMCA, see Sec. 512 (d)(3) and E-Commerce Directive Article 14 (1b). The wording is similar in both regulations. Intermediaries must act "expeditiously" to "remove or disable access to" the targeted information.

²³⁸ See Google's Removal policies <https://support.google.com/websearch/answer/2744324>

²³⁹ Ibid.

“objectionable” content vary widely among countries and from issue to issue.²⁴⁰ As part of their efforts to address unacceptable content, Google, Yahoo and Bing belong to the U.S.-based Financial Coalition Against Child Pornography, which is managed by the U.S.-based National Centre for Missing and Exploited Children.²⁴¹ For this organization and a similar association in the European Union called the Internet Watch Foundation, search engines voluntarily agree to block access to webpages blacklisted by the organization as containing child pornography. They also voluntarily remove search results that link to webpages containing child sexual abuse content (see Laidlaw 2012).

ii) *Regulating Domain Registrars*

Domain registrars are governed by a series of contractual agreements between the registrant (i.e., site operator) and registrar (e.g., GoDaddy), as well as contracts among ICANN (the Internet Corporation for Assigned Names and Numbers), the registrar and its registries. ICANN is a private, non-profit institution based in California that oversees and coordinates the Internet’s technical infrastructure, including the domain name system. It sets out the responsibilities of registrants, registrars and registries that are then echoed in each of the contractual agreements (ICANN 2012). Domain registries, which comprise a range of public-sector organizations, non-profits and commercial firms, each act as specific databases for all the domain names registered within a specific top-level domain. The U.S.-based company Verisign, for example, is the authoritative registry for the .com designation, which means that all registrars that want to issue .com domains must work with it.²⁴²

²⁴⁰ See, for example, Deibert et al. (2011) for a valuable analysis of the varying ways Internet intermediaries act on behalf of states to control and censor information and monitor citizens in countries throughout Southeast Asia.

²⁴¹ FCACP is part of the Centre for Missing and Exploited Children and the National Centre for Missing and Exploited Children, a non-profit organization working with the U.S. Department of Justice. Other members of FCACP include PayPal, Visa, MasterCard and American Express. The Internet Watch Foundation, funded by the European Union, is a non-profit organization that has law enforcement and industry partners and operates through voluntary industry regulation.

²⁴² Verisign is also an important part of the domain name system as it operates one of the thirteen root name servers. This means that Verisign, along with the twelve other root servers, contains the complete database of Internet domain names and the corresponding IP addresses for particular top-level domains (e.g., .com for Verisign, along with the other top-level domains it manages). These servers are the first to respond to queries for resolving domain names to the corresponding IP addresses.

ICANN sets out policies that each registry must adopt or institute in the registries' agreements with registrars. ICANN has the authority to suspend or terminate registrars that violate its policies by, for example, permitting illegal activity or failing to comply with court orders (ICANN 2013). ICANN also accredits registrars, although not all choose accreditation. Each domain registrar may work with multiple registries, for example, for Verisign with .com and the U.S.-based registry Neustar for .biz. GoDaddy, then, is bound by agreements with multiple registries and must also abide by ICANN's policies and ICANN's accreditation agreement.

Registrars' contracts with website operators also echo state laws. GoDaddy, for example, prohibits users of its services from involvement with malware, spam, hacking, the promotion of terrorism or the distribution child sexual abuse images (GoDaddy 2013). The company also prohibits its users from promoting, selling or distributing prescription medication without a valid prescription or infringing on any entity's intellectual property rights (GoDaddy 2013). Like search engines, domain registrars are also active in efforts to counter online child pornography. GoDaddy, for example, is also a member of the UK-based Internet Watch Foundation and voluntarily removes its services from sites that the Foundation identifies as distributing child pornography (Jones 2011).

iii) *Creation of Private Enforcement Agreements*

Search engines and domain registrars have varying degrees of experience addressing online infringement. For search engines, the first public reference to voluntary industry regulation of infringing sites came in 2009 when the International Trademark Association (INTA) released its best practices to address the online sale of counterfeit goods (INTA 2009). This is the same document that recommends payment providers voluntarily act against infringing sites, as was discussed in chapter 4. It proposes that rights holders and search engines "work collaboratively" to address the online distribution of counterfeit goods and that search engines establish some kind of "clear and effective process" to deal with infringing search results (INTA 2009:4). Google and Yahoo's agreement to these best practices commit them, at most, to discussions with trademark owners and instituting processes to receive

complaints of infringement. This is in stark contrast to rights holders' demands several years later for vastly strengthened enforcement practices, as the next sections will explore.

As e-commerce and file-sharing technologies developed throughout the 2000s, rights holders increasingly began complaining about the online distribution of counterfeit goods and copyright-infringing products. Google, as the largest search engine, was the target of the most complaints of infringing search results, and the vast majority of these are from the music and movie industries (Google 2013). As discussed in chapter 1, search engines and domain registrars would have been required under PIPA and SOPA to withdraw their services from infringing sites. Under these bills, both search and domain intermediaries could have taken voluntary action against sites endangering public health.²⁴³ Prior to these bills, search and domain intermediaries worked voluntarily against child pornography sites and to prevent online fraud. PIPA and SOPA, however, expanded the idea of voluntary regulation from state-driven efforts (child safety) and security-driven measures (fraud) to include working with corporate actors to protect intellectual property.

These bills, as discussed in chapter 1, aroused fierce public opposition, especially SOPA. Google, in particular, voiced its protest to proposals that search engines should increase their enforcement efforts against infringing sites. Kent Walker, senior vice president and general counsel at Google, spoke before a House Judiciary Subcommittee in 2011. He reminded them "search engines are not in a position to censor the entire Internet, deleting every mention of the existence of a site" (Walker 2011:7). Walker went on to remark that search engines cannot make problematic sites "unfindable" (Walker 2011:7). In addition to critics' concerns of censorship, SOPA's opponents warned about possible damage to the domain name system. Technologists, including engineers who built the Internet, protested that SOPA's provisions to block the domain name system could irreparably harm the systems' stability, security and universality. In a provision alternately referred to as "blocking" and "filtering," SOPA proposed to use Internet service providers (e.g., Verizon) to

²⁴³ PIPA Sec. 5(b) and SOPA Sect. 105.

prevent resolution to the corresponding Internet Protocol address.²⁴⁴ This provision would mean that certain sites targeted by the U.S. government or rights holders would be “unreachable by, and invisible to, Internet users in the United States and abroad” (Lemley, Levine, and Post 2011:36). This provision did not directly affect domain intermediaries. However, a representative from GoDaddy, a strong supporter of SOPA, proposed in testimony before the U.S. Congress that domain registrars, not Internet service providers, were better equipped to block undesirable sites (see Jones 2011). Google and GoDaddy were, therefore, on opposite sides of SOPA and had different approaches to the regulation of online infringement.

In 2010, as critics of COICA were sounding the alarm about significant problems with the bill, Victoria Espinel, head of the Office of the Intellectual Property Enforcement Coordinator (IPEC) was meeting with macro-intermediaries in relation to creating an industry-based, informal regulatory regime that would operate outside of the proposed intellectual property bills. As introduced in chapter 4, the goal was to agree upon non-binding initiatives to address what Espinel referred to as “illegal fake online ‘pharmacies’—criminals masquerading as legitimate pharmacies” (Espinel 2012a). In December 2010, two months after the introduction of COICA, Espinel announced the creation of the Centre for Safe Internet Pharmacies (IPEC 2012). Signatories to the agreement are payment providers (MasterCard, Visa, American Express, PayPal), search engines (Google, Bing, Yahoo) and domain registrars (eNom and GoDaddy) (IPEC 2012). In creating the Centre for Safe Internet Pharmacies, Espinel brought together companies with vast regulatory capacities in a regulatory regime with global reach across multiple Internet industry sectors.

The purpose of the Centre for Safe Internet Pharmacies (CSIP) is to raise public awareness about unauthorized online pharmacies and to encourage consumers to purchase medication from licensed, accredited pharmacies.²⁴⁵ CSIP also has

²⁴⁴ SOPA, for example, proposed to block infringing sites using the domain name system. Domain registrars would prevent queries from accessing the proper sites and would instead return error messages. SOPA Sec. 102(c)(2)(A) and PIPA Sec. 3(2).

²⁴⁵ As will be explored later in the chapter, one method of accrediting pharmacies is through the private-sector firm LegitScript, which analyses and verifies the operations of online pharmacies.

a more unusual focus: enforcement. Advertising intermediaries like Google that are members of CSIP remove advertisements for unauthorized pharmacies, while GoDaddy cancels or seizes domain names.²⁴⁶ These measures are similar to those proposed in COICA.²⁴⁷ This chapter examines CSIP as one of its case studies because it offers a useful opportunity to examine how domain registrars, specifically GoDaddy, became gatekeepers to control online infringement. In addition, CSIP differs from the other informal private agreements because it involves a coalition of macro-intermediaries that work in a coordinated fashion to disable sites that CSIP designates as illegal online pharmacies. As will be discussed later in the chapter, GoDaddy was largely a willing participant in these discussions, in stark contrast to Google, which was under considerable pressure from intellectual property and government actors to participate.

While macro-intermediaries' negotiations with IPEC occurred against the shadow of impending legislation, those in the United Kingdom were set against stalled legislation. In the United Kingdom, the 2010 *Digital Economy Act* had stalled amid industry infighting over the cost of the system.²⁴⁸ The legislation focuses solely on sites offering copyright-infringing content (e.g., unauthorized downloads of music, movies or software). It proposes to have Internet service providers, like Virgin Media, institute three-strikes programs in which they would pass on warnings from rights holders to users and then terminate users' Internet access.²⁴⁹ Copyright-related trade associations, unhappy at the long delay over the implementation of this legislation, pressured the government to facilitate informal discussions among industry stakeholders. Ed Vaizey, the Parliamentary Under-Secretary for Culture, Communications and Creative Industries at the Department for Culture, Media and Sport convened a series of roundtables in 2011 and 2012 with search engines, rights holders and trade associations. In a series of closed-door, industry-only meeting in 2011 and 2012

LegitScript, which is a member of CSIP, also works for pharmaceutical companies, indicating the potential of pharmaceutical industry interests influencing standards for online pharmacies.

²⁴⁶ Payment providers would also terminate the pharmacies' payment processing capacities.

²⁴⁷ The measures also closely resemble provisions that PIPA and SOPA would have when they were introduced in May and October 2011.

²⁴⁸ The *Digital Economy Act*, introduced in 2010 in the United Kingdom has stalled amid conflict between rights holders and Internet service providers over the cost of implementing the system. The government hopes to finally institute the program sometime in 2015 (see BBC 2013).

²⁴⁹ Digital Economy Act 124A.

that were chaired by Vaizey, rights holders and search engines discussed voluntary enforcement efforts. In February 2012, Google, Yahoo and Bing drafted a voluntary code of conduct. It is the first of its kind anywhere for search engines (see Appendix D).²⁵⁰

The search engines' code is the product of both threats of legislation and direct pressure by government officials. At those roundtable meeting, Jeremy Hunt, who was then Secretary of State at the Department for Culture, Media and Sport, warned the search intermediaries that the government was "willing" to employ legislation but wanted "industry to find a way forward" (Bradwell 2011). With this threat of legislation in the background, Hunt then "tasked" search engines to draft a voluntary code of conduct to guide their enforcement efforts after they rejected the one proposed by rights holders as too stringent (Bradwell 2011). As will be explored in the following section, rights holders were "disappointed" by the search engines' code (Bradwell 2012). Hunt and Vaizey pressured the search engines to work with rights holders to amend their enforcement practices in line with rights holders' demands. Google, which has faced unremitting pressure from government officials and rights holders in the United States and United Kingdom, made significant alterations to its enforcement practices.

To summarize, the U.S. and U.K. governments exerted varying degrees of coercive pressure on search and domain macro-intermediaries to secure their participation in private regulatory arrangements, which is a similar situation to the macro-intermediaries examined in chapter 4. The private enforcement agreements adopted by Google and GoDaddy comprise an important component of the private anti-counterfeiting regime. As described in chapter 3, underlying the regime are inter-dependent interests between rights holders and the regime's state actors that are oriented toward strengthened protection for intellectual property rights. The regime relies upon the technological capacity of its macro-intermediaries as without their ability to monitor and control transactions and behaviour across their platforms, rights holders would be unable to control online infringement at a scale that they consider necessary.

²⁵⁰ The Open Rights Group obtained this code of conduct through a freedom of information request (Bradwell 2012).

III) Intermediaries' Enforcement Programs

As the largest search engine, Google is the target of the most complaints about search results linking to infringing webpages and is removing ever-increasing numbers of search results from its search index. The search giant faces considerable government and industry pressure, as evident in the U.K. roundtable discussions, in which industry and government actors encouraged Google to modify its enforcement practices (Bradwell 2011). GoDaddy, in contrast, is relatively new to working as a gatekeeper in relation to intellectual property and, except for the threat of legislation on all macro-intermediaries, did not appear to experience direct government pressure.

i) Search Intermediaries' Enforcement Policies

Search intermediaries operate notice-and-takedown programs to remove search results that link to problematic webpages, such as those containing copyright-infringing goods. In order to have results removed, search engines generally require complainants to provide a name and contact information and describe the nature of infringement. Complainants must provide the URL²⁵¹ of the infringement, an electronic signature of the rights holder or the authorized agent, and a statement attesting the information is correct.

Google publishes its enforcement efforts in its *Transparency Report*, which is a standalone site dedicated to tracking the complaints Google receives from rights holders and requests for data from governments. In relation to rights holders, Google tracks who submits the requests, and indicates the requests it complies with and those it rejects.²⁵² No other company discloses more information on its enforcement efforts than Google, particularly on behalf of rights holders. Yahoo and Bing, in contrast, do not publish figures on their enforcement activities. Beginning in 2012, the numbers of requests for removal to Google began to increase dramatically. According to the *Transparency*

²⁵¹ The uniform resource locator: this is the string of text that identifies a webpage address. Google requires a link to a specific webpage in order to remove the search result that hyperlinks to that page.

²⁵² Google's Transparency Reports do not include all requests the search giant receives. It does not include, for example, any requests relating to its YouTube or Blogger services, see: <http://www.google.com.au/transparencyreport/>

Report, in 2012, Google removed 50 million search results, compared with only 10 million in 2011. In 2013, it removed 214 million search results. For the first four months of 2014, Google has received a staggering 100 million requests for the removal of infringing search results (Ernesto 2014). Google reports that it complies with just over 97% of the requests it receives and does so in an average of six hours from the time a request is received (Google Transparency Report). The vast majority of these removals relate to complaints of copyright infringement and two of the largest reporting organizations are the British Phonographic Industry and Recording Industry Association of America (Google 2013).

As stated earlier, search engines operating in the European Union are required by statute to remove trademark-infringing search results, but those operating in the United States face no such statutory requirement. Outside the European Union, Google directs complainants who wish to remove results to sites selling counterfeit goods to contact the site operator of the sites in question.²⁵³ Despite Google's policies that it will not remove such results, the search giant is removing small numbers of search results linking to sites selling counterfeit goods and recording them in its Transparency Report. Among the hundreds of millions of copyright-related complaints are a very small number of removal requests from well-known trademark owners Chanel, Gucci, Louis Vuitton and Deckers Outdoor Corporation. For example, in a three-month period in 2013, Deckers Outdoor Corporation, which owns the popular Ugg brand of footwear, submitted requests for the removal of 19,520 URLs from Google's search results.²⁵⁴

Google does not remove all URLs submitted by trademark owners and does not provide reasons for its decisions. The search giant may be removing the results in response to complaints from intellectual property actors under the *E-Commerce Directive* for Google's European operations or as part of its own proactive enforcement. Another possible explanation is that rights holders file

²⁵³ To see Google's advertising policies regarding the use of trademarks and trademark infringement, see: <https://support.google.com/adwordspolicy/answer/2562124?hl=en-AU>

²⁵⁴ These removals were submitted between 3 July 2011 and 26 September 2013. <http://www.google.com/transparencyreport/removals/copyright/owners/25106/Deckers-Outdoor-Corporation/>.

complaints of copyright infringement to remove these results. If the counterfeit goods are advertised using rights holders' copyrighted stock photos, rights holders can submit a complaint of copyright infringement under the *Digital Millennium Copyright Act* to remove search results linking to sites selling counterfeit goods.²⁵⁵

a) Search Engine Code of Conduct

The United Kingdom is home to the first voluntary code of conduct among search engines in relation to intellectual property rights infringement. As discussed earlier in this chapter, U.K. rights holders and trade associations wanted progress in regards to online infringement given delays in the implementation of the 2010 *Digital Economy Act*. They petitioned the Department for Culture, Media and Sport (DCMS) to convene private, industry-only roundtables to discuss intellectual property rights infringement (Bradwell 2011).

Table 5.1: Comparison of Codes for Search Engines

Rights holders' proposed code	Search engines' code of conduct
Demote repeatedly infringing sites	No demotion policy
Prioritize certified sites	No certified sites policy
Stop indexing sites subject to court orders	No such policy
'Improved' notice-and-takedown	'Expeditious' notice-and-takedown
Constrained suggested & related searches	No changes to suggested & related searches

As discussed earlier, between 2011 and 2012, Ed Vaizey, on behalf of DCMS chaired a series of roundtables with search engines, rights holders and trade associations (Bradwell 2012). Prominent trade associations attending the meetings were the Federation Against Copyright Theft, British Phonographic Industry, and the Motion Picture Association of America. Google, Yahoo and Bing participated in the roundtables. Information on the roundtables comes from

²⁵⁵ Some rights holders use this strategy to address the sale of counterfeit goods. Interview with Roxanne Elings, Co-Chair, Global Trademarks/Brand Management Practice, Greenberg Traurig LLP, 20 March 2012, New York City.

U.K. Open Rights Group, a civil-advocacy association, which successfully filed freedom of information requests and obtained meeting minutes and lists of attendees (Bradwell 2012).

Meeting minutes reveal that intellectual property actors wanted search engines to alter their enforcement measures substantially to counter infringing sites (see Table 5.1). In November 2011, rights holders proposed a code of conduct that they wanted search engines to adopt (see Appendix E; Bradwell 2011). Google, Yahoo and Bing balked at this proposal. Jeremy Hunt, who was then the Secretary of State at the DCMS, instructed the search engines to create their own code in consultation with rights holders (Bradwell 2011). In February 2012, the search engines presented their code of conduct (see Appendix D). This code is the first of its kind anywhere for search engines.

The differences between the two codes are striking. The two codes indicate that intellectual property actors and search engines had starkly divergent ideas, at least between late 2011 and early 2012, of how search intermediaries can and should be responsible for regulating infringing sites. Rights holders proposed five key areas where they wanted search engines to revamp their enforcement processes (see Appendix E):

1. They wanted repeatedly infringing sites to be demoted (i.e., de-prioritized) in search engines' rankings of search results. This measure was intended to promote legitimate sources of content and encourage consumers to choose a top-ranked legitimate source instead of an infringing site.
2. Rights holders wanted sites certified by industry to be prioritized in search rankings. This measure was also intended to boost the rankings of legitimate sources.
3. Rights holders wanted any site subject to a court order to be removed automatically and rapidly from search results. This would mean that sites blocked by court order in the United Kingdom, like The Pirate Bay, would be de-indexed from search results.

4. They wanted notice-and-takedown programs to have an “expeditious process” in which rights holders could take advantage of “automated tools” for the “rapid removal and disabling of infringing links.”

5. Rights holders also wanted to curtail certain types of search practices. They wanted to limit “autocomplete” or “suggested” searches in which search engines suggest search terms as users are typing.²⁵⁶

This measure was intended to ensure consumers were not directed toward illegal content.

The search engines largely rejected rights holders’ demands. They did not include measures to demote search results, prioritize certified sites, or de-index sites subject to court orders. They also ignored requests to make changes to suggested-search functions. Instead, the search engines’ code of practice largely reiterates their existent notice-and-takedown procedures but stipulates that they should undertake “expeditious” processing and “eliminate inefficiencies” (Appendix D). Of note, the search engines suggested several practices to guide rights holders’ complaints. They instructed rights holders to deal with infringing sites directly before complaining to search engines and then submit only narrow and specific removal requests. The code suggests that rights holders should be “accountable for improper notices” made to search engines, make complaints publicly available, and to agree to reasonable appeals processes (Appendix D). Unsurprisingly, rights holders and trade associations attending the roundtable meeting expressed “disappointment” that the code did not include any of their key demands (Bradwell 2012). Given the secrecy of the roundtables, it is unclear if the search engines’ code is currently in force, been discarded, or amended to reflect rights’ holders and state’s preferences for tougher enforcement measures.

b) Changes to Google’s Enforcement Practices

Despite the stark differences between the rights holders’ and search engines’ codes of conduct between late 2011 and early 2012, Google’s policies were moving closer to those demanded by rights holders (see Table 5.2). Prior to the

²⁵⁶ Google’s Autocomplete works using algorithms to predict and shows search queries as you type based on the searches of all Google’s users. Google defends the feature by saying that it reflects all search activities (however odd or objectionable) and reflects diversity on the Internet.

rights holders' release of their code in November 2011, Google announced several changes to its enforcement policies. These changes included amendments in two areas (autocomplete and search demotion) that Google had long resisted changing. In December 2010, Google announced on its Policy Blog that it planned to prevent "terms that are closely associated with piracy" from appearing in Autocomplete (Walker 2010). This was one of rights holders' principal demands in their proposed code of conduct. Google implemented the changes to Autocomplete in January 2011. The second change concerned search demotion. Google had argued for years that it would not alter its algorithms that indexed and ranked its search results. In August 2012 the search giant capitulated. Google announced it would amend its search algorithms to consider the number of "valid copyright removal notices" against sites and then demote search results from sites with a "high" (unspecified) number of removal notices (Singhal 2012).

Table 5.2: Comparison of Proposed and Actual Rules for Search Engines

Rights holders' code	Search engines' code	Google's Policies
Demote repeatedly infringing sites	No demotion policy	Demotion policy introduced in August 2012
Prioritize certified sites	No such policy	No such policy
Stop indexing sites subject to court orders	No such policy	No such policy
'Improved' notice-and-takedown	'Expeditious' notice-and-takedown	'Streamlined' notice-and-takedown
Constrained suggested & related searches	No such policy	Changes to Autocomplete feature introduced in January 2011

Google's policy changes in this area would appear to indicate that it is giving in to long-term sustained pressure and threats of legal action and legislation from rights holders and governments. By changing its Autocomplete feature and demoting infringing search results, Google addresses critics' biggest criticism that it facilitates infringement by guiding consumers toward unauthorized

content instead of emphasizing legitimate content.²⁵⁷ However, Google is also increasingly becoming a content owner (e.g., paid YouTube channels) that must protect its intellectual property. As Google operates multiple services—search, advertising, and content distribution—its interests in addressing infringement are becoming more diverse.

ii) ***Domain Intermediaries' Enforcement Policies***

Given the complexity of registrars' operations, companies like GoDaddy have multiple methods to regulate the domain names they register to individuals or companies (see Table 5.3).²⁵⁸

1. They can change the name of the registrant (i.e., who registered domain name) to another party. This can involve changing the name from an individual accused of infringement to the rights holder.
2. They can prevent the transfer of a domain name. This can be done while an investigation or court proceeding is undertaken.
3. They can cancel a domain name. This means that the name goes back into pool of available names that anyone may register.
4. They can transfer the domain name to a different registrar. Courts may order the registrar to hold the name in trust pending the outcome of a case.
5. They can suspend DNS resolution (also called 'seize and takedown'). The domain name will not resolve to its proper site and will instead show an error message.²⁵⁹
6. They can redirect domain resolution (also called 'seize and post notice'). The domain name will not properly resolve and will instead be directed to another webpage with, for example, a banner warning against purchasing counterfeit goods.

²⁵⁷ This was a complaint by rights holders at the U.K. roundtable and a demand in the code of conduct rights holders drafted for the search engines (Bradwell 2011).

²⁵⁸ ICANN published a helpful how-to guide on how domain name seizures and takedowns can be undertaken (Piscitello 2012).

²⁵⁹ The domain name system may be return a "false No Such Domain signal, simulating network loss and let the question 'time out'" or use the "Administrative Denial response code" (Vixie 2012).

Table 5.3: Domain Intermediaries' Enforcement Measures

Technique	Result
Change registrant name	Registrant loses domain name
Prevent transfer of domain name	No change or modification of name
Delete domain name	Domain returns to common pool
Transfer to different registrar	Transfer to new registrar
Suspend DNS resolution (seize & takedown)	No resolution (e.g., site not found)
Redirect DNS resolution (seize & post notice)	Redirection to warning page

Seize and post-notice measures, which involve redirecting domain names to warning banners, are an increasingly common way to deal with infringing sites. David Lipkus, an associate with Kestenberg, Siegal, and Lipkus, LLP in Toronto, says that some rights holders he works with seek court orders to “point the domain name to their authorized website so even if you are looking for ‘brand fakes.com’ you’ll end up at the authorized site for that product.”²⁶⁰

a) Centre for Safe Internet Pharmacies

The Centre for Safe Internet Pharmacies (CSIP), as discussed earlier, provides a useful case in which to examine how domain registrars undertake enforcement against online infringement through non-binding private enforcement agreements. In addition, by focusing on CSIP, the researcher can examine pressure from the U.S. government and the pharmaceutical industry on macro-intermediaries to crack down on unauthorized online pharmacies.

In July 2012, a group of Internet intermediaries—led by Google and GoDaddy—officially launched CSIP. This followed an agreement macro-intermediaries struck with Victoria Espinel, head of IPEC, in 2010. CSIP brings together firms representing payment, search, domain name, and advertising sectors. Marjorie Clifton, CSIP’s executive director, describes the centre as providing “a first-ever private sector solution” to the problem of illegal online pharmacies (Clifton

²⁶⁰ Interview with David Lipkus, Associate, Kestenberg, Siegal, and Lipkus, LLP, Toronto, Canada, 10 August 2012.

2012).²⁶¹ CSIP focuses on consumer education, information sharing, and, more unusual in a non-profit, non-governmental organization, private enforcement efforts against unauthorized online pharmacies (IPEC 2013:36). By creating CSIP under the auspices of IPEC, Espinel legitimized private regulatory efforts against unauthorized online pharmacies.

Online pharmacies in the United States must operate according to federal and state laws regarding the use of prescriptions and the distribution of pharmaceuticals (GAO 2013). Some states in the United States, for example, have laws prohibiting prescriptions from being issued online and instead require in-person prescriptions (GAO 2013). This means that an online pharmacy operating legally outside the U.S. jurisdiction may be in violation of U.S. federal or state laws regarding the advertisement, prescription, sale and distribution of pharmaceuticals if they target individuals in the United States. As used by enforcement actors, the term “illegal online pharmacies” refers to sites that distribute over-the-counter and/or prescription pharmaceuticals that may be unsafe, poor quality, counterfeit, or unapproved and/or issued in the absence of appropriate prescription processes (GAO 2013). This is an incredibly broad concept that combines safety concerns (e.g., poor quality and counterfeit medication) with procedural concerns (how prescriptions are issued). It encompasses sites peddling misbranded, unapproved or adulterated medication, as well as pharmacies that offer professional services and legitimate, safe medication.

Christine Jones, GoDaddy’s former general counsel and executive vice president, describes the role of members of CSIP as working “to eviscerate the online sale of counterfeit and otherwise illegal prescription drugs” (Berkens 2011). As a member of CSIP, GoDaddy voluntarily withdraws its services from sites identified as illegal online pharmacies. GoDaddy receives tips from the public about suspected wrongdoing in relation to sites distributing pharmaceuticals. It also accepts complaints from LegitScript, which operates what it claims is the “world’s largest database of Internet pharmacies.”²⁶² LegitScript sells its monitoring and investigative services to pharmaceutical

²⁶¹ According to Clifton, CSIP is also involved in creating a ‘white list’ of approved Internet pharmacies in cooperation with other private-sector partners (Clifton 2012).

²⁶² On its website, LegitScript describes how it monitors clients’ platforms for illegal online pharmacies, see: <http://www.legitscript.com/services/monitoring>

rights holders. The company is an ex-officio member in CSIP. As part of its role with CSIP, LegitScript uses set of publicly available standards that it devised to evaluate pharmacies as legitimate, unverified (subject to ongoing review), or unapproved according to whether LegitScript determines if they are compliant with U.S. law.²⁶³

The Centre for Safe Internet Pharmacies releases little data on its members' enforcement activities on its website, but there are indications of its efforts from other sources. CSIP's members are involved in the annual Operation Pangea, a weeklong, international project coordinated by Interpol to crack down on problematic online pharmacies. GoDaddy and other members of CSIP, like Google and PayPal, work with federal and state law enforcement agencies and regulatory bodies like the U.S. Food and Drug Administration. As part of Operation Pangea, CSIPs' members shut over 18,000 sites in 2012 and over 13,700 in 2013 (Interpol 2012; Interpol 2013). By drawing together macro-intermediaries from the payment, search, advertising and domain name sectors, CSIP has a considerable regulatory capacity. As its members have committed to addressing illegal online pharmacies, they are a valuable resource for law enforcement or state regulatory bodies, like Interpol and the U.S. Food and Drug Administration, to draw upon.

IV) Analysis of Intermediaries' Enforcement Measures

The two private enforcement agreements examined in this chapter reveal the roles of search and domain macro-intermediaries in the private regulatory regime. Chapter 4 illustrated the payment and advertising components of the regime, which can enact revenue chokepoints, while this chapter focuses on macro-intermediaries that can thwart access to infringing sites. Google and GoDaddy, the dominant firms in their industry sectors, are technologically sophisticated regulators that use complex algorithms to deliver and rank searches, register domain names, and to monitor their platforms for violations of their policies.

²⁶³ LegitScript created criteria to determine the legality of online pharmacies, including whether it is licensed or registered, complies with regulations pertaining to controlled substances, and dispenses medication using a valid prescription process, see: <http://www.legitscript.com/pharmacies/standards>

Both firms have a capacity for mass policing: Google removes hundreds of millions of search results and GoDaddy cancels the domain names of thousands of sites. Neither removes content from the targeted sites but only impairs access to those sites. Search and domain macro-intermediaries are prolific in their regulation but not particularly effective. In relation to search, the sites are still accessible to individuals that can find its domain name elsewhere.²⁶⁴ Site operators that lose their domain names can shift to another domain name registrar. In contrast to the online payment sector, which is dominated by a small number of companies, there are many providers of domain names, although GoDaddy is the largest. Sites can obtain a domain name from a small, relatively unknown domain registrar and function effectively. However, these sites cannot rely upon a small, relatively unknown payment firm as the sites must provide payment services that consumers will trust and use.

i) *Google's Regulatory Capacity*

Google has a tremendous regulatory capacity to respond to complaints from rights holders and trade associations about problematic search results. The number of requests to Google for the removal of infringing links is skyrocketing, with 214 million removals in 2013 and 100 million for the first four months of 2014 (Ernesto 2014a; Google Transparency Report). This explosion in requests occurred after the failure of PIPA and SOPA in 2012, which suggests that rights holders are able to use existing legal avenues to address complaints of copyright infringement. Currently, Google is only removing a small portion of results linking to sites selling counterfeit goods. SOPA would have required search engines to remove results linking to sites selling counterfeit goods as well as copyright infringing content. With the death of this bill, trademark owners do not have the same access as copyright owners to remove infringing links, however, the traffic to sites selling counterfeit goods is much less than that to sites offering unauthorized downloads.

²⁶⁴ For well-known sites like The Pirate Bay, users do not need search engines. For other, lesser-known sites, they can use links from other webpages to point to their sites.

Despite Google's regulatory capacity as a macro-intermediary, its enforcement efforts against infringing sites are relatively ineffective. Search engines can only remove hyperlinks to content but do not impair access to the site itself. Google is a prolific regulator but there is little evidence that this regulatory strategy is effective at reducing copyright-infringing content. In fact, there is a serious problem with complainants' submission of improper removal notices, which results in search engines wrongfully removing legitimate, non-infringing content (Quilter and Urban 2006). Google, Yahoo and Bing highlight this problem in their code of conduct and propose that rights holders' narrowly target search results and be held accountable for wrongful removals (Appendix D). The scale of wrongful removals is unknown because Google does not specify reasons for all the requests it denies. In 2013, for example, Google denied 21 million requests for various reasons, including that they were duplicates of other requests, inaccurate or made claims involving intellectual property owned by another party (Google Transparency Report).

Google has adopted policies to streamline and speed up its enforcement practices. In 2012, for example, Google created the Trusted Copyright Removal Program to fast-track complaints from complainants with "a proven track record of submitting accurate notices" and "a consistent need to submit thousands of URLs each day" (Google 2013). This program is designed to serve reporting agencies that submit 95% of the URLs Google receives (Google 2013). These include the British Recorded Music Industry and Recording Industry Association of America, as well as private monitoring and investigative firms, like the multinational U.S.-based MarkMonitor. Google's removal of over 97% of search results for which it receives complaints indicates that the company errs on the side of removing links rather than refusing requests (Google 2013). Google's creation of the trusted members' program indicates the degree to which large trade associations dominate copyright enforcement. It also demonstrates the growth of the intellectual property protection industry as companies like MarkMonitor collectively file tens of millions of requests for the removal of search results from Google annually. These companies and trade associations wield significant power as they distinguish 'legitimate' from 'infringing' search results in the absence of any judicial process and issue requests for Google to de-index the search results. As Google continues to adopt more enforcement-

friendly policies, these actors will be able to submit ever-increasing numbers of removal requests and thereby shape the kind of content and technologies that users can access.

ii) ***GoDaddy's Regulatory Capacity***

Like Google, GoDaddy has a significant regulatory capacity as the largest domain name registrar. GoDaddy can incapacitate domain names through a seize-and-takedown action, which means that the site will not be found or an error message will be displayed. It can also perform a seize-and-post-notice action, which means that sites will be redirected toward a warning banner. Both actions mean that the sites will not resolve properly.²⁶⁵ Unlike Google, GoDaddy does not publicly track its enforcement activities but it does release some information about the scale of its regulatory efforts. For example, GoDaddy worked with U.S. regulators to take down over 36,000 illegal online pharmacies in 2010 and 47,000 such sites in 2011 (Clifton 2012).

Efforts by GoDaddy and other domain registrars have been successful in pushing operators of infringing sites to less-reputable domain registrars. John Horton, president of LegitScript, which monitors the compliance practices of online pharmacies, calculates that 80% of registrars have effective policies. He claims that unscrupulous site operators “cluster at a handful of domain name companies” that are so-called “rogue registrars” for their inadequate regulation of their registrants’ activities (PR Newswire 2013). Existing regulatory policies, such as ICANN’s accreditation of registrars, and domain registrars’ withdrawal of services from non-compliant site operators are effectively shifting bad actors to a small number of less-scrupulous registrars. Macro-intermediaries like GoDaddy are unable to deal with site operators who do not use their services. This is why Victoria Espinel advocated a multi-intermediary regulatory approach for the Centre for Safe Internet Pharmacies. Domain, search, payment and advertising macro-intermediaries working together in a coordinated approach are more likely to disable infringing sites more effectively.

²⁶⁵ These actions are also respectively referred to as suspending or redirecting DNS resolution.

GoDaddy's regulatory efforts against infringing sites, like those of Google, have limited efficacy. The strategy of seizing domain names (either accompanied with takedowns or post-notice actions) does not affect the sites' content. Enforcement strategies that only target sites' domain names are "disruptive" at most, a fact acknowledged by U.S. government officials in interviews with the U.S. Government Accountability Office in a review of regulatory efforts against illegal online pharmacies (GAO 2013). Sites that lose their domain names can easily obtain another and resume operations quickly once users are aware of the new domain name, as recent scholarly studies have found (e.g., Liu et al. 2011). This dissertation concludes that payment providers are more effective at disabling sites than domain registrars, which corroborates analysis of domain intermediaries' regulatory capabilities against infringing sites (Liu et al. 2011).

Infringing sites' movement among domain registrars to avoid enforcement action brings to mind the whack-a-mole phenomenon discussed earlier. If, however, the domain registrar operates web-hosting services for the targeted site, it can remove site content along with domain services. GoDaddy, as the world's largest domain registrar and web host, has a considerable advantage to withdraw both types of services from infringing sites. As a regulator of both domain names and hosted content, GoDaddy has significant regulatory capacity. The consequences of enforcement errors, however, are compounded as the registrar can essentially cripple a site by incapacitating its domain name and seizing its content. Google, in contrast, can only de-index a webpage from its search engine.

V) State Pressure and Actors' Interests

Returning to this dissertation's main question, why did Google and GoDaddy agree to adopt non-binding private enforcement agreements to guide their regulatory efforts against infringing sites? Like the payment and advertising macro-intermediaries, there were threats of legislation and legal action, and search and domain macro-intermediaries have financial and reputational interests in strengthening their enforcement practices, similar to those discussed in chapter 4. Consumers, meanwhile, are the missing constituency of

this regulatory regime, even though the Centre for Safe Internet Pharmacies is ostensibly dedicated to serving their interests.

i) ***The Role of the State***

State actors played pivotal roles in establishing both the search engines' code of conduct in the United Kingdom and the Centre for Safe Internet Pharmacies in the United States. The degree of coercive pressure, however, was considerably greater on Google than on GoDaddy. The search giant faced the possibility of legislation in both countries. In the United Kingdom, the government preferred industry-created regulation but was willing to legislate if there was no industry consensus. Former Secretary of State Jeremy Hunt delivered that warning to Google, Yahoo and Bing and then directed them to work with rights holders to draft a code of conduct (Bradwell 2011). In the United States, in contrast, the government was trying to pass COICA, a tough new intellectual property bill. While the debate over COICA was ongoing, Victoria Espinel, of IPEC, brought together domain name, search/advertising, and payment macro-intermediaries—all targeted under COICA—and “challenged” them to come together to address illegal online pharmacies (IPEC 2011).

In addition to the threat of legislation in the U.S. and U.K., as described above, Google faced a criminal investigation for accepting advertisements from unauthorized pharmacies and the search giant forfeited \$500 million (DOJ 2011). Pressure from the U.S. pharmaceutical industry, which is a powerful voice for strong intellectual property laws, likely influenced the U.S. government to crack down on Google. The Centre for Safe Internet Pharmacies, for example, has among its members the Alliance for Safe Online Pharmacies. This Alliance represents pharmaceutical companies and pharmacies, as well as other health care providers.²⁶⁶ Moreover, U.S. pharmaceutical companies are the most vocal critics of online pharmacies, particularly those that do not operate according to U.S. state and federal laws (see GAO 2013).

²⁶⁶ Pharmaceutical companies have aggressively pursued stronger protection for its intellectual property since the 1970s, including tougher measures on parallel importation (Drahos and Braithwaite 2002).

Politicians in the United Kingdom clearly indicated their preference that Google take a stronger stance against online infringement. Members of the House of Commons Culture, Media and Sport Committee pronounced that they were “unimpressed by [Google’s] evident reluctance to block infringing websites on the flimsy grounds that some operate under the cover of hosting some legal content” (House of Commons 2013:3). They further argued that the “continuing promotion by search engines of illegal content on the Internet is unacceptable” and Google’s attempts to address the problem “have been derisively ineffective” (House of Commons 2013:3-4).

GoDaddy, in contrast, has elicited no similar criticism from policymakers. There is no publicly available information indicating that Espinel or other government officials pushed GoDaddy to adopt non-binding enforcement measures. Given GoDaddy’s strong support of industry and voluntary enforcement efforts as evidenced in Christine Jones’ testimony to the U.S. Congress, it is probable that the company joined IPEC’s initiatives voluntarily.

ii) *State and Corporate Interests in Informal Private Regulation*

Search and domain macro-intermediaries’ financial and ideational interests affect how they undertake the regulation of infringing sites. In contrast with the other macro-intermediaries, there is little publicly available information of how GoDaddy came to adopt non-binding enforcement agreements. There are several reasons that explain this lacuna. GoDaddy has a much lower public profile than the other macro-intermediaries. As a privately held company, it publishes few details of how it deals with violations of its policies. GoDaddy is also a relatively new entrant into the realm of intellectual property protection, although it has experience working against child pornography sites alongside PayPal, Google and Visa. Rights holders have not publicly targeted GoDaddy to crack down on infringement. GoDaddy has financial interests in protecting its services and users from wrongdoing and preserving its brand from being associated with counterfeit goods. Like the other macro-intermediaries, GoDaddy wants to maintain its dominant market position.

Like GoDaddy, Google has an interest in protecting its valuable brand from being associated with criminality. Google does not contest that infringement is a problem but disagrees with rights holders over the regulatory strategy of relying upon search engines to remove linkages to infringing sites. Indeed, Kent Walker, senior vice president and general counsel of Google, argues that shutting down sources of revenue is a more effective enforcement avenue (Walker 2011:7). Google has material interests in shifting the regulatory focus away from its search engine practices but, as the digital advertising giant, it would continue to address the problem of infringement by policing its advertising services.²⁶⁷ Google's ideational interests affect how it regards the regulation of infringement. "It's not Google's job to go around the web to declare whether sites are legal or illegal," said Theo Bertram, manager of U.K. public policy for Google at an industry-sponsored event to discuss how funding sources for online infringement could be throttled (Bertram 2013).²⁶⁸ To "edit the web and literally delete sites," argued Eric Schmidt, Google's chief executive officer, "goes counter to our philosophy" (Ernesto 2013).

Google's critics, however, argue that the company has the resources and technical skill to address the problem of infringement but not the requisite commitment. Detective Superintendent Wishart of the City of London Police argues that Google's resistance to modifying its search processes to screen out content that infringes intellectual property is hypocritical:

Google has said to us that they are massively reluctant to police the Internet, massively reluctant to do anything where they are perceived to be influencing peoples' choices or intrusively looking at what people are doing. Our argument is, 'you do that anyway. You do that from the commercial perspective.'²⁶⁹

²⁶⁷ Google also offers a payment service—Google Wallet—that it would presumably regulate to ensure it does not facilitate payments of infringing goods. Google has only a tiny share of the online payment sector, which is a highly competitive market and dominated by Visa, PayPal, MasterCard and American Express.

²⁶⁸ Bertram did not disregard Google's role as a regulator, particularly in relation to its advertising services. He went on to say "but if Coca-Cola comes to us and says 'here's a list of 500 dynamic sites, and we don't want you to place ads on those...' that's a slightly different thing" (Bertram 2013).

²⁶⁹ Interview with Det./Supt. Bob Wishart, Head of National Operational Delivery, Regional Fraud Project, City of London Police, 6 September 2012, London.

These critiques aptly illustrate the differing interests Google has toward the regulation of online infringement. Google claims an ideological position against censorship but it has strong economic interests in crawling certain types of sites and prioritizing specific types of information in its search index. Its ideational position on removing search results; however, is likely tempered by its dependence on its advertising services for its revenue. Google's desire to mitigate the risk from legislation and legal action also influences its decisions to adopt voluntary measures to strengthen its enforcement efforts. Patrick Robinson, former director of public policy at Yahoo in the United Kingdom, remarked that search engines' removal of infringing links does not indicate an "admission" that the content is infringing but rather a desire to avoid legal action from rights holders (Bradwell 2012). By removing problematic search results for rights holders and amending its enforcement policies, Google is mitigating the possibility of future legal action from rights holders and states.

iii) *Consumers' Interests*

Consumers' interests are ostensibly at the heart of discussions among rights holders, macro-intermediaries, and the U.S. and U.K. governments over infringing sites. In reality, however, the private enforcement agreements are primarily designed to serve large corporations whose interests do not always align with those of consumers. Similar to chapter 4, there was no representation from consumers in the creation of the agreement that launched the Centre for Safe Internet Pharmaceuticals or the search engines' code of conduct. Little information is publicly available of these state-negotiated agreements. Further, the U.S. and U.K. governments, along with intellectual property actors, strategically used closed-door meetings to draft the enforcement measures in secret and side step controversial and stalled legislation.

CSIP is unlike the other informal agreements that Victoria Espinel negotiated as head of IPEC because CSIP focuses on a particular type of infringing site, so-called illegal online pharmacies. Online pharmacies that sell or advertise pharmaceuticals in violation of states' laws can pose health and safety risks to consumers (GAO 2013). However, some of these pharmacies may only violate

U.S. laws on prescriptions but provide safe, genuine medication. On the surface, its mission appears to serve consumers' interests as CSIP promotes safe purchases of medication from approved, accredited online pharmacies.

Consumers' interests in purchasing medication for the best possible prices do not always align with the interests of large, multinational pharmaceutical companies intent on protecting their profit margin. The pharmaceutical pricing structure set by U.S. pharmaceutical companies means that pharmaceuticals are typically more expensive in the United States than other countries, and, in consequence, consumers often seek medication from online pharmacies that may not be licensed for operation in the United States (GAO 2013). As a result, consumers may be unfairly caught in a situation between legally accessible, less-affordable medication and (some) unauthorized pharmacies that provide safe, affordable medication. State and industry efforts to crack down on all types of unauthorized online pharmacies, even those that supply safe medication, does not serve consumers' interests, particularly in the United States where many individuals struggle to afford pharmaceuticals (see GAO 2013).

The principal problem with CSIP is that it relies upon corporate actors connected to the pharmaceutical industry to identify "safe" pharmacies. LegitScript verifies pharmacies on behalf of government and corporate clients, including pharmaceutical companies. CSIP can then encourage its members to withdraw their services from targeted sites. State and industry actors benefit from CSIP's global network of macro-intermediaries. Government actors, particularly the U.S. Food and Drug Administration, can reach extra-territorially to police sites that it contends are distributing pharmaceuticals to individuals in the United States in violation of federal and state laws (GAO 2013).²⁷⁰ Rights holders (pharmaceutical companies) benefit from CSIP's considerable regulatory capacity and the ability of its macro-intermediary members to withdraw services from targeted online pharmacies. Consumers, however, may

²⁷⁰ The U.S. Food and Drug Administration uses informal enforcement measures to request Internet service providers and domain name intermediaries to withdraw their services from pharmacies over which the FDA has no jurisdiction but designates as operating illegally within the United States (see GAO 2013).

be much worst off if they lose access to pharmacies that prescribe safe, affordable medication.

In terms of search engines, the creation of the code of conduct—the first in the world—demonstrates the close, inter-dependent relationships between intellectual property owners and the U.K. Department for Culture, Media and Sport. Minutes and proposed codes of conduct from the roundtable meetings demonstrate that rights holders had the full support of Ed Vaizey, Parliamentary Under-Secretary, and Jeremy Hunt, then Secretary of State to create private enforcement agreements. Non-binding agreements among key industry actors enable the government to bypass its unpopular and stalled *Digital Economy Act*. These roundtable discussions, in which rights holders proposed to change fundamentally how search engines operate, have the potential to alter how individuals access information and can use search engines. Such discussions that can affect critical Internet services, like search, payment and domain names, should not left to small groups of corporate and government actors in closed-door meetings.

VI) Conclusion

The two private enforcement agreements examined in this chapter—the Centre for Safe Internet Pharmacies and the search engines' code of conduct—illustrate the complex, loosely coordinated private regulatory regime. Actors from the Office of the Intellectual Property Enforcement Coordinator and the Department for Culture, Media and Sport are central figures in the regime as they secured macro-intermediaries' participation in negotiations with rights holders and facilitated the creation of the agreements. The role of state actors is paramount to this regime because rights holders alone did not have the requisite authority to bring together all the macro-intermediaries involved in CSIP or direct Google, Yahoo and Bing to draft a non-binding code of conduct. By compelling Google and GoDaddy into talks through threats of legislation and legal action, IPEC and the DCMS legitimized rights holders' demands that macro-intermediaries assume greater regulatory responsibility for online infringement. As a result, rights holders' authority to pressure macro-intermediaries to amend their enforcement practices can be seen as partially

derived from the state (see Büthe 2010; Hall and Biersteker 2002; Sassen 2002).

A principal component of techno-regulation—the shaping of human behaviour through technology—is that technology and politics mutually shape one another (Brey 2005). This was evident in the U.K., for example, when rights holders and politicians pressured search engines to demote repeatedly infringing sites in their search indices. Google announced it has adopted this practice, thus showing how certain interests can shape intermediaries' use of technology to police wrongdoing on their platforms (Singhal 2012). For search engines, however, changes to the ways they detect and control perceived wrongdoing among search results affects the results they display to users and how they rank those results.

State and corporate pressure on Google to amend its enforcement practices in relation to intellectual property can have profound consequences on Google's overall operation of its search engine, which can negatively affect how users search for and access information. Certain types and sources of information could be rendered inaccessible or relegated far down in the rankings of search results. In a similar fashion, GoDaddy, working through the Centre for Safe Internet Pharmacies along with other macro-intermediaries, is shaping how consumers can purchase pharmaceuticals online and what types of pharmacies are designated as "safe." Google and GoDaddy's regulatory efforts through informal, privately drafted measures demonstrate the ways in which macro-intermediaries' regulatory practices can affect the provision and use of key Internet services, as well as the types of products individuals can access.

Chapter 6: Online Marketplaces and Private Enforcement Agreements

Online marketplaces have fundamentally transformed how consumers and businesses buy and sell goods and services. With the creation of eBay in 1995, individuals have convenient, real-time access to a global marketplace. From their homes individuals can buy and sell products from around the world. In many ways these marketplaces are fundamentally different from their brick-and-mortar counterparts. Online marketplaces do not handle or sell the goods themselves, nor do they verify products' quality, legality or authenticity (eBay 2013a). Instead, they facilitate commercial transactions between parties. The U.S.-based eBay and the China-based Taobao marketplace are the two largest online marketplaces globally. They are consumer-to-consumer platforms, which blur the lines between consumers and merchants as they allow individuals to buy and sell goods with other individuals globally.

Since the creation of online marketplaces, unscrupulous individuals have used them to sell illegal or controlled goods, such as drugs, weapons, endangered species or counterfeit goods (see e.g., Lehrer 2012). With the growing popularization of online shopping in the early 2000s, prominent multinational rights holders began to complain that the marketplaces contain numerous sales listings for counterfeit goods (i.e., "infringing listings"). This chapter focuses on eBay and Taobao because rights holders, particularly those with well-known, sought-after brands, and their trade associations argue that these marketplaces have significant problems with the sale of counterfeit goods on their platforms.²⁷¹ This is because they serve massive populations, have significant market share and are therefore an efficient way for individuals to sell counterfeit goods.

eBay operates globally and has 128 million active users (eBay 2013). The China-based Taobao, meanwhile, boasts 231 million active users, along with its sister marketplace Tmall, which operates storefronts that businesses sell to

²⁷¹ This is according to my interviews with rights holders, investigative firms, attorneys and trade associations in Australia, Canada, the United States and the United Kingdom.

consumers (Alibaba 2014). Taobao, created in 2003, is a Chinese-language marketplace that primarily operates in China. Taobao is of particular concern to U.S. and European rights holders because, as China's largest online marketplace, it is an ideal entry point into the Chinese e-commerce market and rights holders want the marketplace's hundreds of millions of users to purchase authentic products. Further, Taobao is part of the massive, China-based Alibaba Group, which, among its many services, operates several online marketplaces and a payment provider, and is one of the top three e-commerce platforms in China.²⁷²

eBay and Taobao represent an important component of the private regulatory regime because they facilitate a massive volume of trade, enable consumers to sell to one another, and have hundreds of millions of users. Both marketplaces use technology as a regulatory instrument as they have sophisticated surveillance and enforcement programs to detect wrongdoing on their platforms and remove problematic listings or sellers. eBay, with its global scope, massive trading volume and dominant market share, is a macro-intermediary. Taobao, in contrast, operates primarily within China and does not have the global scope to be considered a macro-intermediary. However, given its size and market dominance in China, it has a considerable regulatory capacity to control the online distribution of counterfeit goods on its marketplace.

In 2011, both eBay and Taobao signed non-binding enforcement agreements with rights holders to strengthen their enforcement policies and practices. eBay joined a memorandum of understanding to regulate the distribution of counterfeit goods through marketplaces in the European Economic Area.²⁷³ Taobao signed a memorandum of understanding with an influential trade association, the International Anti-Counterfeiting Coalition. Similar to the agreements adopted by other macro-intermediaries discussed in chapters 4 and 5, the coercive pressure of the state was at the centre of both agreements. The European Commission facilitated the creation of the European agreement and warned industry stakeholders that legislation would be considered if a

²⁷² The other two dominant e-commerce companies in China are Baidu, a search giant, and Tencent, an online gaming company (*The Economist* 2014).

²⁷³ The European Economic Area is comprised of the European Union and member states of the European Free Trade Area, Iceland, Liechtenstein, and Norway.

“voluntary” agreement were not reached (European Commission 2009). Taobao signed its agreement because, at the time, it was listed on the Notorious Market List operated by the Office of the U.S. Trade Representative (USTR).²⁷⁴ Taobao’s adoption of the agreement was a factor in its release from the list in 2012. In addition to direct pressure from the European Commission and the USTR, both marketplaces have financial and reputational interests in working with rights holders, similar to the other macro-intermediaries examined. The marketplaces want to mitigate their risk of legal liability, establish a degree of regulatory certainty as to their enforcement responsibilities, and protect their corporate reputations from association with counterfeit goods.

As will be discussed later in the chapter, the United States does not have legislation pertaining to online trademark infringement.²⁷⁵ The European Union, in contrast has legislation that governs how online marketplaces deal with counterfeit goods and the European Commission’s private agreement builds upon that legislation. In contrast with the other macro-intermediaries, marketplaces would not have been targeted under the *Stop Online Piracy Act* or its predecessors. However, marketplaces’ informal private agreements are similar to those of the other macro-intermediaries. Through their private agreements, eBay and, in particular Taobao, significantly altered their regulation of the third-party distribution of counterfeit goods on their platforms. Their enforcement efforts are more rapid, streamlined, and proactive than their previous enforcement measures. Further, marketplaces’ private agreements can be understood as embodying the spirit of SOPA as these agreements encourage marketplaces to institute what the European Commission calls “beyond-compliance” regulatory strategies (European Commission 2013).

This chapter examines how and why eBay and Taobao adopted non-binding enforcement agreements. The rest of the chapter proceeds in five parts. First it briefly introduces eBay and Taobao and then describes how the marketplaces

²⁷⁴ The USTR’s Notorious Market List, published in the Out-of-Cycle Review, is part of the Special 301 process described in chapter 3. The USTR listed Taobao as a notorious market in 2008 and removed it in 2012 after the USTR judged that Taobao had instituted sufficiently improved enforcement practices.

²⁷⁵ Marketplaces in the United States are subject to the 1998 *Digital Millennium Copyright Act* in relation to copyright infringement but there is no similar statutory measure for online trademark infringement.

operate. Next, the chapter examines state and industry pressure on the marketplaces to adopt the private enforcement agreements. Third, the chapter examines two private agreements: the European Commission's agreement with eBay and Taobao's agreement with the International Anti-Counterfeiting Coalition. Fourth, the chapter analyses these programs and then, in the fifth section, examines the role of the state and actors' interests in the regulatory regime. The chapter then provides a brief conclusion.

I) Online Marketplaces

Online marketplaces are an integral feature of the digital economy. They use a wide variety of business models: some sell goods directly to consumers while others provide only the interface and support for third-party users (buyers and sellers) to carry out transactions. For example, the U.S.-based Amazon and the China-based Tmall marketplace, which is owned by the same company as Taobao, the massive Alibaba Group, enable businesses both large and small to sell their products directly to consumers through their platforms.²⁷⁶ Goods may be sold for fixed fees or through a variety of types of auctions. These marketplaces allow businesses to buy and sell goods at a far lower cost than their previous distribution models allowed and reach consumers and markets that would otherwise be inaccessible or prohibitively expensive.

i) *eBay and Taobao Marketplaces*

Marketplaces like eBay and Taobao that offer a broad diversity of newly manufactured and second-hand goods serve consumers' desire for multiple types of products at a range of prices. They also allow consumers to trade in secondary-market goods, such as second-hand clothing or nostalgia items like vintage video games, toys and jewellery. With the growth of consumer-to-consumer marketplaces like eBay and Taobao, individuals began to supplement their incomes by selling goods online and small businesses exploited the platforms to serve new and existing markets.

²⁷⁶ Another category of marketplaces is business-to-business platforms like the China-based Alibaba marketplace, owned by the Alibaba Group, in which companies can purchase and sell goods at wholesale levels.

eBay, created in 1995, is one of the earliest online marketplaces, and remains the dominant consumer-to-consumer marketplace outside of China. In 2013, eBay claimed over 128 million active users and more than 550 million listings globally (eBay 2013:4). It generated \$14 billion in 2013 and has platforms in 1,000 cities around the world. eBay is more than a marketplace: it describes itself as a “global ecommerce platform” with localized sites around the world, such as eBay.se in Sweden and eBay.co.uk in the United Kingdom (eBay 2013). It also operates marketplaces in a variety of countries, such as Gumtree, Kijiji, Marktplaats.nl, and mobile.de (eBay 2013).

To understand Taobao, one must situate it within the context of the Alibaba Group. Many outside China probably had little familiarity with the Alibaba Group until it filed its much-anticipated initial public offering in the United States in May 2014. Financial analysts estimate the deal could raise between \$15 and \$20 billion on a company with an estimated worth of anywhere between \$160 to \$250 billion (Owles 2014). The Alibaba Group is comprised of multiple businesses, including marketplaces, payment services, cloud storage businesses, and a search engine. In 2003, the Alibaba Group launched the Taobao marketplace (in Chinese the name means ‘hunting for treasures’) as a rival to eBay, which entered China in 2002. The eBay-Taobao rivalry was fierce but brief. Within three years of its birth, in 2006, Taobao had displaced eBay claiming 67% of the consumer-to-consumer market in China (Mitchell 2010). Jack Ma, executive chair of the Alibaba Group, remarked of the eBay-Taobao rivalry: “eBay may be a shark in the ocean, but I am a crocodile in the Yangtze River. If we fight in the ocean, we lose—but if we fight in the river, we win” (Wang 2010).

Taobao maintains a dominant presence in China’s e-commerce landscape, with 90% of China’s consumer-to-consumer market share in 2012 (Erickson 2012). As a Chinese-language site, over 98% of Taobao’s sales are made to consumers in China with fewer than two percent of users in the United States (Spelich 2012). The marketplace has approximately 800 million product listings on its marketplace (Erickson 2012). Alongside Taobao, one of the Alibaba Group’s other important marketplaces is Tmall, created in 2008. Tmall is China’s top business-to-consumer site with approximately 40 to 50% of the

market share in China, compared to Amazon²⁷⁷ at less than five percent (Millward 2013). Many U.S. and European rights holders regard Tmall as an entry point into the Chinese e-commerce marketplace and a way to access hundreds of millions of Chinese shoppers. For example, Tmall sells more than 70,000 multinational brands and Chinese brands (Spelich 2012).

eBay remains the marketplace leader in terms of generated revenue but Taobao and Tmall are rising rapidly. For the first 11 months of 2012, the Taobao and Tmall marketplaces surpassed the gross merchandise value of Amazon and eBay for 2012 (Alibaba 2013). This refers to the total value of merchandise that is sold over a particular period of time. Amazon and eBay together generated approximately \$155 billion in gross merchandise value in 2012, while sales from Taobao and Tmall accounted for \$161 billion (Alibaba 2013). Online commerce is growing about 60% a year in China, compared with 10% in the United States (Tabuchi 2014), making the Chinese e-commerce environment highly attractive to multinational rights holders. For example, on November 11, 2013, which is the Chinese equivalent of the “Black Friday” shopping day in the United States, Taobao and Tmall generated more than \$5.75 billion in sales in 24 hours (Millward 2013a). In comparison, shoppers spent \$1.9 billion in the United States for Black Friday and Thanksgiving sales (Carlson 2013).

ii) *How Online Marketplaces Work*

Online marketplaces enable Internet users from around the world to participate in different markets and create specialized markets (Casarosa 2009:4). Marketplaces are often categorized as to whether they facilitate transactions among businesses, provide businesses a platform to sell goods to consumers, such as Amazon or Tmall, or enable consumers to sell to one another, such as eBay or Taobao. There is, however, some blurring amongst these categories. While Taobao is China’s biggest consumer-to-consumer marketplace, it also contains storefronts through which merchants sell directly to consumers. Users

²⁷⁷ This chapter does not focus on Amazon because it is a business-to-consumer site (unlike eBay and Taobao) and rights holders claim that eBay and Taobao present a larger problem than Amazon in terms of the online trade in counterfeit goods.

can also adopt different roles: a wholesaler in one market and a consumer in another. “There are a lot of sites in China which are where people tend to buy in bulk,” explains Damian Croker, founder of BrandStrike, a London-based brand-monitoring firm. Those people then “maybe sell it on eBay or sell it in the markets or wherever.”²⁷⁸

Online marketplaces provide a venue for rights holders to reach consumers globally at a far lower cost than their previous distribution models (and thus potentially secure higher profits). These marketplaces are fundamentally different from traditional, brick-and-mortar stores as they only provide the interface and support for third-party users (buyers and sellers) to carry out transactions. Online marketplaces do not handle or sell the goods themselves nor do they verify the listings’ accuracy or the goods’ authenticity. eBay underlines this distinction in its User Agreement. “You acknowledge that we are not a traditional auctioneer. Instead, our sites are venues to allow users to offer, sell, and buy just about anything, at any time, from anywhere, in a variety of pricing formats and location” (eBay 2013a).

Buyers can generally register for free as marketplaces earn revenue by charging sellers various fees. eBay, for example, charges sellers fees for listing their products and upon the conclusion of sales.²⁷⁹ Taobao does not charge sellers for transactions, but rather charges them for marketing, shipping and advertising services, and export-related services such as customs clearance, logistics and cargo insurance (Alibaba 2011:22). Marketplaces also generate significant revenue by charging transactional fees for the use of their proprietary payment systems.²⁸⁰ The Alibaba Group owns Alipay, a payment processor with about 50% of the market share in China (Jackson 2014). eBay owns PayPal, which in 2012 generated 40% of eBay’s \$14.1 billion in revenues (eBay 2013).

²⁷⁸ Interview with Damian Croker, founder and CEO, BrandStrike Limited, London, 25 September 2012.

²⁷⁹ For eBay’s fees and services: http://pages.ebay.com/help/sell/fees.html#if_auction.

²⁸⁰ Amazon charges transaction fees for the use of Amazon payment services (ranging from 1.9% to 2.9%). For Amazon’s fee’s and services, see: <http://services.amazon.com/amazon-payments/pricing-plan.html>.

II) **Pressure on Marketplaces from Industry and State**

Given the size of eBay and Taobao and the hundreds of millions of people they serve and transactions they facilitate, rights holders are keen to ensure that they do not trade in counterfeit versions of their products. “The stand-alone [infringing] site is a lower priority than taking action on the trading platform,” explains Tim Waring, director of the U.K.-based Intelligence Technologies, a brand-monitoring firm, “because the trade platform has a much higher visibility than a stand-alone site.”²⁸¹ Rights holders’ strategy in relation to the distribution of infringing goods through legitimate marketplaces is to “get them off the bigger auction sites,” says Kieron Sharp, director general of the Federation Against Copyright Theft, a trade association in the United Kingdom, thereby “reducing their opportunity and people looking to find that kind of thing.”²⁸² As the two largest online markets serving consumers, much of rights holders’ enforcement efforts are concentrated on eBay and Taobao.

To pressure eBay and Taobao to strengthen their enforcement efforts, rights holders and their trade associations employed tactics similar to those discussed in chapters 4 and 5. They used threats of legal action and also worked with state actors. In the European Union, prominent rights holders, like Nike and Proctor & Gamble, and their trade associations petitioned the European Commission to pressure eBay to sign onto a non-binding enforcement agreement under a threat of legislation. For Taobao, U.S. rights holders and trade bodies worked with the Office of the United States Trade Representative (USTR) to blacklist Taobao on the Notorious Market List to compel it to strengthen its enforcement policies. Before discussing these events, the next section outlines the legal frameworks within which the marketplaces operate.

i) ***Legislative frameworks***

Prior to the introduction of the private enforcement agreements in 2011, eBay and Taobao both had enforcement procedures in place to deal with complaints

²⁸¹ Interview with Tim Waring, Director, Intelligence Technologies, 3 October 2012, by Skype.

²⁸² Interview with Kieron Sharp, Director General, Federation Against Copyright Theft, 9 October 2012, by Skype.

of counterfeit goods. These notice-and-takedown programs remove specific infringing content (i.e., takedown) upon receiving rights holders' complaints of specific incidents of infringement (i.e., notice). As outlined in chapter 3, marketplaces operating in the United States, like eBay, base their notice-and-takedown programs on the provisions outlined in the U.S. 1998 *Digital Millennium Copyright Act* (DMCA), even though the DMCA does not cover trademark infringement. (Marketplaces are required under the DMCA, as hosting providers, to institute notice-and-takedown programs to deal with copyright infringing content (DMCA).)²⁸³ In the absence of a statutory regime to deal with online trademark infringement, marketplaces have adopted DMCA-like measures to address complaints of sales listings offering counterfeit goods (Goldman 2009). eBay, for example, has operated a notice-and-takedown program, called the Verified Rights Owner (VeRO) program, since 1998, which removes listings pertaining to counterfeit goods (Doughery 2011).

Marketplaces operating in the European Union, meanwhile, like eBay's European operations are subject to the 2000 European Commission *Electronic Commerce Directive*, which is adopted into member states' laws. This directive covers copyright and trademark infringement and considers marketplaces to be hosting intermediaries. Marketplaces are required, once they gain "knowledge or awareness" about infringement to act "expeditiously to remove or to disable access to the information."²⁸⁴ Removal of infringing information in the *E-Commerce Directive* occurs through a notice-and-takedown regime, highly similar to that prescribed by the DMCA.²⁸⁵ For its part, China also has a notice-and-takedown regime that resembles those in Europe and the United States (see Mostert and Schwimmer 2011). In 2010, China revised Article 36 of the Tort Law of People's Republic of China, which sets out measures for Internet intermediaries to remove infringing content, including sales listings (see Mostert and Schwimmer 2011).

To summarize, both the European Union and China had laws in place to address the online sale of counterfeit goods prior to the introduction of the

²⁸³ DMCA Sec. 202(512)(b).

²⁸⁴ E-Commerce Directive Art. 14 (b).

²⁸⁵ E-Commerce Directive Art. 12-15.

private enforcement agreements with eBay and Taobao in 2011. In the United States, marketplaces generally adapted the DMCA to deal with complaints of counterfeit goods. Despite these measures, however, rights holders kept pressuring marketplaces to remove infringing listings more quickly and to monitor their platforms proactively to remove sales listings for counterfeit goods before rights holders made complaints. Prior to the private agreements, eBay was reluctant to undertake proactive monitoring and argued that it was not required to do so under the *E-Commerce Directive* (Dougherty 2011).²⁸⁶ Before the USTR placed Taobao on its Notorious Market List between 2008 and 2012, the marketplace had no real incentive to crack down on the trade in counterfeit goods. Overall, marketplaces' enforcement practices prior to the private agreements could be characterized as relatively reactive (particularly Taobao) and fragmented with distinct regulatory differences between countries.

As will be explored in the following section, eBay and Taobao adopted the private agreements as they faced, to varying degrees, an uncertain legal environment because of threats of legislation and litigation, and direct pressure from state actors.

ii) ***Pressure from Rights Holders***

For rights holders, litigation and threats of legal action are useful tools to shape intermediaries' regulatory efforts. Intellectual property attorneys argued, for example, that legal threats convinced eBay to implement its Verified Rights Owner program (VeRO) in 1998. Describing the pressure on eBay, the attorneys said, "It took many years to get there, by threatening to sue them under the doctrines of contributory and vicarious infringement" (Kolson, McDonald, and Pogoda 2004).

Even after eBay introduced its VeRO program, the marketplace has faced pressure from rights holders for years that it is not doing enough to address or prevent third-party infringement on its platform. In an early private enforcement agreement in 2004, eBay and Tiffany Inc., the U.S. luxury jewellery store, worked together to detect and remove listings for counterfeit Tiffany products

²⁸⁶ E-Commerce Directive, Art. 47.

(Rimmer 2011). By 2005, however, the agreement crumbled as Tiffany launched one of the first lawsuits against eBay alleging that the marketplace facilitated the sale of counterfeit versions of Tiffany products.²⁸⁷ Tiffany characterized eBay as “a pirate bazaar, a ‘flea-market’, and a seller of fakes and counterfeits” (Rimmer 2011:134) and alleged that the marketplace facilitated the trade in counterfeit Tiffany products by turning a blind eye to bad actors.²⁸⁸ The court found in eBay’s favour that it had sufficient enforcement policies and practices in place to deal with rights holders’ complaints of infringement.²⁸⁹

eBay argued that the case “broadly endorsed eBay’s anti-counterfeiting efforts” (Dougherty 2011:1). Rights holders disagreed and pursued the marketplace over similar claims in courts in Europe and won judgments against eBay that required the marketplace to undertake proactive monitoring for counterfeit goods.²⁹⁰ These cases highlight tensions between marketplaces and rights holders and underscore the debate over the nature and limitations of marketplaces’ responsibilities for policing their platforms for third-party infringement undertaken by their sellers. Moreover, divergent court rulings between the United States and Europe also further cloud the nature and scope of marketplaces’ responsibilities in relation to third-party infringement on their platforms (McNamee 2011; Rimmer 2011). Commentators on the differing court rulings against Internet intermediaries’ responsibilities for third-party infringement argue that there is “little clarity on what constitutes a proper takedown notice and what intermediaries are entitled to limited liability” (Goldman 2009; see also McNamee 2011).

eBay is thus operating in an uncertain regulatory climate that affects its operations. Furthermore, the lack of legal clarity regarding its enforcement responsibilities and exposure to liability complicates the operation of its platforms worldwide. eBay acknowledges the challenges working in this

²⁸⁷ In the case, *Tiffany, Inc. v. eBay, Inc.* (2008), Tiffany alleged that eBay was “liable for direct and contributory trademark infringement, unfair competition, false advertising, and direct and contributory trademark dilution” (Rimmer 2011:134).

²⁸⁸ For a detailed analysis of the *Tiffany, Inc. v. eBay* case, see Rimmer (2011).

²⁸⁹ The ruling in 2008 and appeal in 2010 found that eBay was not liable for facilitating trademark infringement and the judge concluded that the “burden of policing the Tiffany mark appropriately rests with Tiffany, see: *Tiffany (NJ) Inc., v eBay, Inc.*, (SD NY, 2008), page 57.

²⁹⁰ For example, courts in France ruled against eBay and found it liable for facilitating the sale of counterfeit goods in cases brought by Hermès and Louis Vuitton (Guthrie 2012:3).

environment in its 2013 annual report in which eBay states that it “believe[s] that the legal climate, especially in Europe, is becoming more adverse to our positions” (eBay 2013:22). eBay further claims that this legal climate could require the marketplace to “take actions which could lower our revenues, increase our costs, or make our websites less convenient to our customers” (eBay 2013:22). eBay continues to operate with these legal uncertainties but the European Commission’s agreement offered a respite from litigation in Europe as all signatories agree to abstain from litigation while participating in the agreement (European Commission 2013). As will be explored in the following section, the European Commission proffered a carrot-and-stick approach: it promised a break from the pressure of litigation but warned of legislation if industry could not come up with a voluntary agreement (European Commission 2013).

In contrast to eBay, Taobao has faced considerably less legal pressure from rights holders. Courts in China have been unwilling to hold online marketplaces liable for trademark infringement (Woo 2010:51). U.S. and European rights holders appear generally reluctant to pursue litigation in China. A Hong Kong-based lawyer interviewed said that undertaking intellectual property cases through the legal system in China is difficult because the judiciary is inadequately trained and the lack of separation between government and the judiciary results in politically motivated decision-making.²⁹¹

Litigation offers rights holders a useful avenue to pressure intermediaries to strengthen their enforcement practices. As discussed above, eBay instituted its VeRO enforcement program after years of pressure from rights holders. “They had to be pulled kicking and screaming into doing it,” recalls Siân Croxon, a London-based lawyer with the law firm DLA Piper.²⁹² Rights holders’ capacity to use the threat of litigation varies widely. There “aren’t many rights holders with the interest and the resources and, I suppose, the commercial interest to bring significant cases to court,” observes Jeremy Newman, a partner with Rouse Legal in London.²⁹³ There are also significant drawbacks to litigation. “It’s slow.

²⁹¹ Interview with Hong Kong-based lawyer in Washington.

²⁹² Interview with Siân Croxon, partner DLA Piper, 14 September 2012, London.

²⁹³ Interview with Jeremy Newman, Partner, Rouse Legal, 10 September 2012, London.

It's expensive," notes Newman.²⁹⁴ "It returns a variety of answers by jurisdiction, which is hopeless for the likes of eBay having numerous laws," he says.²⁹⁵ This latter point is particularly problematic not only for Internet firms with global operations but also for multinational rights holders that want equal protection for their goods in all the markets in which they operate.

One of rights holders' main goals for the European agreement was to get eBay to increase its infringing or suspicious sales listing before being altered to do so by rights holders. Ruth Orchard, director of the U.K.-based Anti-Counterfeiting Group, a trade association, explains that intellectual property actors wanted eBay "to take a bit of proactive enforcement on their side."²⁹⁶ Failing in their attempts to get eBay to strengthen its proactive efforts across all its marketplaces through litigation, rights holders' other option was to pressure eBay to undertake proactive enforcement voluntarily. Intellectual property actors admit that outside court proceedings, eBay has "always been very reluctant to negotiate" explains Robert Cumming, a solicitor with the firm Walker Morris in England.²⁹⁷ As a result, rights holders and their trade associations had to petition the European Commission to intervene and compel eBay to enter negotiations with rights holders on a non-binding private enforcement agreement.

For eBay, its operation in an uncertain legal requirement contributed, in part, to its adoption of the European agreement. The marketplace acknowledges that the legal climate is "adverse" to its business (eBay 2013:22). The threat of legislation is a strong motivation to cooperate, as is a respite from litigation from rights holders in Europe. In the case of Taobao, litigation was not an effective option. Instead, rights holders employed a powerful state-backed tool of economic coercion—the Special 301 process operated by the Office of the U.S. Trade Representative (USTR).

²⁹⁴ Interview with Jeremy Newman, Partner, Rouse Legal, 10 September 2012, London.

²⁹⁵ *Ibid.*

²⁹⁶ Interview with Ruth Orchard, Director, Anti-Counterfeiting Group, England, 17 September 2012, by Skype.

²⁹⁷ Interview with Robert Cumming, Solicitor, Walker Morris, England, 21 September 2012, by Skype.

iii) *Pressure Through the State*

Similar to the cases of the other macro-intermediaries, state actors played a direct role in exerting pressure to convince eBay and Taobao to adopt non-binding enforcement agreements. The European Commission warned marketplaces operating in the European Economic Area, including eBay and Amazon, that “if voluntary arrangements cannot be agreed” it would “need to consider legislative solutions” (European Commission 2009). The Commission took on a direct and, it acknowledges, “a novel function as facilitator” to coordinate the 2011 private agreement among marketplaces, rights holders and trade associations (European Commission 2013: 5-6). This non-binding agreement is the first of its kind for online marketplaces. One of its principal goals is to push marketplaces, in the words of the European Commission, “to move beyond mere compliance with legislation” (European Commission 2013:5-6).²⁹⁸ A related goal of the European Commission’s agreement was to provide a forum in which industry could work cooperatively instead of being stuck in an endless cycle of legal battles. All signatories to the memorandum agreed “not to initiate any new litigation against each other” during the period of the agreement (European Commission 2013:4).

For U.S. and European rights holders frustrated with the sale of counterfeit goods through Taobao a useful option for rights holders and trade associations is to work through the USTR. As chapter 3 explained, the USTR is one of the most powerful venues for intellectual property actors to strong-arm countries and non-U.S.-based firms to adopt appropriately tough (i.e., U.S.-style) intellectual property laws and enforcement practices. In 2006, the USTR started publishing the Notorious Market List, which identifies problematic physical and virtual marketplaces. In 2010, the USTR began publishing this list separately in a report called “Out of Cycle Review of Notorious Markets” to emphasize the problem of online infringement. Rights holders submit industry data and analysis alleging that specific companies, like Taobao, are failing to protect intellectual property in a manner rights holders consider sufficient.

²⁹⁸ The European Commission’s position on voluntary industry commitment to ‘compliance-plus’ enforcement and self-regulatory measures is drawn from its consumer agenda, which encourages industry to draft voluntary codes of conduct (European Commission 2012a).

When the USTR names companies or websites as “notorious markets,” it pressures them to make specific changes to their enforcement policies and practices as identified by rights holders. The Notorious Markets List is more than a name-and-shame process: it is part of the Special 301 process that is backed by the U.S. government. As described in chapter 3, the U.S. government provides the bureaucratic reinforcement for rights holders’ complaints of inadequate enforcement as the USTR threatens and sanctions countries where rights holders have identified problems, using the leverage of access to U.S. market (Drahos and Braithwaite 2002).

The USTR listed Taobao as a notorious market in 2008 and released it from the list in 2012 after the Alibaba Group made significant changes to the marketplaces’ enforcement practices.²⁹⁹ Prior to Taobao’s removal from the list, in September 2012, John Spelich, vice president of international corporate affairs at the Alibaba Group, wrote to senior USTR officials and outlined changes to Taobao’s policies.³⁰⁰ Spelich argued that the Alibaba Group instituted “broad-based measures and severe penalties to prevent the sale of infringing goods” and to “cleanse” the platform of problems (Spelich 2012:1). He said that Taobao had conducted “extensive consultations with U.S. stakeholders” to identify ways to strengthen the platforms’ enforcement processes and “eliminate bottlenecks” in processing and removing listings (Spelich 2012:3). In response to rights holders’ directives, Taobao made several significant changes to its policies:

- “Significantly upgraded” notice-and-take-down program, including adding measures for complaints to be made in English;
- “Substantially reduced” the timeframe to remove infringing listings;
- Toughened penalties for repeat offenders (Spelich 2012:3-7).

In addition to these measures, Taobao signed a memorandum of understanding with the International Anti-Counterfeiting Coalition (IACC 2013).³⁰¹ Rights

²⁹⁹ For the USTR Reports, see <http://www.ustr.gov/about-us/press-office/reports-and-publications/2013/2013-special-301-report>.

³⁰⁰ Spelich’s letter and the accompanying 29-page report provide a useful overview of the marketplaces’ enforcement practices (Spelich 2012).

³⁰¹ Taobao also signed similar memoranda of understanding with the Motion Picture Association, which is the international wing of the Motion Picture Association of America, and

holders and trade associations judged these significant changes to Taobao's policies sufficient and in 2012 the USTR removed Taobao from the Notorious Markets List. When the USTR announced Taobao's rehabilitation, it congratulated the platform but urged Taobao "to further streamline procedures" for dealing with infringing sales listings (Erickson 2012). The USTR also called upon the marketplace to continue working toward "a satisfactory outcome with U.S. rights holders and industry associations" (Erickson 2012).

In sum, the U.S. government and European Commission pressured eBay and Taobao into adopting non-binding enforcement agreements in a manner similar to the cases examined in chapters 4 and 5. Pressure from the European Commission and the USTR provided intellectual property actors with the coercive force that they could not achieve themselves through legal action or pressuring eBay and Taobao. These marketplaces constitute the final dimension of the global private regulatory regime that also features revenue chokepoints (payment and advertising actors) and access chokepoints (search and domain name actors). The marketplaces' agreements also illustrate the spatial dimensions of the regime: it is based in the United States and Europe and stretches globally, including to China, which is a major manufacturing location of counterfeit goods. Moreover, the private agreements with eBay and Taobao further demonstrate the degree to which interests are aligned between rights holders and the states involved (the U.S. government and European Union). Before describing the marketplaces' private enforcement agreements, the next section explains how they regulate their platforms to address the online trade in counterfeit goods.

III) Intermediaries' Enforcement Programs

Marketplaces explicitly prohibit the offer, sale or distribution of counterfeit goods on their platforms in their policies and terms-of-use agreements (eBay;³⁰² for

U.S.-based rights holders, including the luxury handbag company Coach, the North Face, an outdoor-wear apparel manufacturer, and Samsonite, makers of luggage (Spelich 2012:3).

³⁰² eBay's policy against counterfeits states: "For a safer buying and selling experience on eBay, we don't allow listings for counterfeit items, fakes, replicas, or unauthorised copies, unauthorised copies include things that are backed-up, bootlegged, duplicated, or pirated—which are all illegal." For eBay's policy on counterfeit goods, see: <http://pages.ebay.co.uk/help/policies/replica-counterfeit.html#policy>.

Taobao see Spelich (2012)). Their notice-and-takedown programs are relatively straightforward. Rights holders (or their authorized third parties, such as attorney or investigative firms) submit notices of infringement, proof of ownership of the trademark/s in question, references to specific listings, and a sworn statement. These statements attest, in the words of eBay, that the complainants have “good faith belief” that certain listings “are not authorized by the IP Owner, its agent, or the law.”³⁰³

In addition to reactive enforcement practices, marketplaces also generally employ some preventive measures to enable them to identify and deal with any violations of their policies, such as listings with illegal, misleading or inappropriate content, fraudulent activity, or manipulating prices. eBay users, for example, must supply identifying information and a credit card to eBay upon registration, as well as accept PayPal, which is owned by eBay. These steps “make it easy to track [offenders] down once their illegal behavior becomes apparent,” says Robert Chesnut, eBay’s Senior Vice-President of Rules, Trust and Safety (Chesnut 2007:24).

The private enforcement agreements adopted by eBay and Taobao expanded upon their existing policies. A principal feature of the private agreements is that eBay and Taobao agreed to undertake proactive monitoring and policing of their platforms, as is explored in the following sections on the European Commission’s agreement and Taobao’s agreement.

i) *eBay’s Enforcement Policies*

eBay’s notice-and-takedown efforts are undertaken through its Verified Rights Owner program, which is the earliest and most well established enforcement program (Dougherty 2011). Approximately 40,000 rights holders participate in VeRO and each may own one to several hundred brands (eBay 2013). Rights holders belonging to the program have “dedicated priority email queues” for

³⁰³ For eBay’s “Notice of Claimed Infringement” form for rights holders to report infringement to the marketplace, see: <http://pics.ebay.com/aw/pics/pdf/us/help/community/NOC11.pdf>.

reporting alleged infringement.³⁰⁴ eBay accepts notifications of infringement from rights holders in relation to counterfeit goods, as well as trademark, copyright, and patent infringement, including “unlawful comparison to trademark owner’s brand name” or “unlawful use of a trademark.”³⁰⁵

eBay, like most marketplaces, allows complainants to submit notifications of infringement electronically. The marketplace generally deletes infringing listings within hours of receiving a notification of infringement.³⁰⁶ Once the listings are removed, eBay notifies the seller and any bidder, cancels the bid or calls for any outstanding transactions not to be completed, advises the seller of the reason for cancellation and provides educational material on intellectual property rights.³⁰⁷ Sellers’ repeatedly found to be in violation of eBay’s policies may be suspended from the marketplace without a refund of their fees.

eBay also grants access to online monitoring or investigative firms working on behalf of rights holders to use software to communicate with eBay’s system in what is known as an application-programming interface (API). Developers may design APIs for any type of program or platform.³⁰⁸ Brand-protection firms using an API with eBay can automate the process of monitoring sales, extract eBay user information, and send takedown notices more quickly and effectively.³⁰⁹ Using the API, “we can automate a cease-and-desist,” explains James Ramm, director of the London-based Commercial Security International, an investigative firm. The “system fills out the necessary details on the VeRo and squirts it through our API back to eBay and it’s an instant removal request.”³¹⁰ By using APIs, brand-protection firms can submit thousands of complaints for the removal of sales listings on behalf of their clients, monitor multiple trading

³⁰⁴ For information about eBay’s Verified Rights Owner program, see: <http://pages.ebay.co.uk/vero/about.html>.

³⁰⁵ For eBay’s “Notice of Claimed Infringement” form, see: <http://pics.ebay.com/aw/pics/pdf/us/help/community/NOC11.pdf>.

³⁰⁶ In *Tiffany, Inc. v. eBay, Inc.* (2008), the U.S. court found that eBay removed 75% of listings within four hours and eBay’s practice was to remove listings within 24 hours of receiving a notice of infringement. *Tiffany (NJ) Inc., v eBay, Inc.*, (SD NY, 2008), page 12.

³⁰⁷ *Ibid.*

³⁰⁸ Google API “Places,” for example, converts any address into geographical coordinates that transferred onto a map. For Google’s Place API, see: <https://developers.google.com/places/documentation/?csw=1>.

³⁰⁹ Interview with James Ramm, Director, Commercial Security International, 10 October 2012, London.

³¹⁰ *Ibid.*

platforms simultaneously and track individuals as they target different marketplaces.

a) European Commission's Memorandum of Understanding

In May 2011, the European Commission quietly published on its website a non-binding agreement called the “Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet.”³¹¹ This agreement, which was the result of two years of negotiations, is one of the most ambitious steps to increase the regulation of intellectual property rights and is the first agreement of its kind for online marketplaces. Signatories include an array of trade associations and rights holders from the pharmaceutical, consumer electronics, sporting goods, software, apparel, and toys industries, including Proctor & Gamble, Nokia, Louis Vuitton, and Nike. The agreement also covers 39 online marketplaces, including multiple country-specific versions of eBay and Amazon (e.g., from France, Belgium and Poland) as well as other marketplaces operating throughout Europe, like Ricardo, Tuktuk and Allegro.³¹² The agreement covers only counterfeit and copyright-infringing goods and excludes any disputes over parallel trade.

As discussed earlier, the European Commission, which coordinated the agreement, motivated industry actors by warning that legislation would be considered if they could not agree upon “voluntary” measures (European Commission 2009). The overarching goal of the agreement is to push marketplaces to go “beyond mere compliance” in two areas: notice-and-takedown programs and what the European Commission refers to as “preventive and proactive” anti-counterfeiting measures (European Commission 2011). In relation to notice-and-takedown programs, the agreement sets out general principles to streamline the programs and speed up the removal of problematic sales listings (see Table 6.1).³¹³ This is where eBay's enforcement

³¹¹ When first released, the agreement was titled only “Memorandum of Understanding” and curiously, it did not contain European Commission's logo anywhere on the document (European Commission 2011).

³¹² For a full list of signatories to the agreements, see European Commission (2013).

³¹³ The agreement is based upon sets of general principles. The Commission acknowledges that participants are reluctant to adopt uniform standards and processes, particularly given the

policies changed. First, eBay streamlined and simplified its enforcement practices to make its notice-and-takedown process more rapid and, secondly, it formalized its proactive monitoring practices to remove problematic listings.³¹⁴

Table 6.1: Key Provisions in European Commission’s Agreement³¹⁵

Measures	Non-binding Principles
Notice-and-takedown programs	Marketplaces agreed to institute streamlined, simplified programs to remove infringing listings more rapidly and effectively
Proactive measures	Marketplaces and rights holders agreed to monitor sales listings to prevent sales of counterfeit goods
Penalties	Marketplaces agreed to increase sanctions against repeat offenders

Both marketplaces and rights holders had complained about poor enforcement practices. Rights holders argued that the platforms’ notice-and-takedown programs were ineffective or too slow at removing infringing listings. In turn, marketplaces argued that rights holders submitted notifications that were incomplete or too general, sometimes targeting “whole catalogues of products” (European Commission 2013:9). Under the agreement, marketplaces agree to institute notice-and-takedown programs that are “not excessively burdensome and simple to subscribe to, complete and process” and deal with complaints “in an efficient and comprehensive manner” (European Commission 2011:4, 5).

Rights holders would look for infringing versions of their products and marketplaces would identify and prevent the sale of counterfeit goods (see European Commission 2011). Signatories could conduct this monitoring through technical (e.g., automated software) measures or analysis by humans. “You have to be very quick to be able to do the take down of an auction that is going on,” say Ruth Orchard, of the Anti-Counterfeiting Group. “You have to be able to do it that same day.”³¹⁶ In addition to strengthening reactive and proactive

differences among their business models and existing enforcement measures (European Commission 2013).

³¹⁴ In its 2008 lawsuit with Tiffany, eBay argued it undertook some proactive monitoring of its platform. With the European Commission agreement, however, eBay adopted proactive monitoring as an integral part of its enforcement efforts.

³¹⁵ Information is from the text of European Commission’s agreement (European Commission 2011).

³¹⁶ Interview with Ruth Orchard, Director, Anti-Counterfeiting Group, England, 17 September 2012, by Skype.

enforcement measures, marketplaces also agreed to sanction repeat infringers including “the suspension (temporary or permanent) or restriction of accounts or sellers” (European Commission 2011:6-7).³¹⁷

ii) *Taobao’s Enforcement Policies*

Taobao’s online complaint system closely resembles that of eBay. There are English-language instructions for submitting complaints to Taobao, but the system is in Chinese.³¹⁸ Rights holders must submit proof of identity,³¹⁹ proof of ownership of the intellectual property in question, details of the intellectual property right,³²⁰ and hyperlinks to the relevant allegedly infringing listings (Spelich 2012). Once Taobao receives notifications of infringement, it notifies sellers of claims of infringement and discloses details of the complaint to sellers. If the sellers fail to contest the complaint, Taobao removes the listing. For complainants with “an established track record of submitting accurate and complete takedown notices,” Taobao undertakes removals more rapidly, usually within hours or a day (Taobao N.d.). The marketplace imposes escalating penalties on individual sellers and operators of storefronts on its marketplace and it may temporarily or permanently ban those who sell counterfeit goods (Spelich 2012).³²¹ Taobao shames repeat infringers through a public blacklist of online merchants it penalizes for selling counterfeit or substandard products on its platform (Erickson 2012a).

³¹⁷ Marketplaces may consider a number of variables when determining how to discipline repeat infringers, including “the severity of the policy violation, the number of alleged infringements, repeat infringement, period of time since prior infringement, seller feedback, language that indicates clear intent, scale of legitimate business as well as other more suspicious behaviour, such as efforts to avoid detection” (European Commission 2013:11).

³¹⁸ For information in English on how to submit a complaint to Taobao, see: <http://qinquan.taobao.com/report/iprOperation.htm>. The online complaint system itself is entirely in Chinese.

³¹⁹ Taobao requires complainants provide contact information and proof of identification (e.g., identity card, passports and businesses license, see Spelich (2012).

³²⁰ Rights holders must provide a registration number, type of intellectual property (i.e., trademark, copyright, invention patent, design patent, utility model patent), country of registration country, and period of validity. For Alibaba’s “User Guide of AliProtect for a Complainant” (for rights holders to submit complaints, see: http://service.alibaba.com/ggs/safe_trade_tips/article/User_Guide_of_AliProtect_for_a_Complainant_200001301.htm?channel=03#).

³²¹ For example, Taobao may remove a storefront from search results in its marketplace for seven days, close the shop for 21 days or permanently (see Spelich 2012).

b) Taobao's Memorandum of Understanding

Taobao is a favourite target for rights holders because of their interest in selling their brands in China's rapidly expanding population of online shoppers. As discussed earlier, between 2008 and 2012, the USTR listed Taobao as a notorious market based upon recommendations from U.S. rights holders and trade associations. Taobao changed its enforcement practices considerably in order to be released from the USTR's Notorious Market List. The Alibaba Group reported that it significantly strengthened Taobao's notice-and-takedown program, increased penalties and reduced the timeframe for removing infringing listings (Spelich 2012). Enforcement was streamlined and more rapid.

As part of Taobao's conditions of release from the USTR blacklist, the marketplace worked with rights holders and signed multiple memoranda of understanding with trade associations and rights holders. One of those agreements, signed in September 2012, is with the International Anti-Counterfeiting Coalition (IACC). The IACC had long pressured Taobao to reform its enforcement practices in the IACC's submissions to the USTR's Special 301 report.³²² The IACC's agreement with the marketplace is important because the IACC is a large, influential trade association that represents multiple multinational rights holders, including Nike, Proctor & Gamble and Adidas.³²³ Taobao approached the IACC in the summer of 2012 with an "interest in partnering" with the trade association to address the sale of counterfeit goods on its platform (IACC 2012). The private agreement is intended to strengthen existing enforcement standards, enhance cooperation between Taobao and rights holders, and improve efficiency. In the words of the IACC, the goal of the agreement is "to leverage available technologies to ensure a streamlined and efficient system for the identification and reporting of illicit sales through the platform, and to identify the worst offenders" (IACC 2012). As a result of its agreement with the IACC—and Taobao's changes to its enforcement practices as part of its conditions to be released from the USTR

³²² The International Anti-Counterfeiting Coalition, for example, regularly submits recommendations to the USTR in relation to its Special 301 report that target countries that its members consider to have insufficient protection for intellectual property rights. For the IACC's submission, see: <http://www.iacc.org/advocacy-and-policy.html>.

³²³ These rights holders are all members of the European Commission's agreement. For a list of the IACC's rights holder members, see: <http://www.iacc.org/member-companies.html>

list—Taobao's enforcement practices are more streamlined, coordinated, rapid and efficient (Spelich 2012).

IACC president, Bob Barchiesi says rights holders want Taobao to assume greater responsibility for online infringement occurring on its platform. "Every legitimate business has a shared interest, and a shared responsibility," Barchiesi says, "in making sure that the online marketplace continues to develop as a trusted commercial platform" (IACC 2012). In a formal announcement of the agreement in August 2013, John Spelich, vice president of international corporate affairs with the Alibaba Group, said, "Our goal at Taobao is to be synonymous in consumers' minds with trust and value" (IACC 2013). In addition to its agreement with the IACC, Taobao also signed memoranda of understanding with the Motion Picture Association, which represents the film industry, and two U.S.-based rights holders – Samsonite, manufacturers of luggage, and Coach, a luxury apparel brand (Spelich 2012).

IV) Analysis of Intermediaries' Enforcement Measures

The two private agreements examined in this chapter reflect a private regulatory regime that is rooted in the United States and the European Union and extends both across the European Economic Area and to China. Similar to the findings in chapters 4 and 5, coercive state pressure underpins the private agreements adopted by eBay and Taobao. In the marketplaces' agreements, as with the regulatory arrangements discussed in chapters 4 and 5, the states involved are not neutral arbitrators among competing interests. The cases of eBay and Taobao illustrate inter-dependent interests between rights holders and the European Commission and with the Office of the U.S. Trade Representative in relation to the protection of intellectual property rights.

Both Taobao and eBay regulate through technology with sophisticated monitoring and enforcement programs to detect and remove suspicious listings, both in response to complaints and proactively. Taobao significantly strengthened its enforcement practices by working with U.S. rights holders and trade associations in order to be released from the USTR's Notorious Market List. The Alibaba Group claims that Taobao's notice-and-takedown program is

more streamlined and rapid because of the pressure from the USTR (Spelich 2012). eBay, in contrast, already had a well established notice-and-takedown program through its Verified Rights Owner Program. Intellectual property actors, however, wanted eBay to join the European Commission's agreement to force eBay to undertake "a bit of proactive enforcement."³²⁴

Rights holders and brand-protection investigators interviewed for this dissertation generally consider eBay's enforcement practices satisfactory but they claim Taobao's efforts need more work, as is discussed in the following section. Criticism of Taobao, however, needs to be understood in the context that changes to its enforcement efforts, which occurred in 2011, are relatively recent. Those who work with marketplaces observe a correlation between their age and responsiveness to the demands of states and rights holders in relation to wrongdoing on their platforms. "The larger and more established the platform, the easier it is to deal with," observes Tim Waring, director of Intelligence Technologies, a U.K. brand-monitoring firm.³²⁵

i) *Results of Private Enforcement Agreements*

In addition to strengthening its notice-and-takedown practices, Taobao, along with eBay, agreed to strengthen proactive enforcement efforts. Both marketplaces have software monitoring their platforms for potential violations of their policies by users and gather data on sales, products, and user activities and behaviour (Erickson 2011). This software extracts information including suspicious key words (e.g., knock-off or lookalike) and the seller's user feedback, and information from the seller's account to identify suspicious activities that may result in the removal of listings or penalties against the seller.³²⁶

Detailed information about marketplaces' enforcement efforts is not released publicly, but there is some indication of the scale of their proactive enforcement

³²⁴ Interview with Ruth Orchard, Director, Anti-Counterfeiting Group, England, 17 September 2012, by Skype.

³²⁵ Interview with Tim Waring, Director, Intelligence Technologies, England, 3 October 2012, by Skype.

³²⁶ In 2002, eBay launched a system called FADE (Fraud Automated Detection Engine) to detect signs of fraudulent activity (Kirsner 2003).

activities. In 2011, for example, Taobao reported removing 53 million listings proactively, compared with 9 million listings based upon rights holders' complaints (Spelich 2012). In the first six months of 2012, Taobao said it removed 45.2 million listings proactively, in contrast to 2.3 million through rights holders' notifications (Spelich 2012). The European Commission also reports that marketplaces' proactive removal of infringing listings exceeds complaints from rights holders. In its report on the agreement's first eighteen months of operation, the Commission cited an unnamed marketplace that said it "voluntarily and proactively removes more potentially problematic listings than are removed reactively" (European Commission 2013:8). The Commission cited another unnamed marketplace that observed a 20% decrease in rights holders' complaints while the marketplace nearly doubled its proactive removal of suspicious listings (European Commission 2013:15).

In terms of due-process measures, the most significant problem with these private agreements is that there is no threshold of evidence for an infringing listing. What "proof is a rights owner giving to third parties like eBay?" asks Robert Guthrie, an associate in London with the law firm SJ Berwin. "At what level does eBay say that price is suspicious enough for us to pull the listing?"³²⁷ Further, in the agreements, both eBay and Taobao consent to streamline their enforcement processes to facilitate the rapid takedown of mass numbers of infringing listings. The challenge with technologically facilitated enforcement is the wrongful removal of legitimate listings. Marketplaces do not have the requisite brand-specific knowledge to distinguish counterfeit goods across hundreds or thousands of brands. "They're not experts," explains Graham Robinson, managing director of the U.K. investigative firm Farncombe International. "There are instances where they agree to take down legitimate auctions at the request of rights holders. These are legitimate auctions and then they get a load of bad publicity."³²⁸

³²⁷ Interview with Robert Guthrie, Associate, SJ Berwin, 5 October 2012, London.

³²⁸ Interview with Graham Robinson, Managing Director, Farncombe International, 28 September 2012, London.

ii) *Perspectives on Private Regulation*

Given the broad range of rights holders, trade associations, and investigative firms that deal with marketplaces in relation to anti-counterfeiting efforts, there are diverse perspectives on marketplaces' enforcement activities. Rights holders participating in the European Commission's agreement report general satisfaction with marketplaces' enforcement efforts (European Commission 2013). They favourably comment that they "experienced more pro-active cooperation" from marketplaces (European Commission 2012). Rights holders say that marketplaces seldom reject rights holders' removal requests (European Commission 2013). Marketplaces and rights holders participating in the agreement say it "increased a sense of trust and confidence between parties" and has been "instrumental in opening avenues to more in-depth dialogues and exchanges of information" (European Commission 2012).

Those interviewed for this dissertation offered mixed views on eBay. eBay is "very good," remarks Susie Winter, director general of the Alliance for Intellectual Property, a U.K. trade association. "They've got their VeRO program and were one of the first to the table with some form of program that they could do."³²⁹ Winter, however, criticizes the marketplace for allowing those kicked off the platform for selling counterfeit goods to register again.³³⁰ Several interviewees stressed that eBay should assume more responsibility. "eBay has certainly tried a bit," argues Sian Croxon, a partner with the law firm DLA Piper in London. "It is just the sheer scale of the criminality that is still going on. It seems to me that you have to still question whether it's enough."³³¹

Gavin Hyde-Blake, director of research and investigation at the investigative firm Eccora, argues that eBay could "be more proactive," but he acknowledges the difficulty of marketplaces being able to distinguish genuine from counterfeit goods. Investigators generally have a positive opinion of eBay's enforcement practices. "I think on the whole we've had a very good experience with eBay," says Alastair Gray, head of the London branch of Cerberus Investigations.

³²⁹ Interview with Susie Winter, Director General, Alliance for Intellectual Property, 12 September 2012, London.

³³⁰ Ibid.

³³¹ Interview with Siân Croxon, Partner, DLA Piper, 14 September 2012, London.

“Once you’ve got relationships with people there, it’s a lot easier to deal with them and explain the issues behind it.”³³²

In contrast, Taobao elicits a more negative reaction. “I consider for us the fight on eBay pretty much won,” comments Andrew Love, global brand protection manager of Specialized, the Utah-based manufacturer of high-end bicycles. “I consider the fight on Taobao ongoing.”³³³ Tim Waring, director of Intelligence Technologies, a brand-monitoring firm in the United Kingdom, characterizes Taobao as “very fastidious in the request for documentation.”³³⁴ Other investigative firms, in contrast, work relatively cooperatively with Taobao. Allan Watson, director of global operations at Gamble Investigations International in London, says that when his company sends complaints to Taobao “they comply.”³³⁵ For other investigators, establishing a relationship with Taobao was more difficult. “There was a learning curve,” recalls Duncan Mee, co-owner of Cerberus Investigations.³³⁶ Alastair Gray of Cerberus Investigations says his company secured cooperation from Taobao by “going to the head of their legal department and saying ‘this is a major problem,’” he recalls. If you don’t sort it out then we’re going to have to look at other ways of policing it.³³⁷ This threat of legal action stimulated Taobao to become “a lot more responsive,” says Gray.³³⁸

V) State Pressure and Actors’ Interests

Like the enforcement programs examined in chapters 4 and 5, the private informal agreements with eBay and Taobao are underpinned by the coercive power of the state. The European Commission and USTR pressured the marketplaces with threats of possible legislation (eBay) and warnings of

³³² Interview with Alastair Gray, Head of London Cerberus Investigations, 4 September 2012, London.

³³³ Interview with Andrew Love, Global Brand Protection Manager, Specialized, United States, 24 August 2012, by Skype.

³³⁴ Interview with Tim Waring, Director, Intelligence Technologies, England, 3 October 2012, by Skype.

³³⁵ Interview with Allan Watson, Director, Global Operations, Gamble Investigations International, 12 September 2012, London.

³³⁶ Interview with Duncan Mee, Co-owner, Cerberus Investigations, 4 September 2012, London.

³³⁷ Interview with Alastair Gray, Head of London Cerberus Investigations, 4 September 2012, London.

³³⁸ Ibid.

potential economic sanctions against China (Taobao). Marketplaces are motivated to comply with the agreements to mitigate the risk of legal action by states or industry, as well as to serve their financial and reputational interests in a safe e-commerce environment. As was the case in the preceding chapters, the potential effects of secretive, private enforcement programs on consumers are largely overlooked.

i) *Role of the State*

The U.S. government and the European Commission played central roles in facilitating greater regulatory cooperation between rights holders and marketplaces. In the case of Taobao, U.S. rights holders and trade associations used the USTR's Notorious Market List to pressure non-U.S. firms or sites, like Taobao, with the weight of the U.S. government behind them. The USTR demands that these firms institute changes outlined by rights holders before it releases them from the list. If the USTR faces recalcitrant actors, it can threaten to or impose sanctions on the country in which they are located, thus imposing pressure on the country to deal with the notorious market. The USTR's Special 301 process is a powerful tool for rights holders because it offers a way to pressure companies (and countries) into strengthening their protection of intellectual property rights that is backed by the economic leverage of the U.S. market (Drahos and Braithwaite 2002).

The European Commission had a direct role in bringing rights holders, trade associations and marketplaces together. It provided a sufficient threat to motivate cooperation among participants—a warning of legislation—and offered an incentive to calm the adversarial environment—a moratorium on litigation (European Commission 2009; European Commission 2013). The Commission also played an active role in coordinating negotiations amongst industry stakeholders in closed-door meetings between 2009 and 2010 and in pushing marketplaces to exceed their legal responsibilities and adopt beyond-compliance enforcement practices (European Commission 2013).

ii) ***State and Corporate Interests in Informal Private Regulation***

Private enforcement agreements enable states to create transnational regulatory agreements and provide marketplaces a degree of regulatory certainty. For the European Commission, creating a private agreement enabled it to institute an agreement relatively quickly instead of working for years with all European Union member states.³³⁹ In addition, by emphasizing non-binding measures, the Commission established a coordinated, standardized enforcement framework across the European Economic Area.

Legal action can be an effective tool for rights holders with the resources and inclination to sue or make credible legal threats; however, rights holders' have varying degrees of capability and interest in doing so. Moreover, as explained earlier, litigation is slow, resource intensive and "returns a variety of answers by jurisdiction."³⁴⁰ Litigation is only an effective tool when courts are likely to hold intermediaries responsible for infringement. In China, courts have been reluctant to do so (Woo 2010),³⁴¹ making litigation an unhelpful tool for rights holders to pressure Taobao to strengthen its enforcement policies.

Marketplaces, particularly eBay with its global operations, operate in an uncertain legal climate. This uncertainty is due, in part, to court rulings in the United States and Europe that have different interpretations of eBay's regulatory responsibilities and the degree of responsibility it bears for third-party infringement on its platform (see Mac Síthigh 2013; Rimmer 2011). The European agreement offers rights holders and eBay relief from litigation, as signatories agree not to engage in litigation while participating in the agreement. In general, however, eBay still faces considerable legal uncertainty. This is because there is a lack of clarity on what constitutes an appropriate takedown notice and what kinds of Internet intermediaries are entitled to limited liability, which makes it difficult to determine compliance (McNamee 2011). In addition, in the United States, eBay enjoys no protection from liability under the *Digital*

³³⁹ The European Commission's agreement took approximately two years to complete in closed-door meetings with industry stakeholders (European Commission 2013).

³⁴⁰ Interview with Jeremy Newman, Partner, Rouse Legal, 10 September 2012, London.

³⁴¹ A lawyer working in China corroborates this point as he has found the legal system unhelpful for protecting his clients' intellectual property rights. Interview with lawyer at Hong Kong law firm, 7 May 2012, Washington.

Millennium Copyright Act for its enforcement measures relating to the removal of sales listings for counterfeit goods, as the legislation only relates to copyright efforts. For eBay, striking partnerships with rights holders may provide a fragile but important respite from litigation, at least from rights holders that are signatories to the European Commission's agreement.

For Taobao the main pressure to reform its enforcement practices came through the USTR's Notorious Market List. The case of Taobao nicely illustrates the inter-dependencies of large multinational corporations and Internet giants. As described earlier, U.S. and European rights holders desire an avenue into China's e-commerce sector and want to ensure that Chinese consumers purchase authentic, branded merchandise, and, in turn, the Alibaba Group wants access to popular foreign brands (Jackson 2012). The Alibaba Group also had a larger strategic goal: it wanted to polish its corporate image to launch a lucrative initial public offering in the United States (Jackson 2012). Other sites that the USTR designates as notorious markets, such as The Pirate Bay, are less susceptible to pressure because they do not have similar interests in operating in the legal marketplace.

iii) ***Consumers' Interests***

Consumers are the missing voices in these private agreements. Similar to the agreements examined in chapters 4 and 5, consumers were shut out of the drafting and implementation of the European agreement. Although marketplaces and rights holders have interests in maintaining consumer trust in their services and products, consumers' interests are assumed to align with corporate interests.

The Commission identifies consumers as one of its main stakeholder groups (European Commission 2013). However, it is extremely problematic that the European agreement was drafted in closed-door, industry-only meetings. It is vitally important to involve consumers in regulation that is, ostensibly, carried out to protect them. However, seeking consumer representation after all the rules and procedures have been drafted significantly constrains the ability of such groups to participate fully and represent their members' interests.

The European agreement came as a “surprise” to those who study the online regulation of intellectual property in Europe, as intellectual property scholar Monica Horten noted in her blog post about the agreement (Horten 2011). No member of any consumer organization or civil-society group, or the general public appears to have been involved or consulted in the drafting of the agreement. In its 18-month review of the memorandum, the European Commission reported it “will continue to seek the involvement, and preferably full participation, of representative consumer organisations and civil rights groups” (2013:17). If any of these groups are currently involved in the agreement, the Commission does not list them as participants. Although little information is publicly available about Taobao’s agreement with the International Anti-Counterfeiting Coalition, it does not appear that consumer groups or Taobao users were consulted. In addition to the lack of consumer representation, consumers can be negatively affected by secretive, unaccountable enforcement strategies that constrain their access to a wide variety of new and second-hand goods or limit their ability to sell goods.

VI) Conclusion

Marketplaces represent a different dimension of the private anti-counterfeiting regime as they regulate legitimate trading platforms through which some individuals sell counterfeit goods, rather than infringing sites that may have few, if any, legitimate activities. Despite this, there are strong similarities to the elements of the regulatory regime described in chapters 4 and 5. State coercion was central to the creation of the marketplaces’ private enforcement agreements and, following the pattern established in previous chapters, the regime has roots in Europe, as well as in the United States. However, as the case of Taobao demonstrates, the regime also extends to China. U.S. rights holders’ use of the USTR’s Special 301 process illustrates the state-market condominium in which states and certain corporate actors’ interests mutually shape one another (Underhill 2003). Taobao’s agreement with the U.S.-based International Anti-Counterfeiting Coalition, which the USTR facilitated, illustrates the degree to which U.S. corporate actors set standards in relation to intellectual property, even in China.

Under their private agreements, in addition to strengthening their reactive notice-and-takedown programs, eBay and Taobao also expanded their proactive enforcement efforts. Both marketplaces operate technologically sophisticated enforcement programs with the capacity to monitor and proactively remove tens of millions of problematic sales listings annually. Through the private agreements, states and rights holders directly shaped marketplaces' enforcement practices by pressuring eBay and Taobao to formalize their proactive enforcement activities and adapt their technological processes to identify counterfeit goods through sales listings. Thus, similar to the situation with Google, the USTR and the European Commission, together with rights holders, shaped how marketplaces employ technology to regulate infringement. Marketplaces' regulatory practices, which prioritize streamlined, proactive mass enforcement, often sacrifice precision for speed. This is a particular problem in relation to intellectual property where it is difficult to determine the legality of products through marketplaces' sales listings (or, indeed, through images on a standalone infringing website). Further, state and industry pressure on marketplaces to shift their enforcement efforts from largely reactive to increasingly proactive activities can negatively affect how marketplaces operate in terms of the types of goods that their users are permitted to buy and sell. Marketplaces that rely upon automated, mass policing "make it more difficult for people who genuinely sell second-hand goods or old stock" (Horten 2011) as listings for these types of goods may be wrongly identified as suspicious and removed.

Chapter 7: Private Regimes and the Public Interest

To reflect upon the emergence and operation of the private regulatory regime discussed in the three previous chapters, it is appropriate to return to the *Stop Online Piracy Act* and the *Protect Intellectual Property Act* and the massive public backlash they generated. The defeat of SOPA and PIPA—an unprecedented loss for U.S. intellectual property advocates—remains a high point for protests against intellectual property and, more broadly, for online grass-roots social movements on the Internet (Sell 2013). The SOPA protests, the largest in the Internet's history, made fully visible the politicisation of the online enforcement of intellectual property in the United States. Given the strongly bipartisan support in favour of strong intellectual property rights in the United States, the defeat of the influential-intellectual property lobby is a considerable achievement (Sell 2013). One of the SOPA opponents' main objections was to the bills' provisions granting corporate actors the right to identify and take action voluntarily against certain types of infringing sites. In articulating their concern, SOPA protesters tapped into wider societal anxiety over state and corporate actors' power to determine what kinds of content we can access, share and use, what we can buy and where, and how we can use Internet services, technologies and platforms. The U.S. Congress, overwhelmed by the massive public uprising, withdrew the bills. Anti-SOPA protesters reasonably believed that the bills' controversial provisions were dead. They were wrong.

Instead, the bills' proponents—including the U.S. administration—went underground. Government officials coordinated negotiations among small groups of industry stakeholders in closed-door meetings. The non-binding enforcement agreements, which incorporate SOPA-like measures, represent a pernicious kind of forum shifting, a shift from public law to private informal regulation that is undertaken in the shadows. Forum shifting is commonly used to refer to rights holders strategically moving among multilateral, plurilateral and bilateral agreements to achieve better outcomes, as well as shifting between different international institutions like the World Trade Organisation (Braithwaite and Drahos 2000; Sell 2011). Participation in these trade agreements may be

limited and proceedings may be secret,³⁴² however, they occur within the public realm and among government officials. Although SOPA and PIPA had highly problematic measures, elected officials drafted and publicly debated their provisions, and stakeholders gave their opinions in testimony before the U.S. Congress.³⁴³ These bills would have been subject to judicial interpretation. SOPA had provisions that would enable the U.S. Congress to review its performance and effectiveness two years after its implementation.³⁴⁴

In contrast, the private enforcement agreements assessed in this dissertation were created in the absence of judicial and legislative safeguards. Pro-enforcement actors strategically shifted from the visible public realm to secret backroom deals to circumvent legislative processes and side step public protests. Unlike other cases of forum shifting where interested parties can generally observe the shift from one forum or institution to another, critics of SOPA have little idea that some of the bill's provisions live on in a series of informal agreements among powerful U.S.-based corporations. Even now, these agreements are relatively unknown. They have attracted little scholarly attention or media coverage outside specialised technology and intellectual property websites.

The private anti-counterfeiting regime involves a distinct constellation of actors—prominent multinational rights holders, macro-intermediaries and powerful state actors—in complex, inter-dependent relationships. Despite the connotations of the term “voluntary” agreements, this dissertation has demonstrated that the state has a paramount role in each of the informal agreements. More importantly, while one would expect the state to represent

³⁴² The Anti-Counterfeiting Trade Agreement and the Trans-Pacific Partnership Agreement, both led by the United States, are plurilateral trade deals with the aim of setting tough new standards for the protection of intellectual property rights. These agreements have been negotiated in secret among participating countries, although there has been extensive consultation with prominent corporate actors, particularly from the United States (Flynn et al. 2012).

³⁴³ Testimony before Congress on PIPA and SOPA was largely limited to pro-enforcement actors, such as the Motion Picture Association of America and Pfizer, as well as Internet intermediaries that supported aspects of the bills, like MasterCard and GoDaddy. Google was the only witness invited that opposed the bills.

³⁴⁴ SOPA Sec. 106 (b)(2) would have required the Register of Copyrights to submit reports to the Judiciary Subcommittee of the House of Representatives and the Senate on the enforcement resulting from the bill and any suggested amendments. While this report would have only covered copyright-related issues, it would have provided an indication of the overall progress of and problems with the legislation.

the public in these agreements, in practice it has largely represented the interests of rights holders. As a result, the public is absent from this regime and generally overlooked in the agreements. Proponents of these agreements argue that they protect consumers' interests by ensuring consumers are protected from being defrauded or harmed by counterfeit goods. From this perspective, intellectual property actors and consumers have common interests in a safe e-commerce environment in which consumers are not deceived or endangered by counterfeit products or those that are legitimate but shoddy. From a broader perspective, however, individuals have larger interests that include a growing concern over digital privacy because of state and corporate surveillance practices. They also have interests in good governance principles of transparency and accountability for state and corporate actors that undertake regulation in the name of protecting the public interest. These public-oriented interests, however, are largely absent from the informal private agreements.

This chapter reflects upon the three preceding chapters to examine the interdependencies and varying interests among corporate and state actors in the regulation of online infringement. First, the chapter summarises the private regulatory regime and reviews the coercive role of states in compelling macro-intermediaries' cooperation and constructing the regime. Then the chapter discusses rights holders' capacity to pressure macro-intermediaries to accept their rules (i.e., private authority) and the limitations of that authority. Third, the chapter examines corporate interests in informal private regulation and then, in the fourth section, turns to examine states' interests in the regime. Then the chapter examines how the regime regulates through technology and the attendant challenges associated with techno-regulation. In the sixth section, the chapter turns to the overlooked actors—consumers and the general public and considers the normative challenges elicited by this type of regulation. In its conclusion, the chapter proposes ways to raise public awareness and strengthen the protection of the public interest.

I) Private Anti-Counterfeiting Regime

The private anti-counterfeiting regime extends globally from its roots in the United States and the European Union. There are distinct U.S. characteristics

as all the macro-intermediaries are headquartered in the United States and it is through their internal terms-of-service contracts that macro-intermediaries have the authority to remove content or withdraw services. The regime's regulatory practices diffuse outward to Canada and, more importantly, to China. For rights holders, China is of particular concern because of its manufacture of counterfeit goods that are exported to North America and Europe. China is also important because U.S. and European rights holders want to expand sales of their brands in China's burgeoning e-shopping environment.

The regime's spatial pattern, which reaches globally from distinct U.S. and European roots, accords with ideas from regulatory capitalism and the non-state governance literature (Graz and Nölke 2008; Levi-Faur 2005). The regime follows a global north-south configuration in which rules and standards are set in the United States and Europe and then exported worldwide to shape standard-setting practices in other countries (Graz and Nölke 2008; Levi-Faur 2005). Despite the scope of the regime, it is a small group of powerful multinational corporate actors and government officials that exert considerable authority in making rules and compelling participation from macro-intermediaries. The regulatory reach of the anti-counterfeiting regime brings to mind the creation of TRIPS described in chapter 3, in which twelve executives from U.S.-based corporations set international standards to protect intellectual property (Sell 2003). In both that case and in relation to this private regime, a handful of U.S. and European corporate actors fundamentally reshaped the global regulatory environment for the protection of intellectual property rights.

The private anti-counterfeiting regime relies fundamentally on the state for its existence. In relation to this regime, state strategically deploys its authority as it legitimises rights holders' demands for a global online regulatory regime and uses coercion to bring macro-intermediaries into the regime. This conception of the state that governs by deploying authority and facilitating non-state regulation echoes ideas from regulatory capitalism discussed in chapter 2 (Braithwaite 2005; Levi-Faur 2005). The state is a non-neutral arbitrator among competing industry interests. The state does not endow all corporate actors with equal degrees of authority as there is a distinct orientation toward ever-increasing enforcement standards for the protection of intellectual property rights. Despite

its key role in creating and endorsing the regime, the state largely acts from the shadows and prefers to emphasise the regime as being driven by voluntary, industry-led initiatives. The narrative of “voluntary initiatives,” however, is inaccurate as the regime is a product of state coercion, as is discussed in the following section.

In terms of its participants, the regime is comprised of rights holders from an array of industry sectors that are loosely coordinated through influential trade associations, particularly the U.S.-based International Anti-Counterfeiting Coalition. Despite the diversity of participants, common enforcement strategies bind the regime. Alongside the traditional strategy of targeting infringing content, this regime also promotes disabling entire websites by using macro-intermediaries to withdraw their essential technical and commercial services. Proponents of this enforcement approach contend it enacts revenue and access chokepoints to throttle unwanted behaviour and deters individuals from seeking content or products that infringe intellectual property rights.³⁴⁵ As a result of their adoption of the private enforcement agreements, macro-intermediaries’ enforcement practices are more streamlined, rapid and proactive than their previous efforts. Taobao, for example, reports that its proactive removals of infringing sales listings outnumber the listings it removes based on complaints from rights holders (Spelich 2012). Enforcement strategies premised upon macro-intermediaries’ technology-facilitated regulation, however, are troubled by the wrongful targeting of legitimate content and activities, as is explored later in this chapter.

i) *State Coercion Underlying Private Regulation*

State coercion underpins the regime. Three government agencies employed varying degrees of coercive pressure to compel participation from macro-intermediaries. In the United States, Victoria Espinel, head of the Office of the Intellectual Property Enforcement Coordinator (IPEC), coordinated multiple informal agreements among payment, search, advertising and domain name macro-intermediaries. The Office of the U.S. Trade Representative (USTR)

³⁴⁵ Interview with David Wood, Director of Anti-Piracy, British Recorded Music Industry (BPI) Ltd., 12 September 2012, London.

pressured Taobao to work with U.S. rights holders. In the United Kingdom, Ed Vaizey, the Under Secretary of State and Jeremy Hunt, former Secretary of State, pushed forward agreements covering search engines and the digital advertising industry through industry roundtables at the Department for Culture, Media and Sport. In Europe, the European Commission facilitated the creation of a memorandum of understanding among rights holders, trade associations and marketplaces. In Canada, the Canadian Anti-Fraud Centre created an agreement with Visa.³⁴⁶

a) Soft Pressure

Each of the private agreements relies upon direct pressure from governments in the United States, United Kingdom and European Union, although the degree of coercion varies. At the softer end of the spectrum, government can “open the lines of communication” among industry actors.³⁴⁷ Official government support can stimulate industry cooperation because the “White House” can be “an important endorsement.”³⁴⁸ The European Commission “took on a novel function as facilitator” (European Commission 2013:5-6) to coordinate discussions among industry stakeholders but also threatened legislation. Victoria Espinel, head of IPEC, strongly encouraged payment providers to ramp up their regulatory efforts against infringement. Julie Bainbridge, senior brand protection manager at PayPal, recalls Espinel saying to PayPal, “We know you’re at the table being proactive but you need to do more.”³⁴⁹ Espinel also “challenged” (IPEC 2011:2) companies from the payment, search, advertising and domain name sectors to come up with best practices to confront unauthorized online pharmacies.

³⁴⁶ As discussed in chapter 4, the CAFC, as a law enforcement agency, has authority to exert pressure on Visa to compel its cooperation in its anti-counterfeiting program and also has moral suasion to persuade Visa, particularly as the payment provider is an official partner of the CAFC. Visa’s experience of being threatened with criminal charges in the United Kingdom may also have motivated the payment provider to cooperate with informal programs in other states.

³⁴⁷ Interview with Senior Policy Advisor, Office of the Intellectual Property Enforcement Coordinator, Executive Office of the President, 18 May 2012, Washington.

³⁴⁸ Ibid.

³⁴⁹ Interview with Julie Bainbridge, Senior Brand Protection Manager, PayPal, 1 July 2012, by telephone.

b) Shaming, Threats of Legislation and Legal Action

In addition to softer tactics of encouragement, the states involved in the regime publicly criticised macro-intermediaries to force them to amend their regulatory practices. Google is a particular target because of its dominance within the search sector and because critics argue it facilitates access to infringing sites. Politicians in the United Kingdom and United States have repeatedly singled out Google for harsh words. The U.K. government's Culture, Media and Sport Committee, for example, denounced Google's enforcement of online infringement as "derisively ineffective" and condemned "the failure of Google, notable among technology companies" (House of Commons 2013:3).

Behind the rhetoric of governments facilitating dialogue amongst stakeholders was the ever-present threat of legislation. Victoria Espinel's discussions of informal regulations with macro-intermediaries took place against the backdrop of the U.S. Congress' debates over COICA, PIPA and SOPA that would have required Internet firms and payment providers to withdraw their services from infringing sites. Debates over these bills began in September 2010, approximately the time that Espinel first brought together all the macro-intermediaries. Espinel carried on negotiations after the U.S Congress withdrew the *Stop Online Piracy Act* in January 2012 after massive protests.³⁵⁰ To take another example, the European Commission underscored its commitment to facilitating voluntary arrangements with a warning that if an agreement were not forthcoming it would "need to consider legislative solutions" (European Commission 2009:11). In the United Kingdom, Jeremy Hunt at the Department of Culture, Media and Sport, made it clear that the government was "willing" to legislate search engines but wanted "industry to find a way forward" (Bradwell 2011).

Alongside the spectre of legislation, government actors may threaten corporations with legal action to motivate their compliance. The City of London Police threatened Visa and MasterCard with criminal charges for laundering

³⁵⁰ In May 2012, for example, just four months after the SOPA protest, three of the largest advertising associations in the United States announced that, after discussions with IPEC, they had agreed to non-binding principles to guide their members' efforts in relation to advertising on infringing sites (ANA 2012).

proceeds of crime from copyright-infringing music sites unless they voluntarily terminated the sites' merchant accounts.³⁵¹ A senior office with the agency described its role as the "leverage" to secure payment providers' cooperation with rights holders.³⁵² The same pattern is evident in the United States. U.S. authorities investigated Google for accepting advertisements from so-called illegal online pharmacies and Google settled the case in August 2011 by forfeiting a record-breaking \$500 million and making changes to its advertising practices (DOJ 2011). U.S. Department of Justice officials acknowledged that the forfeiture was intended to "get Google's attention" (DOJ 2011). While Google was under investigation, it joined negotiations coordinated by Victoria Espinel at IPEC and, in December 2010, co-founded the Centre for Safe Internet Pharmacies along with the domain registrar GoDaddy.³⁵³

c) Market Leverage

The U.S. government also employs the leverage of its market to threaten sanctions against countries that do not implement what the U.S. government (and its rights holders) considers sufficient protection for intellectual property rights. The U.S. government can also threaten or issue sanctions against countries that fail to take action against companies within their borders that facilitate infringement of U.S rights holders. As discussed in chapter 3, U.S. rights holders and trade associations use the Office of U.S. Trade Representative's (USTR) Notorious Market List to blacklist firms that they consider inadequate in their protection of intellectual property. This means that rights holders' complaints have the full weight of the U.S. government behind them. Through the USTR's Special 301 process, the USTR can pressure blacklisted firms to amend their enforcement policies and practices in line with rights holders' demands for reform. If there is no action from these firms, the USTR has the authority to place the countries in which these firms are located on watch lists and apply various coercive measures, from warnings to trade sanctions (Drahos and Braithwaite 2002:90).

³⁵¹ Interview with Det./Supt. Bob Wishart, Head of National Operational Delivery, Regional Fraud Project, City of London Police, 6 September 2012, London.

³⁵² Ibid.

³⁵³ This case was not the first of its kind against Google. In 2007, for example, the U.S. Department of Justice fined Google, Yahoo and Microsoft a total of \$21 million for accepting advertisements for Internet gambling, a violation of state and federal law (PR Newswire 2007).

The case of Taobao aptly illustrates the utility of the Notorious Market List for U.S. rights holders. The USTR blacklisted Taobao in 2008, demanded that the marketplace work with rights holders, and then released it from the list in 2012 after Taobao made considerable amendments to its policies (Spelich 2012). The Alibaba Group that owns Taobao campaigned vigourously to release its marketplace from the list. It hired a Washington-based lobbying firm to present the company's case for removal from the USTR blacklist to the U.S. government and trade associations (Lee 2012). It also approached the International Anti-Counterfeiting Coalition to establish a memorandum of understanding with U.S. rights holders (IACC 2012 and 2013). The Alibaba Group had an additional incentive to work to remove Taobao from the USTR blacklist: it wanted to court the U.S. financial industry and securities regulator to access the U.S. financial system so it could hold an initial public offering in the United States in 2014.³⁵⁴

In summary, each of the macro-intermediaries examined in this dissertation faced direct state pressure through the threat of legislation or legal action. In addition, state actors encouraged, demanded, or publicly rebuked the macro-intermediaries to stimulate their cooperation in relation to online infringement. Intellectual property actors, such as the Motion Picture Association of America, explicitly acknowledge the coercive nature of these informal "voluntary" agreements and observe, "parties are always bargaining in the shadow of the law" (Sheffner 2013:2). A macro-intermediary's choice to participate in informal agreements depends "on what it perceives to be the legal consequence (or lack thereof) of continuing its current course of action, and not committing to any voluntary agreement" (Sheffner 2013:2). Macro-intermediaries have few options to decline involvement in informal regulatory regimes when the states involved credibly employ threats of legislation and legal action. In part, macro-intermediaries' adoption of the private agreements is "defensive" (Lindenbaum and Ewen 2012) to reduce the firms' risk of being targeted by states or rights holders.

Macro-intermediaries candidly acknowledge the role of government pressure in shaping their enforcement practices. Linda Kirkpatrick, a senior executive with

³⁵⁴ The Alibaba Group filed its initial public offering on 7 May 2012 (Owles 2014)

MasterCard, recalls that prior to the IPEC-facilitated private agreement, payment providers had “different fragmented approach[es] to attacking the problem” and “no formal process for addressing inquiries” (Kirkpatrick 2012). Advertising actors in the United Kingdom credit “political imperatives from government” for the rapid implementation of the Digital Trading Standards Group.³⁵⁵ As discussed, Taobao significantly altered its enforcement practices according to rights holders’ demands in order to be released from the USTR Notorious Market List. As well, the International Anti-Counterfeiting Coalition thanked Espinel for facilitating what IACC president Bob Barchiesi described as “unprecedented cooperation from the payment processors,” which enabled the creation of the IACC’s merchant-account termination program (IACC 2011).

II) Nature and Limitations of Private Authority

The nature and limitation of corporate actors’ capacity to persuade others to accept their rules goes to the heart of this research. In this context, as chapter 2 noted, private authority refers to the degree to which corporate actors can impose their privately drafted rules and standards on and influence the behaviour of other corporate actors (Green 2013). Private authority is a relational concept. Actors must be able to convince or compel other private parties to accept and abide by their authority. Rights holders’ arsenal of tactics includes high-powered pressure, shaming, granting or withholding business deals, making credible threats of legal action and, where resources and opportunity permit, litigation. These tactics, when employed by wealthy, multinational rights holders or trade associations, can be relatively effective in compelling other private parties to adapt or adopt regulatory measures.

i) *Rights Holders Making Rules*

Some actors are easier to convince than others, or may have a lesser capacity to resist. Further, some corporate actors have greater resources and capacity to lobby the state than others, and their interests may be aligned more closely with the state. These interactions reflect a distribution of authority among corporate

³⁵⁵ Interview with Amit Kotecha, Senior Mobile & Networks Manager, Internet Advertising Bureau, 8 October 2012, London.

actors but preferences can shift or evolve over time. Context is also important, as there may be situations in which actors' interests temporarily align or diverge. Advertising actors, for example, are entirely dependent upon rights holders because they "fund the whole industry and everyone has to meet [their] demands."³⁵⁶ As well, what resonates with one community may be unpalatable in another, as was evident in the deep divide over SOPA. Some sort of recognition or acknowledgement of the actors' authority by the constituency they propose to govern is necessary to grant legitimacy to the regulatory activities (Biersteker and Hall 2002; Avant, Finnemore, and Sell 2010).

Prominent U.S. and European rights holders and trade associations have considerable private authority as is evident in their success over several decades in shaping the creation of rules and standards domestically and internationally (Draho and Braithwaite 2002; Sell 2003). They draw upon rich stores of structural and discursive authority. In terms of their material resources, rights holders emphasise the importance of protecting their popular, multi-billion-dollar brands and the significant economic revenue they generate. Coupled with this is a compelling narrative of the harmfulness of counterfeit goods to public safety and economic integrity. They have also successfully employed high-powered campaigns to persuade and force intermediaries to strengthen their enforcement practices. For example, in response to "years" of threats of legal action by rights holders, eBay created its Verified Rights Owner program in 1998 (Kolson, McDonald, and Pogoda 2004).

ii) ***Constraints on Rights Holders' Authority***

Private authority, while expansive for certain corporate actors, has clear limitations. Corporate actors have a finite array of sticks and carrots with which to convince others. Some actors, particularly large multinational firms, have a greater capacity to employ threats, as litigation requires time and resources. They can also offer more attractive inducements, such as greater access to desirable markets or licenses to sell popular products. They may use strategies that combine incentives and threats, or consistently employ strategies over time to attempt to wear down reluctant parties. Corporate actors' authority is limited

³⁵⁶ Ibid.

when they encounter others with a corresponding capacity to counter their efforts and interests in withstanding certain regulatory arrangements or specific rules. This resistance may be temporary or may persist over time. Corporate actors' authority may also be limited if their demands exceed their ability to apply a corresponding level of threat to persuade others to comply. There is a significant difference, for example, in Visa agreeing to process a handful of account-terminations voluntarily and its adoption of a private agreement to terminate thousands of accounts voluntarily on behalf of rights holders.

In relation to the informal private enforcement agreements, intellectual property actors were largely unable to convince macro-intermediaries to make wholesale changes to their regulatory efforts. Prior to the payment providers' enforcement agreement, for example, a representative from MasterCard acknowledges that the industry's approach to online infringement was "fragmented" and lacking a "formal process for addressing inquiries" (Kirkpatrick 2012).

iii) ***Calling Upon the State***

If actors are loath to expend greater resources in solo campaigns to persuade actors or find that their authority is limited in this regard, they can seek assistance from the state. This assistance may relate to creating, implementing or enforcing particular rules and standards. The degree of direct state involvement varies according to whether the topic of regulation is a matter of concern to the state or aligns with its interests. By constructing intellectual property laws that set out certain responsibilities and liabilities, the state arbitrates among (mostly corporate) interests.³⁵⁷ If called upon, the state may facilitate regulation. The state may endorse a particular strategy or set of rules. It can also act more coercively, by issuing warnings or threats to mandate specific action in ways that favour one group over another.

For rights holders, government involvement was necessary to persuade the likes of Google, Yahoo, Visa, PayPal and GoDaddy to come together and

³⁵⁷ The state's arbitration among competing industry interests is apparent in its drafting of laws that set out responsibilities for Internet intermediaries and conditions under which those intermediaries have limited immunity from liability (Haggart 2014).

negotiate industry-specific informal agreements. The government agencies involved in the regime played key roles in coordinating discussion among industry stakeholders. In doing so, they legitimated the concept of non-binding private agreements and, more broadly, intellectual property actors' enforcement strategy against online infringement. They also legitimated rights holders' authority to set and enforce rules and standards to protect intellectual property on the Internet. Rights holders' private authority can therefore be understood as partly derived from the state, which accords with findings from non-state governance scholars (Büthe 2010; Hall and Biersteker 2002; Sassen 2002).

State and corporate interests shape one another, and both rights holders and macro-intermediaries influence the state's policy preferences and contribute to its goals. Rights holders, macro-intermediaries and government actors in the United States, United Kingdom and European Union have complex mutual interests, which I will explore in the following sections. In relation to the protection of intellectual property, corporate and state regulatory goals are relatively complementary and "mutually inform" one another (Peters, Förster, and Koechlin 2009:504).

III) Corporate Interests in Private Informal Regulation

Macro-intermediaries have varying incentives and disincentives to enter into informal private enforcement agreements. They face pressures to protect their corporate brands and platforms from infringement, and to achieve a measure of legal certainty in relation to their regulatory responsibilities. They also encounter significant enforcement costs, risk alienating their users through unduly aggressive enforcement efforts, and, most importantly, receive no protection from liability, which leaves them vulnerable to litigation from rights holders.

i) *Reputational and Legal Concerns*

Macro-intermediaries have diverse, often conflicting interests about acting as gatekeepers for rights holders. Like rights holders, they are concerned with maintaining and promoting their valuable brands and fear a loss of reputation—

and a risk of liability—if their brands are associated with websites selling counterfeit goods. They also have economic interests in adopting measures that elicit greater consumer trust and confidence in their respective industries. eBay, for example, admits that if its business were associated with counterfeit goods, even inaccurately, it would “damage our reputation, lower the price our sellers receive for their items and damage our business” (eBay 2013:9). Similarly, those in the digital advertising community must protect rights holders’ brands as they “fund the whole industry.”³⁵⁸ As the digital advertising industry is relatively new, it must be particularly vigilant in maintaining rights holders’ trust because “one bad story could ruin a brand for a very long time.”³⁵⁹

Internet firms and payment providers may also decide to adopt informal regulatory strategies in order to minimise the risk of assuming greater liability for infringement. Intellectual property actors recognise their role in pushing eBay into strengthening its policies and creating its signature enforcement program, the Verified Rights Owner program. For example, panellists at a 2004 discussion on infringement described efforts to strengthen eBay’s enforcement measures: “It took many years to get there, by threatening to sue them under the doctrines of contributory and vicarious infringement” (Kolson, McDonald, and Pogoda 2004). Macro-intermediaries may also face legal action, fines or other penalties if they breach due diligence requirements. Domain registries, such as Verisign, can terminate their contracts with registrars, potentially stripping them of lucrative domain name contracts (ICANN 2012). Advertising actors may be fined for violations, forced to refund rights holders for ads that end up on infringing sites, have payment withheld, or lose their industry certification. These penalties provide a powerful motivation for firms to strengthen their enforcement policies.

ii) ***Flexibility and Beneficial Terms***

Informal regulatory agreements can also offer corporate actors an opportunity to adopt rules that benefit their businesses. Transnational private agreements can

³⁵⁸ Interview with Amit Kotecha, Senior Mobile & Networks Manager, Internet Advertising Bureau, 8 October 2012, London.

³⁵⁹ Ibid.

minimise regulatory differences among countries, which can make regulation simpler. Big, global Internet firms, such as Google and Yahoo “want a global initiative,” argues Amit Kotecha, manager with the Internet Advertising Bureau in London. “They don’t want to have different laws in different countries.”³⁶⁰ Standardised, global notice-and-takedown policies to remove infringing content or withdraw certain services may usefully streamline firms’ enforcement efforts across multiple countries. Agreements based upon non-binding best practices may also offer corporate actors greater flexibility and less onerous conditions than legislation or court-imposed requirements. SOPA, for example, would have imposed strict five-day timeframes on payment providers’ to respond to rights holders’ complaints.³⁶¹ Such “artificial deadline[s]” argues Linda Kirkpatrick, senior executive at MasterCard, “may present impossible compliance challenges in some circumstances” (Kirkpatrick 2011:11).

iii) ***Disadvantages for Macro-Intermediaries***

Even with the above-noted advantages of informal private regulation, there are risks for macro-intermediaries that sign onto private enforcement agreements. For macro-intermediaries, one of the major downsides of the flexibility and informality of informal agreements is a lack of protection from liability. Integral to the *Digital Millennium Copyright Act* and the European Commission’s *E-Commerce Directive* are provisions that shield certain intermediaries from liability for infringement on their platforms if they respond to rights holders’ notice-and-takedown requests and remove the specified content.

a) **No Immunity from Liability**

Proponents for tougher enforcement measures recognise that “a constructive dialogue” among industry actors can help mitigate the risk of legislation and deliver “mutually satisfactory arrangements,” says Jeremy Newman, a partner with Rouse Legal in London.³⁶² “If you’re in a litigious environment, then poor

³⁶⁰ Ibid.

³⁶¹ SOPA Sec. 102, (c)(2)(A)(i).

³⁶² Interview with Jeremy Newman, Partner, Rouse Legal, 10 September 2012, London.

old Google would be mad to be saying anything except, ‘It’s not our fault.’”³⁶³ The European Commission recognised the adversarial legal environment between rights holders and macro-intermediaries and placed an embargo on signatories from engaging in litigation against one another because “cooperation is better than litigation” (European Commission 2013:4-5). While the European Commission agreement provides some respite from litigation, other macro-intermediaries are not so fortunate. In the other private agreements discussed in this dissertation, rights holders may sue macro-intermediaries that they claim are recalcitrant or negligent. Users may also seek legal action against macro-intermediaries that wrongfully removed their content or services.

b) Costs of Enforcement

Macro-intermediaries may incur significant enforcement costs depending on the degree to which they amend or augment their regulatory efforts. Enforcement programs are costly to operate when they involve the global monitoring of tens to hundreds of millions of transactions and users annually. Companies are reluctant to disclose the resources they allocate to enforcement. Publicly available information indicates that macro-intermediaries devote significant resources to enforcement. PayPal, for example, reported in 2012 having a team of 90 dedicated to monitoring violations of its intellectual property policies (Bainbridge 2012), while Taobao stated it employs 200 individuals responsible for intellectual property protection, including handling infringement complaints (Spelich 2012). In testimony to the House Judiciary Committee in 2011, Google’s senior vice-president Kent Walker said the search giant invested \$60 million in 2010 to prevent violations of its advertising policies (Walker 2011).

Another cost of enforcement is the risk of alienating customers through the inaccurate removal of content or services or angering those who find enforcement efforts unduly aggressive or unfair. While Internet firms and payment providers have an interest in protecting their brands and services from wrongdoing, ramping up enforcement efforts against infringement may negatively affect aspects of their business models. Marketplaces, for example, argue that their businesses rely upon having a large, varied array of offerings to

³⁶³ Ibid.

meet consumer demand, including second-hand goods, which can be a source of tension with rights holders. eBay argues that some rights holders, particularly luxury brands, are attempting to “exact ever greater control over e-commerce,” which negatively affects what the marketplace can sell (eBay 2008). Similarly, Google has repeatedly expressed discomfort with its role as a regulator for rights holders. “It’s not Google’s job to go around the web to declare whether sites are legal or illegal,” says Theo Bertram, manager of UK public policy for Google, argued in relation to Google’s advertising operations (Bertram 2013).

IV) State Interests In Informal Private Regulation

Non-legally binding private enforcement agreements offer states particular benefits. They enable the states involved in the regulatory regime to continue their efforts to protect intellectual property. More broadly, these states can capitalise upon macro-intermediaries’ regulatory capacity to exert influence online in relation to their law enforcement and national security interests. The secrecy and flexibility of the agreements, which enables participants to side step failed and stalled intellectual property legislation, show that the agreements are primarily oriented toward serving certain corporate and state interests.

i) *Inter-dependence amongst Corporate and State Interests*

Regime theory helps us understand the interactions and inter-dependencies between corporate and state actors that construct and shape regulatory arrangements (Cutler, Hauffler, and Porter 1999). The private anti-counterfeiting regime represents a state-market condominium in which the state and certain influential corporate actors mutually constitute interests, policy preferences and regulatory strategies (Underhill 2003; see also Braithwaite and Drahos 2000). These corporate interests, however, are integrated asymmetrically into the state in relation to corporate actors’ structural and discursive capacity (Underhill 2000:129 in Sell 2003:19). To those outside the regime, boundaries may appear blurred between state and certain corporate interests (Sheptycki 2000:12-13). In the case of this private regulatory regime, however, there are distinct arrangements of aligned and overlapping interests among rights holders, macro-intermediaries and the states involved. The regime’s state actors

arbitrate among competing corporate interests, leaving the public largely unrepresented. Power dynamics favour large, multinational rights holders, like Nike, Pfizer and Louis Vuitton with decades of lobbying successes over relatively recent upstarts like Google.

a) **Ever-Increasing Protection of Intellectual Property**

There are mutually interdependent interests between the state and rights holders and, in turn, between the state and macro-intermediaries, as well as some overlapping economic and reputational interests between rights holders and macro-intermediaries. As discussed in chapters 1 and 3, rights holders and states share economic interests in intellectual property, particularly states that have the greatest proportion of intellectual property owners. Since the 1970s, the United States, along with countries in the European Union, particularly the United Kingdom, have conceptually linked intellectual property with international trade and economic success (Braithwaite and Drahos 2000; Halbert 1997). This narrative is deeply engrained within these states and reveals the lobbying prowess of rights holders.

In the United States, sentiment for the protection of intellectual property rights is widespread and deep-seated, as evidenced by high degrees of bipartisan support for this position (Drahos and Braithwaite 2002). This is particularly evident in relation to debate over the four intellectual property bills the U.S. Congress considered between 2010 and 2012. Disagreements among U.S. legislators over SOPA and its predecessors demonstrate differing views on enforcement tactics considered appropriate to protect intellectual property rather than a fundamental questioning of the need for ever-increasing protection for intellectual property. As noted in chapter 3, Senator Ron Wyden, a Democrat, and Representative Darryl Issa, a Republican, staunchly opposed SOPA and introduced the *Online Protection and Digital Trade Enforcement Act* (OPEN).³⁶⁴

³⁶⁴ The OPEN Act has not progressed since the U.S. Congress' withdrawal of PIPA and SOPA in January 2012

The OPEN bill would have addressed some of SOPA's biggest problems, as it removed the private right of action and filtering of the domain name system. However, it also affirms some of SOPA's key provisions. OPEN would have retained the practice of using Internet intermediaries to withdraw services from infringing sites, although it only includes payment and advertising intermediaries.³⁶⁵ It also preserves the problematic provision that grants voluntary right of action against sites distributing pharmaceuticals in violation of U.S. laws.³⁶⁶ Wyden and Issa intended the OPEN Act as an alternative to SOPA. However, measures in OPEN to withdraw critical services from targeted sites and retain intermediaries' voluntary rights of action indicate that these are now orthodox enforcement tactics among U.S. legislators. Non-binding private enforcement measures are deeply ingrained within the United States as some of the largest Internet firms and payment providers, including PayPal, Visa, MasterCard, Google, GoDaddy and Yahoo have adopted them. Victoria Espinel, as head of IPEC, promoted the benefits of informal private regulation in testimony before the U.S. Congress (Espinel 2012).

b) Entrenched Interests and the Rising “Big Tech” Lobbying Force

In the United States and the United Kingdom, interactions among legislators and rights holders demonstrate the latter's capacity to shape policymaking on intellectual property (Drahos and Braithwaite 2002). Underlying rights holders' success in crafting agreements at the global level are close, inter-dependent ties between industry and government, particularly the U.S. government. Rights holders and their trade associations form an entrenched lobbying force within the U.S. political and economic landscape (Drahos and Braithwaite 2002). The influence of intellectual property actors stems from their efforts in the 1970s and 1980s to get intellectual property onto the agenda of the U.S. government and set standards internationally for the protection of intellectual property (Sell 2003).

The role of major U.S. corporations as trade policy advisors to the United States was institutionalised in the USTR Advisory Committee for Trade Negotiations,

³⁶⁵ OPEN 3(B).

³⁶⁶ OPEN (k).

described in chapter 3 (Sell 2003). U.S. corporations remain involved in shaping international trade agreements, such as the controversial and secretly drafted U.S.-led Trans-Pacific Partnership agreement.³⁶⁷ Further, rights holders and trade associations shape U.S. policymaking on intellectual property through the USTR Special 301 list, as shown by the case of Taobao in chapter 6. Inter-relationships between rights holders and state actors are facilitated by the “well-entrenched politics of money and influence,” in which rights holders generously finance political campaigns and, in return, enjoy preferential access in policymaking (Sell 2013:16).

Despite intellectual property actors’ institutional advantage, Internet firms, which are relatively new to political lobbying, are rapidly developing their lobbying capacity and spending considerable funds to shape policymaking in Washington. Google, in particular, is fast increasing its lobbying activities and acumen. The search giant now ranks among the top five in corporate lobbying expenditures in the United States with \$15.8 million in 2013, which places it behind General Electric at \$16.1 million.³⁶⁸ The search giant’s top concern is intellectual property—issues relating to copyright, trademarks and patents.³⁶⁹ Google’s current status as a lobbying giant is a stark contrast from its one-person lobbying force in 2004 with a rank of 213th place among corporate lobbyists (Hamburger and Gold 2013).

Alongside an increase in lobbying efforts, the U.S. technology industry is expanding its capacity to lobby through trade associations. As of 2012, there were two new, technology industry trade associations in Washington—the Internet Association and the Internet Infrastructure Coalition—to act as lobbying voices for Internet firms.³⁷⁰ These associations undertake advocacy work in an

³⁶⁷ Although details of the TPP, which is still ongoing, are secret to the public and elected representatives outside the negotiating team, corporate representatives from major, multinational companies are involved in the negotiations (see Flynn et al. 2012).

³⁶⁸ The Centre for Responsive Politics’ project OpenSecrets.org tracks corporate lobbying amounts. See: <http://www.opensecrets.org/lobby/top.php?showYear=2013&indexType=s>.

³⁶⁹ According to the Centre for Responsive Politics, Google’s three other top interests are, in order of priority, telecommunications, antitrust and labour, and computers and information technology.

³⁷⁰ The Internet Association describes itself on its website as the first trade association in the United States for the Internet economy, see: <http://internetassociation.org/>. The Internet Infrastructure Coalition says on its site that it supports those who “build the nuts and bolts of the Internet,” see: <http://www.i2coalition.com/about-us/>.

array of policy areas, including data privacy and Internet governance, as well as intermediary liability (Internet Association) and facilitating best practices for addressing online infringement (Internet Infrastructure Coalition). With the growth of Internet firms' lobbying capacity and the creation of these trade associations, it is reasonable to assume that U.S. Internet firms will shape policymaking in relation to intellectual property and to the Internet more generally, although the ways they may do so are issues for future research.

c) Expanding States' Regulatory Capacity Online

In addition to the shared interests among rights holders and governments, there are important inter-dependencies between macro-intermediaries and the states involved in the regulatory regime. Macro-intermediaries enable governments to extend their regulatory reach online to target varying types of problems. Since the mid-2000s, for example, federal and state authorities in the United States have worked with payment macro-intermediaries to withdraw their services voluntarily from sites unlawfully distributing tobacco and illegal gambling sites (MacCarthy 2010). By working with these payment actors through non-binding agreements, the U.S. authorities could target these sites more effectively and rapidly than working through court orders. Similarly, the U.S. and U.K. governments both have non-governmental programs to tackle child pornography sites in which macro-intermediaries—from PayPal, Visa, and Google to GoDaddy—agree to withdraw their services voluntarily from sites identified as distributing child pornography.³⁷¹

Macro-intermediaries assist states in the online regulation of national security-related crimes. The U.K. government, for example, operates a secretive, voluntary website-blocking program targeting “violent extremism” sites (Fae 2014). Under the program, Internet service providers voluntarily block access to sites that the U.K. government identifies as hosting content that violates the country's anti-terror laws (Fae 2014; McIntyre 2010). This program, like those discussed above, enables the U.K. government to adopt a flexible regulatory

³⁷¹ In the United States, this program is part of the National Centre for Missing and Exploited Children and in the United Kingdom it is the Internet Watch Foundation. Internet firms participating in the programs terminate their payment services to targeted sites and block access to the sites (Laidlaw 2012).

approach to deal with the difficult problem of regulating illegal (and sometimes simply objectionable) online content. The anti-extremism program, however, operates in manner that is non-transparent and unaccountable and raises questions of how site content is classified and by whom (Fae 2014; McIntyre 2010).³⁷² Such challenges, which are inherent to private informal regulatory efforts, are explored in more detail later in this chapter.

Macro-intermediaries can also enable states to expand their online surveillance capacity to serve states' national security interests. Bruce Schneier, a well-known Internet security analyst, argues that surveillance is the business model of the Internet (Schneier 2013). Companies like Google, Microsoft, Facebook and Twitter track their users, monitor interactions and record transactions (Mayer-Schönberger and Cukier 2013). Eric Schmidt, Google's outspoken chief executive officer, candidly acknowledges his company's interest in accumulating information on its users:

With your permission you give us more information about you, about your friends, and we can improve the quality of our searches. We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about (Thompson 2010).

Schmidt's comment, while admittedly a relatively extreme example of corporate surveillance, demonstrates the importance that Internet firms place on amassing personal data that they can then mine for commercial purposes. Macro-intermediaries are valuable to state security programs like the U.S. National Security Agency (NSA), because of firms' vast troves personal and commercial information on their users. Revelations from Edward Snowden's leaked files reveal that the NSA heavily depends upon siphoning data from companies Google, Yahoo, Facebook and others (Ball, Border, and Greenwald 2013; Schneier 2014).

Both corporate and state actors have interests in preserving—and expanding—Internet firms' corporate surveillance programs, despite public or political concerns about privacy. These parties also have shared interests, although

³⁷² The U.K. Home Office refuses to release a listing of the industry participants in this program or the list of sites that are blocked. In July 2013, the U.K. government confirmed it was blocking 1,000 sites (Fae 2014; McIntyre 2010).

sometimes differing goals, in shaping policies and standards relating to Internet infrastructure and services. For example, on the issue of data retention and storage, their interests are relatively aligned in favouring broadly conceived standards in relation to the collection, retention and use of personal data. The situation is somewhat different in the case of encryption. As revealed by the Snowden files, the NSA has worked strategically to weaken encryption standards to facilitate the agency's ability to siphon information from all corners of the Internet. Firms that offer Internet services and infrastructure, in contrast, must protect their systems, users and business partners from risks including malware, that may result from using flawed, weakened code.³⁷³

In sum, by working with macro-intermediaries, the U.S. government is embedding its national security apparatus within Internet firms' platforms and services (Ball, Border, and Greenwald 2013; Schneier 2013). The U.S. government is also entrenching itself into the standard-setting architecture of the Internet where it can shape policies, like those relating to intellectual property, security and data storage, that benefit its strategic economic and national security interests.

ii) ***Flexibility and Secrecy: Plausible Deniability***

Informal private regulation offers states particular benefits, such as flexibility to side step controversial, stalled or failed legislation. Avoiding the sometimes-fractious public debates relating to legislation by drafting measures in secret can be a valuable feature for scandal-weary states. The U.S. and U.K. governments, facing unpopular, flawed legislation and delays in implementing legislation intensified their support for non-binding private measures. By working with industry stakeholders informally, IPEC avoided the controversy that still surrounds the *Stop Online Piracy Act*. Government officials are wary of "being SOPA-ed" (Goldman 2012), which is a neologism that refers to massive, unpredictable protests against intellectual property policies. For the U.K.

³⁷³ Following details from the Snowden files that the NSA covertly intruded into the systems of Google and Yahoo, Internet firms encrypted previously unprotected systems or upgraded their encryption systems (Greenwald and MacAskill 2013).

government facing the stalled *Digital Economy Act*,³⁷⁴ private agreements offered an opportunity to bypass legislative problems and pressure industry actors into taking informal enforcement activities.

Secrecy can be useful to coax reluctant industry actors into negotiations that they may otherwise be hesitant to participate in publicly. The U.K. Department for Culture, Media and Sport, for example, invited representatives from civil-advocacy and consumer groups to an industry roundtable meeting following public pressure. A civil-society representative who live-tweeted one of the meetings reported industry participants were concerned about “too much transparency and ‘subjective’ reporting” by civil-advocacy groups (Firth 2011). The civil-society groups were not invited to subsequent roundtables.³⁷⁵

States can also use informal regulation to encourage private-sector stakeholders to establish an industry consensus, at least among the big players, on which legislation could be based. Once industry groups establish informal agreements, particularly those with industry-wide consensus, they can be difficult to alter. In the United Kingdom, for example, former Secretary of State Jeremy Hunt told search engines that the government would prefer that industry set rules, but would consider legislation if necessary.³⁷⁶ The European Commission expressed a similar sentiment in relation to the regulation of counterfeit goods in marketplaces (European Commission 2009).

Governments can employ or rely upon private regulation to bypass traditional legal jurisdictional boundaries. Victoria Espinel, head of IPEC, argued that voluntary, industry-led regulation enables governments to have an “impact on websites that are beyond the reach of U.S. law enforcement agencies” (Bason 2012). Governments can also capitalise upon private enforcement efforts to export their preferred regulatory mechanisms globally. The U.S. Food and Drug

³⁷⁴ The *Digital Economy Act* targets copyright-infringing sites by requiring Internet service providers (ISPs) to pass on warnings to those making unauthorised downloads and then cut off their access to the Internet. Implementation has been delayed until 2015 because of disagreements between rights holders and ISPs over who should bear the costs of the system (BBC 2013).

³⁷⁵ The civil-advocacy groups Open Rights Group was invited to the meeting on 7 December 2011 and then disinvited thereafter.

³⁷⁶ Minutes from the Search Roundtable Discussion with Rights Holders and Search Engines in November 2011 (see Bradwell 2012).

Administration (FDA), for example, asks domain registrars to withdraw their services voluntarily from thousands of sites that the FDA identifies as illegal online pharmacies, as the FDA lacks jurisdiction over sites not based in the United States (GAO 2013). This strategy enables the FDA to extend its reach to govern actors outside its legal jurisdiction and globally impose U.S. policies on pharmaceutical distribution and pricing, which favours large U.S. pharmaceutical interests (Drahos and Braithwaite 2002).

V) Regulation through Technology

Techno-regulation, the deliberate shaping of human behaviour through technology, explains rights holders' shift toward macro-intermediary-facilitated enforcement and the use of technological chokepoints to control online infringement. One of the principles of techno-regulation is the mutual shaping of technology and politics (Brey 2005; Leenes 2011). Regulators—states, rights holders, and macro-intermediaries—shape technology to govern behaviour and, in doing so, imbue the technology with certain values, concepts and norms (Brey 2005).

Macro-intermediaries, for example, are not “natural” gatekeepers: proponents of stronger enforcement conceptualised the firms as well-placed, effective, and skilled regulators of online infringement (e.g., Castro, Bennett, and Andes 2009). Further, intensive pressure from states in the form of threats of legislation and legal action, along with years of campaigning from rights holders, transformed macro-intermediaries into gatekeepers responsible for policing their platforms for third-party infringement. Advocates for greater enforcement also shifted the enforcement approach from removing problematic content to disabling infringing sites. Thus, intellectual property actors shaped the enforcement strategies and techniques that they consider appropriate (e.g., withdrawing services from infringing sites). By pushing for streamlined, simplified enforcement practices, rights holders also constrained—inadvertently or deliberately—macro-intermediaries' due-process mechanisms, as rapid, mass enforcement is generally incompatible with robust oversight and appeal measures.

i) ***Politics Shaping Technologies***

Macro-intermediaries' anti-infringement enforcement practices did not simply evolve but, as discussed above, were constructed and shaped through ongoing interactions with state and non-state actors in a process that demonstrates politics shaping the use of technology (Bendrath and Mueller 2011:1156). Macro-intermediaries amended and altered their practices in response to existing laws, rights holders' lobbying and litigation, judicial rulings, and governments' threats of legislation and legal action. Intellectual property actors, for example, acknowledge their role in shaping companies' enforcement practices and take credit for pushing eBay toward creating its Verified Rights Owner program.³⁷⁷ Similarly, macro-intermediaries created enforcement programs to ensure their compliance in relation to the European Commission's *E-Commerce Directive*. Legislators also shaped enforcement efforts by demanding specific types of technological regulation. For example, Jeremy Hunt, former Secretary of State at the U.K. Department for Culture, Media and Sport, called upon search engines to demote infringing sites in their search indices.³⁷⁸ In this case, the demand was for search engines to re-configure their webpage-indexing and ranking processes to de-prioritise infringing sites and thereby elevate legitimate sites.

Macro-intermediaries' technologically facilitated enforcement processes are not neutral bits of code. Google, PayPal and others created their enforcement programs to protect their platforms and users from various types of wrongdoing, such as fraud or malicious attacks. This technology is both real, in that it performs specific tasks, and constructed because it is imbued with certain norms, ideas and cultural values. These values and norms stem from those who created the technology and the companies that operate, as well as intellectual property actors. For example, the European Commission's *E-Commerce Directive* does not impose a general obligation for intermediaries to monitor

³⁷⁷ Interview with Siân Croxon, Partner, DLA Piper, 14 September 2012, London.

³⁷⁸ Minutes from the Search Roundtable Discussion with Rights Holders and Search Engines in February 2012 (see Bradwell 2012).

their platforms for third-party infringement.³⁷⁹ However, states—on behalf of rights holders—compelled macro-intermediaries to monitor their platforms proactively, thus imposing an obligation to monitor. Intermediaries thus became gatekeepers responsible for detecting and determining the legality of content and transactions.

Macro-intermediaries expanded their monitoring technologies to scan their platforms proactively but, because they do not have the requisite knowledge to distinguish genuine products from suspicious ones, they are dependent upon rights holders' indicators of authenticity for thousands of brands. Denise Yee, senior trademark counsel at Visa, admits that the company is “not well positioned” to identify infringement. Further, “where legality is not clear, we have no authority to decide what is lawful. We are then forced into the precarious position of either agreeing with the IP owner or the merchant” (Yee 2011:13). Rights holders have shaped macro-intermediaries' proactive measures as they determine what constitutes authenticity and compile indicators of suspicious activity that they provide to macro-intermediaries to facilitate their enforcement activities.³⁸⁰

ii) ***Drawbacks to Regulating through Technology***

Regulation through technology offers considerable benefits for regulators like speed and the capability to police mass populations but there are drawbacks. Underlying the regime's proactive enforcement efforts is the assumption that counterfeits (physical goods) can be identified and distinguished from legitimate goods by scanning the products' photographs and text descriptions (digital information) for anomalies. Some cases are obvious, for instance, if the seller labels the goods as “replicas” to indicate their identical appearance to genuine branded goods. In other cases, it is extremely difficult to determine whether a product is genuine or not.

³⁷⁹ The E-Commerce Directive Art. 47 prevents member states from imposing a general obligation on service providers to monitor their platforms but allows monitoring in a specific case.

³⁸⁰ For example, rights holders and trade associations provide training to intermediaries to facilitate their identification and policing of counterfeit goods. They also provide brand-specific information so these intermediaries can distinguish between genuine and suspicious goods.

Technology is not only a socially constructed tool: it may also cause unintended consequences and collateral damage to legitimate users. While automated systems speed up the identification and targeting of suspicious activities, these systems can also result in the wrongful identification and targeting of legitimate content and legally operating sites. As macro-intermediaries process more complaints and police more transactions, mistakes—and abuse—inevitably occur. Internet actors recognise that inaccurate takedowns are a problem. Theo Bertram, Google’s Public Policy Manager in the U.K., told the U.K. government’s industry roundtable on intellectual property that search engines’ notice-and-takedown program were subject to problems, including competitors improperly removing legitimate content.³⁸¹ Legitimate sites, particularly those run by small businesses and individuals, are poorly equipped to defend themselves against heavy-handed enforcement practices. Despite the problem of wrongful takedowns, few complainants are held liable for bad-faith accusations. Further, rights holders have few incentives to be more specific in their targeting of wrongdoing or to react to unjustifiable takedowns, as civil-advocacy groups note (Samuels and Stoltz 2012).³⁸²

a) Weak Due-Process Measures

Regulatory programs that rely upon technology-facilitated enforcement have relatively weak due-process mechanisms. Rights holders have an interest in determining infringement quickly, broadly and at a minimal cost. Testing purchases—buying and examining a suspicious product—is generally accepted as the most accurate way to determine whether a product is counterfeit or genuine. Test purchases, however, can be “tricky if you’ve got a site selling very expensive goods,” notes Siân Croxon, a partner in London with the law firm DLA Piper.³⁸³ As part of their efforts to streamline their enforcement processes, some Internet firms and payment providers no longer insist upon test purchases. Visa, MasterCard and PayPal do not require rights holders to make test purchases as part of the International Anti-Counterfeiting Coalition’s

³⁸¹ Minutes from the Search Roundtable Discussion with Rights Holders and Search Engines in February 2012 (see Bradwell 2012).

³⁸² Although complainants must attest to Internet firms that their submissions are accurate, few complainants are held liable for bad-faith accusations, similar to the case of wrongful takedowns in relation to digital-copyright infringement (see Samuels and Stoltz 2012).

³⁸³ Interview with Siân Croxon, Partner, DLA Piper, 14 September 2012, London.

merchant-account termination program (Montanaro 2012). The European Commission also does not require rights holders to conduct test purchases in its agreement (European Commission 2013).

Macro-intermediaries' appeal mechanisms vary widely in terms of their formality and ease of use. Taobao, for example, has a structured online appeals process that uses the same system that rights holders use to lodge complaints (Spelich 2012). Measures among U.S.-based ad networks, in contrast, are much more under-developed. The ad networks' private agreement only stipulates that the networks "may consider any credible evidence provided by the accused site in defense of the site" in response to a complaint of infringement (Ad Networks 2013). MasterCard's appeal system is complex as it operates through acquiring banks. Site operators who wish to challenge the termination of the MasterCard account must demonstrate to the acquiring bank that issued the merchant account that they are in compliance with the payment industry's rules and prove compliance through documentation from a certified forensic examiner (MasterCard 2013). While some macro-intermediaries operate relatively robust appeals mechanisms, like Taobao, others raise concerns that operators of legitimate sites and merchants would have difficulty or lack resources to navigate through macro-intermediaries' systems to launch appeals.

VI) Missing Voices: Consumer Interests in the Private Regime

Consumers and the public more generally are largely absent from corporate anti-counterfeiting efforts despite rhetoric from government agencies, intellectual property actors and macro-intermediaries about protecting consumers' interests. The mantra of consumer protection underlies anti-counterfeiting measures, whether public or private, because trademarks are intended to serve a public good. Trademarks grant rights holders the ability to preserve their brands. They are also intended to prevent the likelihood of confusion among consumers by enabling individuals to differentiate among goods in the marketplace.³⁸⁴ Consumers rely upon trademarks for information

³⁸⁴ The terms "likelihood of confusion" and "confusingly similar" refer to the standards that form part the test to determine trademark infringement. For a valuable analysis of the difficulties and problems with determining trademark infringement, see Bone (2012).

about products and as indicators of a product's quality or consistency. Rights holders and macro-intermediaries have interests in protecting consumers from being defrauded or harmed. Rights holders want to ensure that consumers retain trust in their brands and keep purchasing their products, while Internet firms and payment providers want to maintain users' confidence in their services.

Two of the private agreements underline the importance of consumers. The European Commission cites the education and protection of consumers as one of its primary reasons for creating an informal private agreement to tackle the online sale of counterfeit goods (European Commission 2013). The ad networks' agreement commits participants, including Google and Yahoo, to an "ongoing dialogue" with stakeholders including "consumer organizations, and free speech advocates" (Ad Networks 2013). Despite the emphasis on consumers' interests, consumers' representatives are curiously absent from all aspects of the private enforcement agreements. There was no participation from consumer groups in the creation of any of the agreements. Nor is there any indication of consultation with consumer groups in relation to the operation of the agreements.

i) *Consumers' Interests in Marketplaces*

As discussed throughout this dissertation, the interests of consumers and multinational corporations are not always aligned. In terms of online shopping, individuals have interests in buying and selling a wide range of products at differing prices from online marketplaces. The popularity of consumer-to-consumer marketplaces, like eBay and Taobao, indicates that consumers want a wide variety of products and value being able to act as small-scale merchants.

For those purchasing goods on these marketplaces, anti-counterfeiting enforcement activities can unduly and unfairly restrict consumers' access to legitimate goods, particularly those that may be unpopular with rights holders. eBay, for example, contends that some rights holders are using the issue of counterfeit goods to set rules governing the online distribution of their products, particularly in relation to the distribution of luxury brands. eBay claims that these

rights holders are unfairly attempting to “exact ever greater control over e-commerce,” which negatively affects what the marketplace can sell (eBay 2008). For rights holders, marketplaces’ practice of mass policing is a desirable enforcement strategy and consumers benefit from the removal of fraudulent or unsafe products from the marketplace. Rights holders and consumers have shared interests in a secure, effectively functioning e-commerce environment, as well as a healthy, vibrant Internet. However, enforcement practices that enable rights holders to determine the legitimacy of products without physical evidence and remove genuine products because they object to their online sale at particular price points are unduly broad and unfair to consumers.

i) *Negative Economic Effects of Informal Private Agreements*

Looking beyond consumers, private informal anti-counterfeiting efforts can have negative effects on business and the Internet as a whole. With respect to firms, given the scale of corporate anti-counterfeiting activities and the reliance upon automated tools, legitimate marketplace merchants and website operators are undoubtedly being swept up in enforcement dragnets. Analysis of wrongful removal of copyright-infringing content (e.g., Urban and Quilter 2006) shows that mass policing of intellectual property is neither targeted nor accurate.

Enforcement efforts that target the sale of counterfeit goods through marketplaces may inadvertently capture small-scale merchants who legitimately sell second-hand or overstock goods, or resell wholesale quantities of goods. The sale of such goods can be a point of contention with rights holders who wish to control the online distribution of their products or discourage the sale of second-hand products because of fears that these sales may damage their brand’s reputation or cut into their customer base. Rights holders, for example, have ordered multiple eBay sellers to stop offering second-hand Coach purses (Masnick 2011).³⁸⁵ As eBay and Taobao increase their proactive enforcement capacities, legitimate merchants will likely be mistakenly targeted.

³⁸⁵ According to eBay sellers in the class action lawsuit against Coach, the luxury brand claimed that their sales listings for second-hand Coach products infringed its trademarks and eBay removed the listings (Masnick 2011).

Macro-intermediaries that enact technological chokepoints can inadvertently throttle legitimate activities alongside unwanted behaviour. Proponents of this strategy say it can “shrink the universe” of Internet firms that provide services to infringing sites (Johnson 2013). The goal is to push infringing sites away from mainstream, legitimate service providers toward less-reputable firms. Legitimate merchants, however, may be negatively affected by the loss of payment or domain name services. These individuals can be understood as “stranded citizens” (Brown and Marsden 2013:183) that typically do not have the resources or knowledge to challenge allegations of infringement, particularly when accused by large, multinational rights holders. Appeal mechanisms are often complex and merchants may be unsure of their legal rights and unable to afford legal representation.

a) Anti-Competitive Behaviour

Anti-competition effects are another potential problem. The eight private enforcement agreements studied in this dissertation involve global firms that dominate the provision of key Internet services in relation to search, advertising, payment, domain names and marketplaces. Intellectual property actors and macro-intermediaries recognise the challenge of avoiding anti-competitive behaviour—or the perception of such behaviour—in relation to their private agreements. Linda Kirkpatrick, a senior executive with MasterCard, referred to the issue when she spoke alongside colleagues from PayPal and Visa on a panel at a conference hosted in 2012 by the International Anti-Counterfeiting Coalition in Washington. “Some of us are competitors in our space,” Kirkpatrick notes. “It’s not often that you get MasterCard, PayPal and Visa on the same panel. Our lawyers don’t let us” (Kirkpatrick 2012). Kirkpatrick’s comments indicate that these big payment providers are sensitive to the perception that coordinated standard setting and enforcement efforts could be construed as anti-competitive actions.

Payment providers—of all the macro-intermediaries studied—have the strongest regulatory capacity because they can commercially cripple targeted sites by withdrawing payment-processing facilities. Site operators that lose their payment services can institute alternative payment methods but these methods

have to be trusted, popular and effective to attract consumers. Through their private enforcement agreements, PayPal, Visa, MasterCard and American Express have significant discretion (and, more importantly, state support) to take action against sites that they reasonably believe are involved in infringement. As discussed in chapter 4, PayPal takes a particularly aggressive approach to determining infringement and has withdrawn payment processing from companies that offer services PayPal contends are a high risk for facilitating infringement (Enigmax 2013; Ernesto 2012). The companies PayPal targets include those offering virtual private networks, BitTorrent file sharing protocol, and file storage services, all of which are legal, valuable technologies with legitimate uses. PayPal can set the conditions under which companies and individuals use its services but the firms' targeting of legal technologies and services is unduly broad and unfair to legitimate companies and their users.

Similar problems are evident in relation to domain name and search/advertising macro-intermediaries. Returning to the Centre for Safe Internet Pharmacies discussed in chapter 5, consumers have interests in accessing safe, affordable medicine and benefit from enforcement activities that remove pharmacies selling dangerous, misbranded or adulterated medication. However, it is problematic when corporate actors with financial ties to the pharmaceutical industry (for example, the pharmacy-verification firm, LegitScript) have the authority to designate online pharmacies as "illegal" and then request macro-intermediaries to withdraw their services. Proper safeguards and oversight mechanisms are not readily apparent in this area, which raises the troubling possibility that legitimate pharmacies may be targeted and lose critical services. Through the Centre for Safe Internet Pharmacies, rights holders and macro-intermediaries have the capacity—and the support of the U.S. government—to shape the online distribution of medication in ways that can benefit the pharmaceutical industry over consumers.

Similarly, Google is wrongly removing legitimate search results, sometimes because of abusive complaints, (Urban and Quilter 2006).³⁸⁶ This problem will

³⁸⁶ Urban and Quilter (2006) observe that some of the wrongful removals they study are from corporate actors who target their competitors' websites and send erroneous takedown complaints to Google.

only grow as Google removes ever-increasing numbers of allegedly infringing search results. In terms of advertising, as discussed in chapter 4, industry-generated blacklists to prevent the placement of ads on infringing sites have the potential to censor sites mistakenly labelled as infringing and stifle businesses that may pose a threat (e.g., the next “YouTube”) to the established corporate interests and business models. Industry-generated blacklists have a troubled history of wrongly designating legitimate sites as infringing (Ernesto 2011), a problem that is compounded when the blacklists are compiled secretly and implemented without effective oversight and auditing processes.

In summary, macro-intermediaries—particularly payment providers—can act as private arbiters in relation to the legality of specific firms, and, more broadly, in relation to Internet services, technologies and applications. This sledgehammer approach to enforcement can retard innovation and constrain the development of new services and technologies that rights holders may argue facilitate infringement (Mazzone 2011; Raustiala and Sprigman 2012).

VIII) Conclusion

As the preceding discussion shows, the states involved in the private anti-counterfeiting regime play a central, if hidden, role. The European Commission, Department for Culture, Media and Sport, and the Office of the Intellectual Property Enforcement Coordinator cajoled and coerced macro-intermediaries into negotiations with rights holders and endorsed the resulting private, non-binding enforcement agreements. These state actors largely operate from the shadows and through closed-door meetings that are off-limits to consumer or civil-advocacy groups. Instead of operating openly, the states involved in the regime strategically under-play their role as architects of the regime and emphasise the voluntary nature of the agreements.

A responsibility of government is to promote and protect important public policy initiatives, such as competition, freedom of expression, and due process. The states involved in the private regime have the capacity to reshape the regulatory efforts to represent public interests. These state actors, however, stress, but do not demand that corporate actors follow established principles of good

governance. By offloading responsibility for good governance principles to the regime's corporate actors, the government agencies involved in the regime are abdicating their duty to represent the public interest. Given the secrecy of the regime's creation and activities, there has been little public awareness of the regime or its activities.³⁸⁷

i) ***Locating the Public Interest in Private Regulatory Regimes***

In July 2013, following the announcement of the ad networks' best practices, Victoria Espinel praised the agreement and said all enforcement must be consistent with "the Administration's broader Internet policy principles emphasizing privacy, free speech, fair process, and competition" (Espinel 2013). These principles are laudable, however, the private agreements fall far short. These agreements have weak procedural measures and serious normative challenges, in part, because they were created in secret to side step the difficulties of drafting and implementing legislation, as well as the controversy that accompanied SOPA in the United States and the *Digital Economy Act* in the United Kingdom. Industry and government actors designed the agreements to give corporate actors significant latitude to target and control online infringement and the ability to do so in relative secrecy. Some rights holders and macro-intermediaries are reluctant to disclose their enforcement efforts publicly because of fears of angering or alienating their customers, or damaging their brand by admitting problems with infringement.³⁸⁸

For these reasons, these agreements are deeply problematic and seriously flawed. Given the interest of these governments in facilitating secretive private regulation on the Internet, they do not represent consumers' interests or those

³⁸⁷ Traditionally, however, states have been very poor at protecting consumers' interests, which is why many consumers' rights campaigns are grass-roots efforts that pressured states to act, often against entrenched economic interests. Braithwaite and Drahos (2000:609-611) examine the gap between what citizens want (often better, higher standards of regulatory protection) and what citizens get (often lower standards of regulatory protection) and conclude that this is largely because of regulatory capture of states by business, similar to the case of intellectual property protection on the Internet.

³⁸⁸ A senior policy advisor with the Office of the Intellectual Property Enforcement Coordinator told me that, "in a post-PIPA and post-SOPA world," private-sector companies are "reluctant to identify publicly the measures they are taking online to address infringements of intellectual property." Interview with Senior Policy Advisor, Office of the Intellectual Property Enforcement Coordinator, Executive Office of the President, 18 May 2012, Washington.

of the general public. Further, in their push to expand corporate regulation that is based upon mass online surveillance and policing, the states involved in the private anti-counterfeiting regime are actively undermining fundamental digital rights, particularly privacy.

ii) ***Toward a Digital Bill of Rights***

Given these significant challenges, how can we begin to address the problems inherent in this case of private regulation and, in particular, bring the public (and public interests) back into the picture? It is not practical to look to the corporate actors participating in the private anti-counterfeiting regime. While these actors are powerful multinational companies with varying degrees of influence with the state, they have stronger interests in facilitating informal private regulation than resisting this type of regulation. More importantly, it is not possible to rely upon the government agencies involved in the regulatory regime from the United States, United Kingdom and European Union. These agencies have abdicated their duty to represent the public interest and protect fundamental due-process measures. In part, these states are unwilling to address consumers' interests because there is a lack of public pressure. However, as is discussed below, public pressure on the regime can come through a push for greater transparency.

It is beyond the scope of this dissertation to propose a framework to guide transnational activism on this subject. However, it is important to outline possible first steps toward this goal based on this dissertation's analysis and findings. Two key themes that emerge from my analysis of the private enforcement agreements are the necessity of transparency and the vital importance of protecting Internet users' digital privacy and, more broadly, digital rights. Transparency is sorely lacking in these agreements, particularly in those coordinated by the U.S. and U.K. governments. Neither government, moreover, is especially enthusiastic about disclosing information in relation to the agreements.³⁸⁹ State transparency is deficient, thus, a push for industry

³⁸⁹ The U.K. Department for Culture, Media and Sport first only released information on its industry roundtables through freedom of information requests but later published minutes from a May 2013 meeting on its departmental website. In contrast, the U.S. Office of Management and Budget, which hosts the Office of the Intellectual Property Enforcement Coordinator, denied a

transparency is a possible interim step to begin to raise public awareness of informal private regulation on the Internet and to stimulate a much-needed critical discussion of regulatory accountability and legitimacy in this area of governance.

a) A Call for Transparency

As will be explored in greater detail in the following chapter, companies use industry transparency reports to disclose their enforcement activities on behalf of governments and rights holders. These reports, if undertaken in a manner similar to Google's *Transparency Report*, would provide valuable data on the scale of corporate anti-counterfeiting efforts, trends in enforcement, and details of complainant (rights holders) and enforcement actors (macro-intermediaries). Regular disclosures could enable researchers and practitioners to track and suggest correctives in relation to errors, unfair or unduly harsh enforcement practices, and systematic problems in relation to weak due-process measures.

Persuading macro-intermediaries to adopt transparency reports in relation to their informal regulatory efforts against online infringement will be challenging. However, many U.S.-based Internet firms are now mindful of the value of transparency reports, as will be discussed in chapter 8. Their interest in disclosing their regulatory efforts on behalf of states came because of a public backlash, as a result of Edward Snowden's leaked files, against firms that supply information to the U.S. National Security Agency.

b) Marco Civil – a Useful Roadmap

In terms of working towards a framework for digital rights, a useful example can be found in Brazil. On April 23, 2014, Brazilian President Dilma Rousseff passed a trailblazing bill, the *Marco Civil da Internet*, which translates as the "Internet Bill of Rights" into law.³⁹⁰ It is the first of its kind in the world. For the

freedom of information request pertaining to payment providers' informal agreements citing confidential trade information (Masnick 2014).

³⁹⁰ An English-language version of the Marco Civil law is available here from InfoJustice.org, a civil-advocacy group: <http://infojustice.org/wp-content/uploads/2013/11/Marco-Civil-English-Translation-November-2013.pdf>

purposes of this dissertation, the *Marco Civil* provides a useful roadmap both in terms of the way it was created and its content.³⁹¹ After policymakers drafted the first iteration of the bill in 2009, there was an 18-month public consultation period through an open-access online platform. Access, a transnational digital rights group that campaigned for *Marco Civil*, describes the consultative process:

It was truly a hybrid and transparent forum: users, civil society organizations, telcos, governmental agencies, all provided comments side-by-side. Each contributor could see the others' contributions, and all cards on the table had to be considered (Access 2014).

Nearly 2,000 people provided comments on the bill and the government then incorporated these amendments into the next version of the bill (Biddle 2014). This open process facilitated debate among all interested parties, not just powerful corporate stakeholders, and allowed a diversity of opinions. Further, it put into practice the oft-lauded but rarely exercised principle of multi-stakeholder consultation.³⁹²

Marco Civil covers a wide range of issues, from intermediary liability and net neutrality to privacy. Importantly, it establishes a set of rights and principles that, among other provisions include the protection of privacy and personal data.³⁹³ Supporters of *Marco Civil* hail it as expressing “strong commitment to an Internet that is an open, collaborative, democratic, space for individual and collective expression” (Moncau and Mizukami 2014). The law is, of course, not perfect. In relation to the corporate collection of personal data, it allows Internet firms to do so if the collection can be justified, is not forbidden, and is specified in Internet firms' terms-of-use agreements.³⁹⁴ The *Marco Civil* is useful because it provides a framework for other countries to model, both in terms of its open-

³⁹¹ The Green Party in New Zealand proposed a similar bill—the Internet Rights and Freedom Bill—in April 2014. It is the first bill that crowdsources comments and amendments from the public through an open digital platform. The bill includes proposals for an Internet Rights Commissioner and a set of ten rights, including the right to encryption technology and the right to privacy, see: <http://www.internetrightsbill.org.nz/>.

³⁹² The Online Protection and Enforcement of Digital Trade Act (OPEN), which was proposed as an alternative to SOPA, also solicited comments from the public. Darryl Issa, a California Republican and one of the bill's co-sponsors, called for public comments on his site. As of January 19, 2012—one day after the anti-SOPA Internet Blackout—the site had 101 “community suggestions” and 72 comments. See: www.Keepthewebopen.com.

³⁹³ *Marco Civil da Internet*, Art. 3 II and III.

³⁹⁴ *Marco Civil da Internet*, Chapter II, Art. 8(a)(b)(c).

consultative process and in its provisions that codify principles of human rights on the Internet. The real test, however, will come in its implementation and enforcement, particularly when individuals' rights are set against corporations' economic interests and the state's security interests.

c) A Path to Digital Rights

The big lesson in relation to *Marco Civil* is that it is possible to craft a law that codifies principles of digital rights, including privacy, freedom of expression, data protection, and net neutrality, even when they are vehemently opposed by entrenched corporate interests. *Marco Civil* was, for example, delayed for over two years in the Brazilian Chamber of Deputies as Internet firms lobbied to water down provisions in relation to privacy, among other issues (Moncau and Mizukami 2014). Despite these challenges, the law is a considerable achievement for digital-rights activists. In the words of the Australian civil-advocacy group Global Voices, *Marco Civil* is a “victory” that “can bring hope to those working to improve user protections worldwide” (Biddle 2014). In the wake of the Snowden files, which stimulated President Rousseff to push forward the *Marco Civil* and propose privacy provisions,³⁹⁵ there is a surge of interest in digital privacy and digital rights.

Following the SOPA protests and ongoing outcry against the NSA's surveillance programs revealed in the Snowden files, Internet users are increasingly aware of and concerned about corporate and state surveillance on and regulation of the Internet. The SOPA protests and the introduction of *Marco Civil* show that it is possible to mobilise individuals over time and to push forward ideas that preserve and enhance individual freedoms. As will be seen in the final chapter, the SOPA protests, the ongoing public criticism of the U.S. National Security Agency's surveillance programs, and *Marco Civil* can provide us with ideas on how to strengthen transparency and digital rights in relation to the private regulation of the Internet. The introduction of an Internet constitution in Brazil—

³⁹⁵ The Snowden files revealed that Rousseff and some of her key aides had their digital communications monitored by the NSA. In response, Rousseff proposed that all Internet firms' data on Brazilians should be held within the country. After an outcry from technologists, civil-advocacy group and Internet firms that it would balkanise the Internet, the government relented (Reuters 2014).

a victory for digital-rights activists and the public, as well as the Brazilian government—shows that the state can be brought back in to regulate on behalf of public interests. This even holds true in relation to governance on the Internet where corporations and state security agencies have strong preferences for minimal safeguards for the collection and retention of personal data that facilitate mass online surveillance and enforcement.

Chapter 8: Locating the Public Interest in Private Regulation

This dissertation began by asking why a small group of U.S. Internet firms and payment providers, which dominate their respective industry sectors, would agree to increase their regulatory responsibilities voluntarily on behalf of rights holders. It questioned why states, particularly the United States and the European Union, would intervene and compel macro-intermediaries to act as voluntary gatekeepers in the regulation of counterfeit goods on the Internet. The eight private, non-legally binding enforcement agreements examined in this dissertation involve some of the largest Internet firms and payment providers, from Google, PayPal and eBay to MasterCard, Visa and GoDaddy. Through an analysis of these private agreements, which were created between 2010 and 2013, this dissertation finds that the private regulatory regime created as a result of those agreements is highly reliant upon state actors in the United States and the European Union and is a product of state coercion. In addition to its coercive underpinnings, there are overlapping interests among the regime's corporate and state actors in protecting intellectual property and, more broadly, shared interests in expanding macro-intermediaries' regulatory capacity on the Internet. For the states involved in the regime, working with (and through) macro-intermediaries enables them to further exert control online to control undesirable or criminal activities, such as child pornography websites, as well as serve their national security interests by expanding their online surveillance capabilities.

This chapter proceeds as follows. First, it gives an overview of the dissertation and draws together its principal empirical findings and theoretical insights. Second, the chapter considers the policy implications raised by this type of state-created private regulatory regime. Reflecting on the regime's transparency deficit discussed in chapter 7, it proposes ways that corporate and state actors can be persuaded to bring transparency into the regime. The chapter concludes by calling for greater political engagement from the public to begin to address the problems inherent in this type of private regulatory regime and, more generally, unaccountable corporate-state online surveillance practices.

I) Overview and Key Findings

Chapter 1 established the secretive, undemocratic manner in which government agencies in the United States, United Kingdom and European Union created the private enforcement agreements in closed-door, industry-only meetings. It laid out the varying interests rights holders, macro-intermediaries, and the above-noted states have in creating a private regulatory regime to govern online infringement. These states are non-neutral arbitrators among competing corporate interests as their interests largely align with strengthening the protection of intellectual property on the Internet.

Chapter 2 set out a three-part theoretical framework that weaves together concepts of regulatory regimes, private authority, and techno-regulation from the non-state governance and law and technology literatures. Through this framework, the dissertation examined the actors, rules, and interests comprising the regulatory regime, as well as the nature and limitations of rights holders' private authority, which is understood in this project as the capacity to make rules that others adopt (Green 2013). The third component, techno-regulation, focuses analysis on the ways macro-intermediaries employ technology to control infringing sites, along with the complexities and challenges of policing through technology.

Chapter 3 established the historical, legal, and technological contexts in which the private enforcement agreements were formed. Politically, the United States and European Union accord great importance to the protection of intellectual property, a socially constructed perspective that rights holders have shaped by conceptually linking intellectual property to trade (Drahos and Braithwaite 2002). Legally, macro-intermediaries face a fragmented, uncertain landscape: there is little clarity on the nature and scale of macro-intermediaries' regulatory responsibilities, or their degree of liability in relation to third-party infringement on their platforms.³⁹⁶ In terms of technology, the online environment is conducive to mass surveillance and policing, particularly by macro-intermediaries. Macro-intermediaries have a global regulatory capacity and the capability to withdraw essential Internet services, a form of techno-regulation,

³⁹⁶ This point draws from McNamee (2011) and Mac Sithigh (2013) and their analysis of the legal uncertainty facing Internet intermediaries.

which makes them indispensable gatekeepers for both corporations and states. These inter-related factors explain both the development of macro-intermediary-facilitated regulation and states' interest in using coercive means to compel their regulation of online infringement through private agreements.

Chapters 4 through 6 analysed eight private enforcement agreements to examine how and why macro-intermediaries adopted informal regulatory measures to address online infringement. These macro-intermediaries, which offer a range of important Internet services, can remove infringing content (e.g., eBay sales listings). They can also withdraw their services from infringing sites in an enforcement strategy intended to “choke” sites' access to key Internet services (e.g., payment). Chapter 4 examined payment and advertising macro-intermediaries' regulation of infringing sites through private enforcement agreements, while chapter 5 did the same for search and domain name macro-intermediaries. Chapter 6 analysed online marketplaces' implementation of private agreements to control the sale of counterfeit goods through their platforms.

These three chapters depicted and critically examined the global private regulatory regime that is based upon the non-binding private enforcement agreements. The regime is comprised of a distinct constellation of actors—prominent multinational rights holders, macro-intermediaries and powerful state actors from the United States and European Union—and has distinct roots in the United States and the European Union. Macro-intermediaries, which have vast platforms and command dominant market shares in their respective industry sectors, are a special type of Internet intermediary with considerable regulatory capabilities. With their global scope and technologically sophisticated surveillance and enforcement programs, these companies have capabilities that outstrip traditional physical-world gatekeepers, like banks. As gatekeepers for online infringement, however, their regulatory effectiveness varies widely. Only payment macro-intermediaries have the regulatory capacity to cripple infringing sites as they withdraw essential commercial services. In contrast, website operators can easily replace services withdrawn by domain³⁹⁷ and advertising

³⁹⁷ As discussed in chapter 5, in addition to cancelling domain names, domain registrars can also suspend DNS resolution. This means that the site may not be found or, instead of

macro-intermediaries,³⁹⁸ and search engines and marketplaces only remove content but do not impair services.³⁹⁹

Technology—and its use as an enforcement tool—is an important part of the regime as automated enforcement processes enable the regime to regulate globally, rapidly and over a mass population. Automation fundamentally changes how regulation can occur. Regulators, whether public or private, can detect and target problems globally in a way that was previously unaffordable or technological unfeasible. In relation to private anti-counterfeiting enforcement, macro-intermediaries' efforts are generally more coordinated, streamlined, and rapid than their previous efforts, and have a lower evidential burden. Precision, however, is often sacrificed for speed and scale. As the actors within the regime undertake policing on a mass scale, the scope for mistakes is considerable, potentially affecting large numbers of legitimate transactions, search results, sites, or individuals. These challenges speak to the complexities and attendant challenges of policing using technology as a regulatory instrument, particularly in the online realm.

Chapter 7 drew together the dissertation's empirical and analytical findings and reflected upon its themes of the role of the state in private regulation, state-corporate inter-dependencies, and the rapidly evolving relationship between regulation and technology. Underlying each of the private enforcement agreements studied in this dissertation, state actors played a central role in constructing and legitimising the regime by applying coercive pressure on macro-intermediaries. State intervention was necessary because rights holders and their trade associations were unable alone to persuade macro-intermediaries to make wholesale changes to their enforcement practices. Rights holders' authority, while significant in shaping states' intellectual property policymaking, is limited in relation to private actors to threatening legal action, shaming, and granting or withholding business deals. Rights holders have an

displaying the proper site, the user may be redirected to a warning banner. However, site operators may simply shift to another domain registrar and register another domain name.

³⁹⁸ Advertising actors can withdraw ads from infringing sites but such sites tend not to reply upon mainstream advertising. If they use ads, they tend to be in less-reputable sectors like the sex industry (see Watters 2014).

³⁹⁹ Search engines remove search results' hyperlinks to infringing webpages but do not affect the content of those webpages, which may be found using other search engines. Marketplaces remove infringing sales listings but individuals can re-list items under another name or move to another trading platform.

institutional advantage over macro-intermediaries, particularly in relation to the U.S. government, which is the global proponent of stronger intellectual property rights. In the United States, rights holders' interests are politically entrenched following their successful, decades-long campaign that has strengthened the protection of intellectual property in the United States and internationally.

Private enforcement agreements offer benefits for all actors within the regulatory regime as they allow for more flexible, rapid, and streamlined enforcement than is generally possible through legislation or litigation. Further, participants can also take advantage of the secrecy of private agreements to avoid public scrutiny. More broadly, the regulatory regime is coupled together by overlapping interests. Rights holders and macro-intermediaries have shared interests in protecting intellectual property, although there are disagreements in relation to enforcement tactics and the degree of regulatory burden each party can (and should) assume.

Macro-intermediaries, particularly Google, have interests in furthering their surveillance-oriented business models that are premised upon accumulating and mining vast troves of users' personal and commercial data (see Mayer-Schönberger and Cukier 2013; Schneier 2013). The regime's state actors, in turn, have interests in capitalising upon macro-intermediaries' regulatory capacity so that the states can further exert their influence in the online environment over illegal content, such as child pornography and terrorist-extremism websites. In addition, macro-intermediaries' global networks and vast troves of data facilitate states' national security interests, particularly those of the U.S. government, and enable states to intensify their online surveillance programs.

Consumers—and the public in general—are largely overlooked by the private online anti-counterfeiting regime. The regime's actors created the enforcement agreements in closed-door meetings and implemented them quietly, without civil-society involvement. State and corporate actors alike emphasize the importance of protecting consumers from counterfeit goods. Consumers, however, have broad interests in accessing a wide range of products at varying prices, both new and second-hand, that can conflict with rights holders' desire to control the distribution and pricing of their products. More seriously, state

actors' encouragement of macro-intermediaries to set rules amongst themselves to govern infringement raises concerns of anti-competitive behaviour. In addition, the secretive, unaccountable nature of the regime is antithetical to democracy and the public interest. The states involved in the regime—government agencies in the U.S. and U.K., and the European Commission—are unwilling to serve consumers' interests in this area, in part because there is no public pressure on states in relation to this issue.

Beyond online regulation, this dissertation's findings raise several areas for future investigation. U.S.-based Internet firms, particularly Google, are rapidly expanding their political-lobbying capabilities in the United States, as demonstrated by their increased expenditure on lobbying.⁴⁰⁰ The rise of Internet firms' lobbying power will affect policymaking in the United States and, given the scale of firms like Google, influence Internet-related policies worldwide. The ways in which this shift in political influence to Internet firms will shape policymaking in relation to intellectual property, digital privacy and corporate online surveillance practices, and regulation on the Internet more generally, are critical areas for future research. Further, my analysis of the private anti-counterfeiting regime points to a need for further research into rapidly evolving practices of regulation through technology and the attendant complexities and challenges. To what degree do my findings translate to other areas in which Internet firms, particularly macro-intermediaries, act as gatekeepers on behalf of states or other corporate actors, such as the control of child pornography websites? How are macro-intermediaries' gatekeeping efforts and, in particular, their latitude in setting and enforcing rules governing the use of their platforms, shaping how Internet users access and employ certain technologies, such as file-sharing software or virtual private networks?

II) Challenging Private Regulation on the Internet

This dissertation's analysis of a relatively secretive global private regulatory regime underscores the procedural challenges and normative complexities of not only corporate online regulation but also policing through technology in ways that facilitate mass online surveillance and enforcement. The private

⁴⁰⁰ As discussed in chapter 3, Google is now among the top five lobbying corporations in Washington, D.C., alongside companies like AT&T.

regime ostensibly targets online infringement; however, the regulatory strategy of mass policing and enacting chokepoints has the potential to sweep millions of legitimate users into enforcement dragnets. Moreover, when corporate interests align with those of the state in relation to the provision of enforcement, lines of accountability are murky and boundaries between “general’ and ‘specific’ interests are hopelessly blurred” (Sheptycki 2001:13). There are also serious practical concerns of how this type of state-facilitated corporate regulation affects how individuals access and use Internet services and technologies. At a broader level, macro-intermediaries have the capacity act as private arbiters of the legality of products offered for sale as they have considerable latitude in determining and targeting infringement. This means that macro-intermediaries, particularly payment providers, can shape the development of new technologies and services on the Internet as they can withdraw their services from companies that they contend facilitate the distribution of counterfeit goods.

As these previously shadowy regulatory efforts come to light, it is timely and important to examine critically the implications of corporate online regulation through technology. Unearthing and examining these challenges requires an inter-disciplinary approach—drawing upon, in particular, socio-legal studies, sociology, computer science, criminology and political science. This scholarship must be accompanied by practical outreach to engage the public and educate key stakeholders who can affect change in this area. While such efforts are beyond the scope of this dissertation, this chapter sets out preliminary steps to improve the regime’s transparency and then engage the public. A focus on transparency is a necessary first step as there is little public awareness of this private regulatory regime or its global enforcement efforts. Before doing so, however, the next section briefly outlines the regime’s principal challenges.

i) *Procedural and Normative Problems*

The regulation of online infringement through private informal agreements raises significant procedural and normative challenges. Government officials who coordinated the agreements stressed that they should adhere to principles of accountability and due process (European Commission 2013). There is little evidence, however, of these principles in practice in any of the agreements studied for this project. The creation of these agreements suggests that this

regime's accountability and oversight mechanisms are problematic. Small groups of industry and state actors drafted the agreements in closed-door meetings and the texts therefore represent relatively narrow interests. There was no involvement from consumer or civil-society organizations, despite rhetoric of working with and on behalf of consumers. There is no mechanism for public or judicial review, or for oversight of the agreements. Further, the government agencies involved provide no indication of any governmental oversight. In fact, representatives from the Office of the Intellectual Property Enforcement Coordinator frankly admitted that the office did not want to stipulate oversight provisions that may "add layers of difficulty that might drive participants away" from informal private agreements.⁴⁰¹ Those involved in the agreements differ in their desire for the agreements to remain below the public radar. For example, the European Commission published its informal agreement with marketplaces on its website (European Commission 2011). In contrast, IPEC and the U.K. Department for Culture, Media and Sport were reluctant to release publicly the private agreements they negotiated. A senior policy official from IPEC argued that publicity may deter some companies from participating in the arrangements and the office did not want disclosure of signatories "to be a bar for the participants."⁴⁰²

All of the private agreements studied here have weak due-process mechanisms. Enforcement is based on rights holders' allegations, not proof of infringement. This is because macro-intermediaries generally do not require complainants to make test purchases of suspect products to demonstrate that they are counterfeit.⁴⁰³ Furthermore, while macro-intermediaries are increasing their proactive targeting of infringing content, they acknowledge that they are not well suited to differentiating genuine from infringing goods (for Visa, see Yee 2011). It is particularly difficult to determine authenticity on the basis of keywords and photographs supplied by sellers. There "are many criteria that help you assess whether it's likely to be a counterfeit," explains Jeremy

⁴⁰¹ Interview with Senior Policy Advisor, Office of the IP Enforcement Coordinator, Executive Office of the President, 18 May 2012, Washington.

⁴⁰² Ibid.

⁴⁰³ For example, test purchases are not required for the International Anti-Counterfeiting Coalition's merchant-account termination program (Montanaro 2012). Nor are they required for the Canadian Anti-Fraud Centre's merchant-account termination program. Interview with Barry Elliott, Criminal Intelligence Analytical Unit, Canadian Anti-Fraud Centre, 27 June 2012, by telephone.

Newman, a partner with Rouse Legal in London.⁴⁰⁴ “You’ll never be sure until you see that physical sample.”

Overall, then, the private agreements studied in this dissertation are fundamentally problematic because stakeholders—both industry and government—designed them to streamline, simplify and accelerate enforcement processes. Principles of due process and accountability are generally incompatible with the shift toward rapid mass enforcement. Automated processes exacerbate these problems as they enable rights holders to submit enormous numbers of complaints to macro-intermediaries like eBay or Google. These firms use automated programs to address the problem, generally within a few hours. Given the volume of complaints and the timeframes for processing, there is not adequate time to review or investigate the allegations. The emphasis on rapid, mass policing exacerbates the problem of wrongful takedowns of non-infringing content and wrongful termination of services to legitimate sites.

ii) ***Preliminary Steps for Greater Transparency***

The private anti-counterfeiting regime’s efforts are antithetical to fundamental, commonly agreed upon principles of good governance, which emphasise transparency of governance efforts, accountability of regulatory actors, fairness, and robust due-process mechanisms. Regulation through private enforcement agreements is also contrary to internationally accepted tenets of Internet policymaking, which emphasize the importance of consulting all relevant stakeholders. As Peter Bradwell from the U.K. Open Rights Group argues, private online regulation “should not be an excuse for invitation-only policy making” (Bradwell 2011). In 2011, the Organisation for Economic Cooperation and Development (OECD) introduced a set of principles for policymaking on the Internet. Chief among these is a recommendation that processes of rule production, implementation, and enforcement should involve multi-stakeholder collaboration in which all interested parties participate. This includes representatives from consumer and civil-society organisations (OECD 2011). The OECD’s guidelines also echo good governance principles in their emphasis

⁴⁰⁴ Interview with Jeremy Newman, Partner, Rouse Legal, 10 September 2012, London.

on the importance of transparency and accountability. The private enforcement agreements, as discussed above, have multiple procedural and normative challenges. The principle of transparency, however, provides a good starting point to consider preliminary steps to address the significant problems with the agreements. In addition, greater transparency about these agreements is necessary to examine their effects in greater detail and track their evolution. As these agreements are global, cover essential Internet services and can police hundreds of millions of transactions and interactions across the Internet, there is a strong argument to cultivate public awareness in this area.

Transparency is the most promising area to begin reform because macro-intermediaries can strengthen this aspect of their enforcement efforts without involvement from the state or rights holders. There are several concrete steps that macro-intermediaries can take to improve the transparency of their enforcement efforts. They should publicly disclose the full text of their private enforcement agreements and publish their enforcement policies and processes relating to these agreements.⁴⁰⁵ These policies should be written in clear, easy-to-understand language. Macro-intermediaries should clearly set out their procedures for receiving and investigating complaints of infringement and for issuing sanctions. This must include how individuals can appeal allegations of infringement by rights holders and provide contact information to facilitate appeals.

a) Industry Transparency Reports

Industry transparency reports are particularly useful tools to facilitate greater transparency of corporate and state regulation on the Internet. Companies use transparency reports to disclose and track requests for data received from the state or complaints of infringement from rights holders. Google provides a good model in this regard because of its years working with rights holders in the removal of infringing search results. The search giant also provides data to government in relation to requests from law enforcement and to the U.S. National Security Agency (NSA) in regards to national security (Google

⁴⁰⁵ Where these policies are incorporated within broader terms-of-use contractual agreements, which can run to hundreds of pages, they should also publish the policies separately on their websites in an area that is easy to locate.

Transparency Report). The concept of industry transparency reports in relation to disclosure of users' data became a topic of considerable interest to Internet companies and their users when files leaked by Edward Snowden revealed that the U.S. and U.K. national security agencies rely heavily upon data from Internet firms (Ball, Border, and Greenwald 2013). These revelations elicited significant concern and protests from users of the targeted companies, particularly Google, Yahoo, Microsoft and Facebook. Further, the targeted companies complain that since the spying revelations they have lost business from firms outside the United States that want to ensure their data is not targeted by the NSA (Miller 2014). Estimates of these losses by think tanks and research firms vary greatly.⁴⁰⁶ In response, multiple U.S. firms adopted transparency reports to reassure their wary users and business partners. These companies include Microsoft, Yahoo, Twitter, Facebook, Dropbox, Apple and LinkedIn, as well as the telecommunications companies Verizon and AT&T.⁴⁰⁷

Google, the first firm to track its enforcement efforts, discloses most of the requests it receives from governments and rights holders. It discloses the reporting organization (or individual) that submitted the request and the URL of the search result linking to the infringing webpage. Google also tracks the requests it complies with and those it rejects. There is room for improvement in Google's reports. It does not capture all of its services as, for example, it excludes takedown requests for YouTube. Nor does Google indicate the reasons that specific requests are denied, which would help researchers track the number of wrongful or abusive complaints. Transparency reports adopted by Facebook, Twitter and others are similar to Google's report.⁴⁰⁸ Most of them, however, focus solely on disclosing law enforcement requests for data and those related to national security requests.

⁴⁰⁶ For example, the Washington-based think tank, the Information Technology and Innovation Foundation, calculates that the scandal could cost the U.S. cloud computing industry \$35 billion by 2016, while Forrester Research, a technology firm, estimates the losses could range as high as \$180 billion (Miller 2014).

⁴⁰⁷ Links to U.S. firms' transparency reports are available on Google's *Transparency Report* site, see: www.google.com/transparencyreport/.

⁴⁰⁸ Facebook, for example, describes what constitutes lawful requests from governments, how it responds and what kinds of information it releases. Facebook also tracks the numbers of requests received over time, the types of request (e.g., search warrants or subpoena), and the number or percentage of requests in which the company discloses some data. See: <https://govtrequests.facebook.com/country/United%20States/2013-H2/>.

The creation of industry transparency reports demonstrates that Internet firms will respond to pressure from their customers and business clients if they perceive risks to their reputation or the loss of clients (Miller 2014; Schneier 2013). This is particularly true in cases where the firms have interests in emphasising their good management of users' data and, consequently, distancing themselves from controversial or unpopular regulatory efforts. Companies that publish these reports, such as Twitter and LinkedIn, tend to stress their commitment to the principle of transparency on behalf of their users and can use these reports to demonstrate their adherence to good governance practices.⁴⁰⁹ Public pressure could be applied to companies with a transparency reporting process in place, like Facebook and Yahoo, to persuade them to expand their transparency processes to track corporate requests for data. Twitter, for example, has followed Google's lead and tracks requests from governments and also rights holders in relation to the removal of copyright-infringing content.⁴¹⁰ This reporting needs to be expanded to all corporate requests for enforcement, including online anti-counterfeiting efforts. Internet users and digital-rights groups could pressure other companies, like PayPal or GoDaddy, to adopt similar reporting practices by pointing to companies with transparency reports as industry leaders in data management practices.

Aside from informing users how their data is accessed and disclosed, and by whom, corporate transparency reports are valuable to researchers and activists interested in examining state and corporate actors' online surveillance and enforcement activities. Individuals studying digital-copyright enforcement, for example, use Google's transparency report to track trends in the scale and nature of takedown notices, as well as identify problematic and abusive reporting practices (e.g., Seng 2014; Urban and Quilter 2006). Civil-society groups, like the Electronic Frontier Foundation, have used Google's Transparency Report and the Chilling Effects⁴¹¹ site to identify actors who

⁴⁰⁹ The professional networking site LinkedIn, for example, states in its transparency report that it discloses government requests for data so that its users and the public better understand the kinds of requests it receives and how it deals with them. See: <https://www.linkedin.com/legal/transparency>.

⁴¹⁰ For Twitter's tracking of the copyright notices it receives, see: <https://transparency.twitter.com/copyright-notices/2013/jul-dec>

⁴¹¹ The Chilling Effects site is a joint project of the Electronic Frontier Foundation and clinics at law schools in the United States, including Harvard University and Stanford University. It is intended to help individuals understand their legal rights in relation to freedom of expression and intellectual property. See: <http://www.chillingeffects.org/index.cgi>

deliberately submit requests to remove lawful content or seek to censor information.⁴¹² Similar levels of data on corporate anti-counterfeiting efforts using macro-intermediaries would be of significant value to researchers and consumer organisations. Research could track trends in enforcement strategies and techniques, as well as regulatory activities by industry sector, trade associations, and individual rights holders. Moreover, such data would help develop a much-needed picture of the rapidly expanding brand-protection industry that undertakes monitoring and enforcement activities on behalf of rights holders.

iii) *Transparency and the State*

Demands for transparency should not fall solely on macro-intermediaries as government departments in the United States and the European Union played a central role in facilitating the creation of informal private agreements, as did the European Commission. These state actors, however, generally have not been forthcoming in providing information about the informal anti-counterfeiting measures. The U.K. Department for Culture, Media and Sport, for example, has both invited civil-society representatives to its industry roundtables and then dis-invited them.⁴¹³ The Office of Intellectual Property Enforcement Coordinator (IPEC) released some information about its agreements in press releases and in reports to the U.S. Congress but refused to release the payment providers' informal agreement.⁴¹⁴ In contrast, the European Commission, which created its agreements among industry stakeholders, published the text publicly (European Commission 2011).

Given the central role of these states in constructing the private regime, they should bear some responsibility for ensuring that the agreements meet basic standards of good governance and that the public is aware of these private regulatory arrangements. Both IPEC and the DCMS should disclose the full texts of all private enforcement agreements that they have coordinated in this

⁴¹² The Electronic Frontier Foundation collects the worst examples of abusive takedowns and showcases them in its "Takedown Hall of Shame." See: <https://www EFF.org/takedowns>

⁴¹³ The department published minutes of its May 2013 roundtable minutes on its website but only released minutes from early meetings after repeated freedom of information requests by the Open Rights Group.

⁴¹⁴ A U.S. lawyer requested the release of these best practices through freedom of information laws and was denied.

area. In addition, the Canadian Anti-Fraud Centre, which has an arrangement with Visa, should publicly disclose the details of its arrangement.

These government agencies should also clearly and publicly lay out guidelines to ensure that corporate signatories have appropriate due-process mechanisms. In their endorsement of the agreements, government actors stressed the importance of respecting fundamental values, particularly freedom of expression and privacy (see Espinel 2013). However, they provide no guidance as to how corporate actors should uphold these values and no oversight to ensure that they do so. At the very least, if each agency publicly disclosed the text of the agreements and drafted a set of clear guidelines explaining how measures should be implemented, the public would have a basic understanding of these private agreements. Individuals who wished to obtain more information on, complain about, or challenge the regulatory activities could contact the government agency responsible for coordinating the agreements. They could also file freedom of information requests to attempt to access or petition for further information.

These preliminary steps to provide a small degree of transparency in relation to private anti-counterfeiting efforts are vitally important to establish a baseline of publicly available information. To date, these agreements have attracted little attention from scholars or the mainstream press because the agreements are relatively new and there is little publicly available information on them, with the exception of the European Commission's reports. By pressing macro-intermediaries and the government agencies involved in this regime to disclose its policies and practices, along with enforcement results, we could begin cultivating public awareness of the existence of this global private regulatory regime.

III) Conclusion: A Future with Digital Rights

Steps to establish transparency measures in relation to the private anti-counterfeiting regime are critical in the short term in order to begin to build public awareness. However, improved transparency alone cannot address the considerable procedural and normative problems inherent in corporate online anti-counterfeiting efforts. As discussed earlier in the chapter, the states

involved in this regime are not representing the interests of consumers or, more broadly, the general public. Given these states' abdication of public interest in this area, greater political engagement by the public is needed. It is beyond the scope of this dissertation to set out how this political engagement should best occur. However, political action targeting the U.S. government is necessary given its influential role in shaping enforcement standards for the protection of intellectual property. Further, the U.S. government, particularly the Office of the Intellectual Property Enforcement Coordinator, was a key driver of the private enforcement agreements and all the macro-intermediaries are headquartered in the United States.

Two recent events—opposition to the *Stop Online Piracy Act* (SOPA) and the introduction of Brazil's Internet bill of rights (*Marco Civil da Internet*)—demonstrate that it is possible to challenge entrenched interests in relation to state-corporate governance on the Internet. In the United States, the protests that culminated in January 2012 with the massive Internet Blackout began in September 2010 with the *Combating Online Infringement Counterfeiting Act* and grew with the introduction of the *Protect Intellectual Property Act* and SOPA. Over approximately sixteen months, a broad-based coalition against these bills raised awareness through social media, launched petitions and explained to average Internet users how they would be negatively affected by the bills (Moon, Ruffini, and Segal 2013; Sell 2013). These protests demonstrate that there is considerable public interest in the topic of regulation on (and of) the Internet. The protests also show that even with relatively technical issues like intellectual property it is possible to raise public awareness and encourage political engagement. Similarly, ongoing protests against the U.S. National Security Agency in relation to the secretive surveillance programs revealed by Edward Snowden demonstrate significant public interest in issues of digital privacy and concern over corporate-state surveillance alliances on the Internet (Levy 2014).

Engaging the states responsible for the private regulatory regime will be difficult as they have varying interests in facilitating online regulation through macro-intermediaries. Brazil's *Marco Civil* can provide ideas to guide engagement with states and shape legislation that protects digital rights. As chapter 7 discussed,

Marco Civil, introduced in April 2014, is the world's first Internet bill of rights. It offers a useful roadmap for activists in other countries to consider how to raise public awareness of digital-rights issues and interact with governments in a practical, meaningful way. The Brazilian government published a first draft of the bill on an open-access online platform for an 18-month public review (Moncau and Mizukami 2014). The government then invited interested parties, including businesses, individuals, and non-governmental organizations, to comment on and suggest amendments to the bill. Importantly, all comments were publicly available and the Brazilian government incorporated these publicly derived amendments into the next version of the bill (Access 2014). An open-access platform for the public to engage with legislation and other government-created rules ensures that all interested parties are aware of different policy positions or suggestions and can respond accordingly. Actors could still lobby the government privately but this open-access process would ensure that the public has a forum in which to suggest amendments that governments would then consider.

Drawing together ideas from the SOPA protest and *Marco Civil*, civil-society efforts to challenge corporate-state surveillance on the Internet should bring together consumer groups with digital-rights organisations and other parties interested in strengthening digital rights. One important line of activity would be to press macro-intermediaries to adopt or amend industry transparency reports in order to track their enforcement activities on behalf of corporations and states. Alongside this work, citizens must pressure the states responsible for the private regulatory regime to re-assume their public regulatory duties of representing the public interest. This could involve enrolling relevant or sympathetic elements within these states, such as competition watchdogs, privacy and human rights commissioners, and agencies responsible for promoting openness on the Internet and net neutrality. Pressure on states could begin with demands for the disclosure of details of non-binding enforcement agreements and government requirements for macro-intermediaries to publish and track their enforcement activities on behalf of states and corporations. These preliminary steps are necessary to begin to build public awareness and to establish a broad-based multi-stakeholder approach to governance on the Internet.

The private, state-backed agreements discussed in this dissertation raise fundamental questions of who owns our data, and what rights we have to control how states and corporations use our digital footprints. As daunting as the challenges are to reform this private regulatory regime—and they are considerable—there is hope. An important consequence of Edward Snowden’s revelations of surveillance programs by the U.S. government (and its allies) is an increased sensitivity among the public toward digital privacy and digital rights in general.⁴¹⁵ These debates concern the shifting nature of privacy in an era of mass online surveillance by both states and corporations. Members of the public are clearly interested in and concerned about surveillance and enforcement practices on the Internet and are engaging in vibrant global debates over the nature and limits of digital privacy.⁴¹⁶ Bringing the private regulatory regime out of the shadows is the first step toward democratising the online enforcement of trademark infringement and the Internet as a whole.

⁴¹⁵ In January 2014, for example, the non-partisan U.S. PEW Research Centre conducted a survey in which 70% of Americans said that they should not have to give up privacy to be safe from terrorism. <http://www.usatoday.com/story/news/politics/2014/01/20/poll-nsa-surveillance/4638551/>

⁴¹⁶ For example, tens of thousands of people protested against NSA surveillance on the Internet on 12 February 2014, which was called “the day we fight back.” People protested in 15 countries and in the United States individuals directed 18,000 calls and 50,000 emails to the U.S. Congress (Gabbatt 2014).

References

I) Legislation, Legal Cases, and Agreements

Agreement on Trade-Related Aspects of Intellectual Property (TRIPS), opened for signature 15 April 1994 (entered into force 1 January 1995). Agreement Establishing the World Trade Organization, Annex 1C, Legal Instruments—Results of the Uruguay Round, Retrieved November 2, 2011 (http://www.wto.org/english/docs_e/legal_e/27-trips.pdf).

Anti-Counterfeiting Trade Agreement (drafted November 15, 2010, signed in October 2011 by Australia, Canada, Japan, Morocco, New Zealand, Singapore, South Korea and the United States and in 2012 by Mexico, and European Union), not yet in force.

Combating Online Infringement and Counterfeits Act (S. 3804, September 20, 2010) 111th Congress, 2009-2010), never enacted, Retrieved January 2, 2012 (<https://www.govtrack.us/congress/bills/111/s3804>).

Digital Economy Act (Pub. L. c. 24, April 8, 2010), Parliament of the United Kingdom, Retrieved January 10, 2012 (<http://www.legislation.gov.uk/ukpga/2010/24/contents>).

Digital Millennium Copyright Act (Pub. L. 105-304, October 28, 1998), 105th Congress, 1997–1998, Retrieved November 13, 2012 (<https://www.govtrack.us/congress/bills/105/hr2281>).

Electronic Commerce (EC Directive) Regulation 2002 (Pub. L. No. 2013, August 21, 2002, implemented the European Commission E-Commerce Directive), Retrieved March 2, 2013 (http://www.legislation.gov.uk/uksi/2002/2013/pdfs/uksi_20022013_en.pdf).

European Union Directive on electronic commerce on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (2000/31/EC, June 8, 2000), European Parliament, Retrieved April 2, 2012 (http://ec.europa.eu/internal_market/e-commerce/directive/index_en.htm).

Madrid Agreement Concerning the International Registration of Marks and the Protocol Relating to the Madrid Agreement (adopted in 1989 and came into operation on 1 April 1996) Retrieved September 10, 2012 (<http://www.wipo.int/treaties/en/registration/madrid/>).

Marco Civil de Internet (Brazilian Civil Rights Framework for the Internet) (Pub. L. 12.965, April 22, 2014), Brazilian Senate, Retrieved April 23, 2014 (<http://infojustice.org/wp-content/uploads/2013/11/Marco-Civil-English-Translation-November-2013.pdf>).

Online Protection and Enforcement of Digital Trade Act (S. 2029, January 17, 2011) 111th Congress, never enacted; The Online Protection and Enforcement of Digital Trade Act (H.R. 3728, January 18, 2012) 112th Congress, never enacted, Retrieved February 20, 2013 (<http://www.keepthewebopen.com/assets/pdfs/OPEN.pdf>).

- Paris Convention for the Protection of Industrial Property (1883, last amended on September 28, 1979) Retrieved September 6, 2012 (http://www.wipo.int/treaties/en/text.jsp?file_id=288514).
- Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (S. 968, May 12, 2011) 112th Congress, 2011–2013, never enacted, Retrieved February 20, 2012 (<https://www.govtrack.us/congress/bills/112/s968>).
- Prioritising Resources and Organisation for Intellectual Property Act of 2008 (Public Law 110-403, October 13, 2008), 110th Congress, Retrieved September 23, 2012 (<http://www.gpo.gov/fdsys/pkg/PLAW-110publ403/pdf/PLAW-110publ403.pdf>).
- Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks (1891, adopted at Madrid on June 27, 1989, last amended November 12, 2007) Retrieved September 1, 2012 (http://www.wipo.int/wipolex/en/wipo_treaties/text.jsp?file_id=283484).
- Stop Online Piracy Act (H.R. 3261, Oct 26, 2011), 112th Congress, 2011–2013, never enacted, Retrieved November 22, 2011 (<https://www.govtrack.us/congress/bills/112/hr3261>).
- Tiffany Inc. v. eBay, Inc., 576 F. Supp.2d 463 (United States Southern District New York (S.D.N.Y.) 2008). Retrieved May 3, 2012 (https://www.eff.org/files/filenode/tiffany_v_ebay/tiffany-v-ebay-dct.pdf).
- Tort Law of the People's Republic of China (PRC Presidential Order No. 21, July 1, 2010), Retrieved May 23, 2013 (<http://www.wipo.int/wipolex/en/details.jsp?id=6596>).
- Trans-Pacific Partnership Agreement (negotiations opened November 11, 2011, negotiations ongoing), Intellectual Property Rights Chapter Consolidated Text, Advanced Intellectual Property chapter for all 12 nations with negotiating positions. 19th Round of Negotiations at Bandar Seri Begawan, Brunei, August 30, 2013, Wikileaks release November 13, 2013. Retrieved December 4, 2013 (<https://wikileaks.org/tpp/static/pdf/Wikileaks-secret-TPP-treaty-IP-chapter.pdf>).

II) Academic

- Abrahamsen, Rita and Michael C. Williams. 2011. *Security Beyond the State: Private Security in International Politics*. Cambridge: Cambridge University Press.
- Arghavan, Nia, Judith Lynne Zaichowsky, and Judith Lynne. 2000. "Do counterfeits devalue the ownership of luxury brands?" *The Journal of Product and Brand Management*:485-497.
- Atkinson, Rowland and John Flint. 2001. "Accessing Hidden and Hard-to-Reach Populations: Snowball Research Strategies." *Social Research Update* 33.

- Avant, Deborah D., Martha Finnemore, and Susan K. Sell, eds. 2010. *Who governs the globe?* Cambridge: Cambridge University Press.
- Barlow, John Perry. 1996, "A Declaration of the Independence of Cyberspace." Retrieved September 9, 2012 (<https://projects.eff.org/~barlow/Declaration-Final.html>).
- Bartley, Tim. 2007. "Institutional Emergence in an Era of Globalization: The Rise of Transnational Private Regulation of Labor and Environmental Conditions." *American Journal of Sociology* 113:297-351.
- Barzilai-Nahon, Karine. 2006. "Gatekeepers, Virtual Communities and the Gated: Multidimensional Tensions in Cyberspace." *International Journal of Communications Law and Policy* 11:1-28.
- . 2008. "Toward a Theory of Network Gatekeeping: A Framework for Exploring Information Control." *Journal of the American Society for Information Science and Technology* 59:1493-1512.
- Béland, Daniel. 2010. "The Idea of Power and the Role of Ideas." *Political Studies Review* 8:145-154.
- Bendrath, Ralf and Milton Mueller. 2011. "The end of the net as we know it? Deep packet inspection and internet governance." *New Media Society* 13:1142-1160.
- Benkler, Yochai. 2011. "WikiLeaks and the Protect-IP Act: A New Public-Private Threat to the Internet Commons." *Daedalus* 140:154-164.
- Black, Julia. 2008. "Constructing and contesting legitimacy and accountability in polycentric regulatory regimes." *Regulation & Governance* 2:137-164.
- . 2009. "Legitimacy, accountability and polycentric regulation: dilemmas, trilemmas and organisational response." Pp. 241-269 in *Non-State Actors as Standard Setters*, edited by A. Peters, L. Koechlin, T. Förster, and G. F. Zinkernagel. Cambridge: Cambridge University Press.
- Blaikie, Norman. 2000. *Designing Social Research*. Cambridge: Polity Press.
- Blakeney, Michael. 1995. "Intellectual Property in World Trade." *International Trade Law and Regulation* 1:76-81.
- Bone, Robert G. 2012. "Taking the Confusion Out of 'Likelihood of Confusion': Toward a More Sensible Approach to Trademark Infringement." *Northwestern University Law Review* 106:1307-1371.
- Bowling, Ben and James Sheptycki. 2012. *Global Policing*. London: Sage Publications, Inc.
- Braithwaite, John. 2000. "The New Regulatory State and the Transformation of Criminology." *British Journal of Criminology* 40:222-238.

- . 2005. "Neoliberalism or Regulatory Capitalism." Regulatory Institutions Network. Occasional Paper 5. Australian National University, Canberra.
- . 2008. *Regulatory Capitalism: How it works, ideas for making it work better*. Cheltenham, UK: Edward Elgar Publishing, Inc.
- Braithwaite, John and Peter Drahos. 2000. *Global Business Regulation*. Cambridge: Cambridge University Press.
- Bracha, Oren and Frank Pasquale. 2008. "Federal Search Commission? Access, Fairness, and Accountability in the Law of Search." *Cornell Law Review* 93:1149-1210.
- Brey, Philip. 2005. "Artifacts as Social Agents." Pp. 61-84 in *Inside the Politics of Technology: Agency and Normativity in the Co-Production of Technology and Society*, edited by H. Harbers. Amsterdam: Amsterdam University Press.
- Brodeur, Jean-Paul. 2007. *The Policing Web*. Oxford: Oxford University Press.
- Brown, Ian and Christopher T. Marsden. 2013. *Regulating Code: Good Governance and Better Regulation in the Information Age*. Cambridge: MIT Press.
- Brown, Ian and Malte Ziewitz. 2013. "A Prehistory of Internet Governance." Pp. 3-26 in *Research Handbook on Governance of the Internet*, edited by I. Brown. Cheltenham: Edward Elgar.
- Brownsword, Roger. 2008. "So What Does the World Need Now? Reflections on Regulating Technologies." Pp. 23-48 in *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, edited by R. Brownsword and K. Yeung. Oxford: Hart Publishing.
- Bryce, Jo, Neil Horton, and Hayley Limmer. 2010. "Deliverable D14: Purchase of Counterfeit Goods in Europe." COUNTER: Counterfeiting and Piracy Research.
- Büthe, Tim. 2010. "Private Regulation in the Global Economy: A P(Review)." *Business and Politics* 12:1-38.
- Bygnes, Susanne. 2008. "Interviewing People-oriented Elites." Eurosphere Working Paper Series. Online Working Paper No. 10, 2008.
- Cafaggi, Fabrizio. 2012. *Enforcement Of Transnational Regulation: Ensuring Compliance in a Global World*. Cheltenham: Edward Elgar Publishing.
- . 2011. "New Foundations of Transnational Private Regulation." *Journal of Law and Society* 38(1):20-49.
- Casarosa, Federica. 2009. "Online Auction Sites: An Example of Regulation in Electronic Communities?" *European Review of Private Law*:1-23.
- Castro, Daniel, Richard Bennett, and Scott Andes. 2009. "Steal These Policies: Strategies for Reducing Digital Piracy." Washington, DC.

- Chaudhry, Peggy E., Alan Zimmerman, Jonathan R. Peters, and Victor V. Cordell. 2009. "Preserving intellectual property rights: Managerial insight into the escalating counterfeit market quandary." *Business Horizons* 52:57-66.
- Chow, Daniel C.K. 2003. "Organized crime, local protectionism, and the trade in counterfeit goods in China." *China Economic Review* 14:473-484.
- Clarke, Ronald V. 1997. "Situational Crime Prevention: Successful Case Studies." Guilderland, New York: Harrow and Heston, Publishers.
- Cutler, A. Claire. 2002. "Private international regimes and interfirm cooperation." Pp. 23-40 in *The Emergence of Private Authority in Global Governance*, edited by R. B. Hall and T. Biersteker, J. Cambridge: Cambridge University Press.
- . 2010. "The legitimacy of private transnational governance: experts and the transnational market for force." *Socio-Economic Review* 8:157-185.
- Cutler, A. Claire, Virginia Haufler, and Tony POrter. 1999. "Private Authority and International Affairs." Albany: State University of New York Press.
- Dashwood, Hevina S. 2012. *The Rise of Global Corporate Social Responsibility: Mining and the Spread of Global Norms*. Cambridge: Cambridge University Press.
- de Beer, Jeremy and Christopher D. Clemmer. 2009. "Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?" *Jurimetrics Journal* 49:375-409.
- de Chernatony, Leslie, Malcolm McDonald, and Elaine Wallace. 2011. *Creating Powerful Brands*. Oxford: Butterworth-Beinemann.
- de Chernatony, Leslie and Francesca Dall'Olmo Riley. 1998. "Defining a "Brand": Beyond the Literature with Experts' Interpretations." *Journal of Marketing Management* 14:417-443.
- Dedrick, Jason, Kenneth L. Kraemer, and Greg Linden. 2009. "Who profits from innovation in global value chains?: a study of the iPod and notebook PCs." *Industrial and Corporate Change* 19:81-116.
- Deibert, Ronald J., John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2011. "Accessed Contested: Security, Identity, and Resistance in Asian Cyberspace." Cambridge: Open Net Initiative and MIT Press.
- Drahos, Peter. 1995. "Global Property Rights in Information: The Story of TRIPS at the GATT." *Prometheus* 13:6-19.
- Drahos, Peter and John Braithwaite. 2002. *Information Feudalism: Who Owns the Knowledge Economy*. Oxford: Oxford University Press.
- Dutfield, Graham. 2006. "'To copy is to steal:' TRIPS, (un)free trade agreements and the new intellectual property fundamentalism." *Journal of Information Law and Technology* 1:1-13.
- Elkin-Koren, Niva. 2001. "Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing." *University of Dayton Law Review* 26:180-209.

- Flynn, Sean M. 2010. "Special 301 and Access to Medicine in the Obama Administration." *Intellectual Property Brief* 2(2):5-13.
- Flynn, Sean M., Brook Baker, Margot Kaminski, and Jimmy Koo. 2012. "The U.S. Proposal for an Intellectual Property Chapter in the Trans-Pacific Partnership Agreement." *American University International Law Review* 28:105-202.
- Franklin, Sarah. 1995. "Science as Culture, Cultures of Science." *Annual Review of Anthropology* 24:163-184.
- Fuchs, Doris. 2005. "Commanding Heights? The Strength and Fragility of Business POver in Global Politics." *Millennium - Journal of International Studies* 33:771-801.
- . 2007. *Business Power in Global Governance*. Boulder, CO: Lynne Rienner Publishers.
- Fuchs, Doris and Agni Kalfagianni. 2010. "The Causes and Consequences of Private Food Governance." *Business and Politics* 12:1-37.
- Gasser, Urs. 2006. "Regulating Search Engines: Taking Stock and Looking Ahead." *Yale Journal of Law and Technology* 8:201-234.
- Gentry, J. W. 2001. "How now Ralph Lauren? The separation of brand and product in a counterfeit culture." *Advances in Consumer Research* 28:258-265.
- Gereffi, Gary and Stacey Frederick. 2010. "The Global Apparel Value Chain, Trade and the Crisis: Challenges and Opportunities for Developing Countries."
- Gereffi, Gary and Olga Memedovic. 2003. "The Global Apparel Value Chain: What Prospects for Upgrading by Developing Countries." Vienna.
- Goldsmith, Jack and Tim Wu. 2006. *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press.
- Grabosky, Peter. 2005. "Using Non-Governmental Resources to Foster Regulatory Compliance." *Governance* 8:527-550.
- Graz, Jean-Christophe and Eva Hartmann. 2010. "Global regulation of the knowledge-based economy: The rise of standards in educational services." Université de Lausanne, Institut d'Etudes Politiques et Internationales, Bâtiment Anthropole, Lausanne, Switzerland.
- Graz, Jean-Christophe and Andreas Nölke. 2008. "Introduction: Beyond the fragmented debate on transnational private governance." Pp. 2-26 in *Transnational private governance and its limits*, edited by J.C. Graz and A. Nölke. New York: Routledge.
- Green, Jessica F. 2013. *Rethinking Private Authority: Agents and Entrepreneurs in Global Environmental Governance*. Princeton: Princeton University Press.
- Gunningham, Neil and Peter Grabosky. 1998. *Smart Regulation: Designing Environmental Policy*. Oxford: Clarendon Press.

- Haggart, Blayne. 2014. *Copyright: The Global Politics of Digital Copyright Reform*. Toronto: University of Toronto Press.
- Halbert, Debora. 1997. "Intellectual Property Piracy: The Narrative Construction of Deviance." *International Journal for the Semiotics of Law* 10:55-78.
- Hall, Rodney Bruce and Thomas Biersteker, J. 2002. "The emergence of private authority in the international system." Pp. 3-22 in *The Emergence of Private Authority in Global Governance*, edited by R. B. Hall and T. Biersteker, J. Cambridge: Cambridge University Press.
- Hall, Rodney Bruce and Thomas Biersteker, J. 2002. "Private authority as global governance." Pp. 203-222 in *The Emergence of Private Authority in Global Governance*, edited by R. B. Hall and T. Biersteker, J. Cambridge: Cambridge University Press.
- Hall, Rodney Bruce and Thomas Biersteker, J., eds. 2002. *The Emergence of Private Authority in Global Governance*, edited by R. B. Hall and T. Biersteker, J. Cambridge: Cambridge University Press.
- Hildebrandt, Mireille. 2008. "A Vision of Ambient Law " Pp. 175-192 in *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, edited by R. Brownsword and K. Leung. Oxford: Hart Publishing.
- Hofmann, Jeanette. 2010. "The Libertarian Origins of Cybercrime: Unintended Side-Effects of a Political Utopia." Centre for Analysis of Risk and Regulation: An ESRC Research Centre. Discussion Paper No. 2. London School of Economics.
- Horten, Monica. 2011. "European Commission brokers eBay counterfeit takedown agreement." *IPtegrity*. May 5, 2011. Retrieved November 13, 2011 (<http://www.iptegrity.com/index.php/ipred/640-european-commission-brokers-ebay-counterfeit-takedown-agreement>).
- Introna, Lucas D. and Helen Nissenbaum. 2000. "Shaping the Web: Why the Politics of Search Engines Matters." *The Information Society* 16:169-185.
- Johnston, Les. 2000. "Transnational private policing: The impact of global commercial security." Pp. 21-42 in *Issues in Transnational Policing*, edited by J. Sheptycki. New York: Routledge.
- Jordana, Jacint and David Levi-Faur. 2004. *The Politics of Regulation: Institutions and Regulatory Reforms for the Age of Governance*. Cheltenham: Edward Elgar Publishing.
- Katyal, Neal Kumar. 2002. "Architecture as Crime Control." *The Yale Law Journal* 111:1039-1139.
- . 2003. "Digital Architecture as Crime Control." *The Yale Law Journal* 112:2261-2289.
- Koch, Martin. 2011. "Non-state and State Actors in Global Governance." Pp. 197-208 in *The Ashgate Research Companion to Non-State Actors*, edited by B. Reinalda. Surrey, England: Ashgate Publishing Limited.

- Kohl, Uta. 2012. "The rise and rise of online intermediaries in the governance of the Internet and beyond – connectivity intermediaries." *International Review of Law, Computers & Technology* 26:185-201.
- Kohl, Uta. 2013. "Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (Part 2)." *International Review of Law, Computers & Technology* 21:187-234.
- Kolson, Barbara, Heather McDonald, and Darren Pogoda. 2004. "Panel III: The New Campaign Against Counterfeiting and Piracy." *Fordham Intellectual Property, Media and Entertainment Law Journal* 14:955-1003.
- Kopel, Karen. 2013. "Operation Seizing in Our Sites: How the Federal Government is Taking Domain Names Without Prior Notice." *Berkeley Technology Law Journal* 28:859-900.
- Kraakman, Reiner H. 1986. "Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy." *Journal of Law, Economics, & Organization* 2:53-104.
- Kraemer, Kenneth L., Greg Linden, and Jason Dedrick. 2011. "Who Captures Value in the Apple iPad and iPhone?" Personal Computing Industry Centre, An Alfred P. Sloan Foundation Centre.
- Krasner, Stephen D. 1982. "Structural Causes and Regime Consequences: Regimes as Intervening Variables." *International Organization* 36:185-205.
- Lacey, Nicola and Lucia Zedner. 2012. "Legal constructions of crime." Pp. 159-181 in *The Oxford Handbook of Criminology*, edited by R. Maguire, R. Morgan, and R. Reiner. Oxford: Oxford University Press.
- Laidlaw, Emily. 2009. "Private Power, Public Interest: An Examination of Search Engine Accountability." *International Journal of Law and Information Technology* 17:113-145.
- . 2010. "A framework for identifying Internet information gatekeepers." *International Review of Law, Computers & Technology* 24:263-276.
- . 2012. "The responsibilities of free speech regulators: an analysis of the Internet Watch Foundation." *International Journal of Law and Information Technology* 20:312-345.
- Latour, Bruno. 2005. *Reassembling the Social: An Introduction to Actor-Network Theory*. Oxford: Oxford University Press.
- Leenes, Ronald. 2011. "Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology." *Legisprudence* 5:143-169.
- Lehrer, Andrew. 2012. "Tiffany v. eBay: Its Impact and Implications on the Doctrines of Secondary Trademark and Copyright Infringement " *Boston University Journal of Science and Technology Law* 18:373-403.
- Lemley, Mark, David S. Levine, and David G. Post. 2011. "Don't Break the Internet." *Stanford Law Review Online* 64:34-38.

- Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.
- . 2006. *Code: And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books.
- Levi-Faur, David. 2005. "The Global Diffusion of Regulatory Capitalism." *The ANNALS of the American Academy of Political and Social Science* 598:12-32.
- . 2013. "The Odyssey of the Regulatory State: From a "Thin" Monomorphic Concept to a "Thick" and Polymorphic Concept." *Law & Policy* 35:29-50.
- Lichtman, Doug and Eric Posner. 2004. "Holding Internet Service Providers Accountable."
- Lindenbaum, Jeffrey A. and David Ewen. 2012. "Catch Me if You Can: An Analysis of New Enforcement Measures and Proposed Legislation to Combat the Sale of Counterfeit Products on the Internet." *Pace Law Review* 32:567-640.
- Liu, He (Lonnie), Kirill Levchenko, Márk Félegyházi, Christian Kreibich, Gregor Maier, Geoffrey M. Voelker, and Stefan Savage. 2011. "On the Effects of Registrar-level Intervention." Pp. 8 in *LEET'11 Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats*. Berkeley, CA.
- Loughlan, Patricia. 2006. "Pirates, Parasites, Reapers, Sowers, Fruits, Foxes...The Metaphors of Intellectual Property." *Sydney Law Review* 28:211-226.
- Mac Síthigh, Daíthi. 2013. "The fragmentation of intermediary liability in the UK." *Journal of Intellectual Property Law & Practice* 8:521-531.
- MacCarthy, Mark. 2010. "What Payment Intermediaries are Doing About Online Liability and Why it Matters." *Berkeley Technology Law Journal* 25:1139-1122.
- Mackenzie, Simon. 2010. "Counterfeiting as corporate externality: intellectual property crime and global insecurity." *Crime Law and Social Change* 54:21-38.
- . 2010. "Fakes." in *Handbook of Crime*, edited by F. Brookman, M. Macguire, H. Pierpoint, and T. Bennett. London: Willan Publishing.
- Majone, Giandomenico. 1994. "The Rise of the Regulatory State in Europe." *Western European Politics* 17:77-101.
- Mann, Ronald J. and Seth R. Belzley. 2005. "The Promise of Internet Intermediary Liability." *William and Mary Law Review* 47:239-307.
- Matthews, Duncan. 2002. *Globalising Intellectual Property Rights: The TRIPs Agreements*. New York: Routledge.
- Mayer-Schönberger, Viktor 2008. "Demystifying Lessig." *Wisconsin Law Review* 4:713-746.
- Mayer-Schönberger, Viktor and Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. London: John Murray.

- Mazerolle, Lorraine and Janet Ransley. 2005. *Third-Party Policing*. Cambridge: Cambridge University Press.
- Mazzone, Jason. 2011. *Copyfraud and Other Abuses of Intellectual Property Law*. Stanford: Stanford University Press.
- McCoy, Damon, Hitesh Dharmdasani, Christian Kreibich, Geoffrey M. Voelker, and Stefan Savage. 2012. "Priceless: The Role of Payments in Abuse-advertised Goods." in *ACM Computer and Communications Security Conference*. Raleigh, North Carolina.
- McCoy, Damon, Andreas Pitsillidis, Grant Jordan, Nicholas Weaver, Christian Kreibich, Brian Krebs, Geoffrey M. Voelker, Stefan Savage, and Kirill Kevchanko. 2012. "PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs." in *Security'12 Proceedings of the 21st USENIX conference on Security symposium* Bellevue, WA.
- McIntyre, T. J. and Colin Scott. 2008. "Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility." Pp. 109-124 in *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, edited by R. Brownsword and K. Leung. Oxford: Hart Publishing.
- McNamee, Joe. 2011. "The Slide from 'Self-Regulation' to Corporate Censorship." European Digital Rights Initiative.
- Meidinger, Errol. 2002. "Forest Certification as a Global Civil Society Regulatory Institutions." Pp. 265-289 in *Social and Political Dimensions of Forest Certification*, edited by E. Meidinger, C. Elliott, and G. Oesten. Remagen-Oberwinter: Gupta Books.
- Mellyn, Jack. 2010. "'Reach Out and Touch Someone': The Growing Use of Domain Name Seizure as a Vehicle for the Extraterritorial Enforcement of U.S. Law." *Georgetown Journal of International Law* 42:1241-1264.
- Mertha, Andrew C. *The Politics of Piracy: Intellectual Property in Contemporary China*. 2007. Ithaca: Cornell University Press.
- Moon, David, David Ruffini, and David Segal. 2013. "Hacking Politics: How Geeks, Progressives, The Tea Party, Gamers, Anarchists and Suits Teamed up to Defeat SOPA and Save the Internet." OR Books.
- Mostert, Frederick W. and Martin B. Schwimmer. 2011. "Notice and Takedown for Trademarks." *The Trademark Reporter* 101:249-281.
- Mueller, Milton, Andreas Kuehn, and Stephanie Michelle Santoso. 2012. "Policing the Network: Using DPI for Copyright Enforcement." *Surveillance & Society* 9:348-364.
- Murray, Andrew. 2011. "Nodes and Gravity in Virtual Space." *Legisprudence* 5:195-221.
- O'Malley, Pat. 2010. "Simulated Justice: Risk, Money and Telemetric Policing." *British Journal of Criminology* 50:795-807.

- O'Reilly, Conor. 2010. "The transnational security consultancy industry: A case of state-corporate symbiosis." *Theoretical Criminology* 14:183-210.
- . 2011. "'From Kidnaps to Contagious Diseases': Elite Rescue and the Strategic Expansion of the Transnational Security Consultancy Industry." *International Political Sociology* 5:178-197.
- O'Reilly, Conor and Graham Ellison. 2006. "'Eye Spy Private High': Re-Conceptualizing High Policing Theory." *British Journal of Criminology* 46:641-660.
- Odell, John S. and Susan K. Sell. 2006. "Reframing the issue: the WTO coalition on intellectual property and public health, 2001." Pp. 85-114 in *Negotiating Trade: Developing Countries in the WTO and NAFTA*, edited by J. S. Odell. Cambridge: Cambridge University Press.
- Osborne, David and Ted Gaebler. 1992. *Reinventing Government: the Entrepreneurial Spirit is Transforming the Public Sector*. New York: Plume.
- Paster, Benjamin G. 1969. "Trademarks - Their Early History." *The Trademark Reporter* 59:551-572.
- Penz, Elfriede and Barbara Stöttinger. 2008. "Corporate Image and Product Similarity - Assessing Major Demand Drivers for Counterfeits in a Multi-Country Study." *Psychology and Marketing* 25:352-381.
- Peters, Anne, Till Förster, and Lucy Koechlin. 2009. "Towards non-state actors as effective, legitimate, and accountable standards." Pp. 492-561 in *Non-state Actors as Standard Setters*, edited by A. Peters, T. Förster, L. Koechlin, and G. F. Zinkernagel. Cambridge: Cambridge University Press.
- Peters, Ann, Lucy Koechlin, Till Förster, and Gretta Fenner Zinkernagel, eds. 2009. "Non-State Actors as Standard Setters." Cambridge: Cambridge University Press.
- Picciotto, Sol. 2011. *Regulating Global Corporate Capitalism*. Cambridge: Cambridge University Press.
- Piscitello, Dave. 2012. "Thought Paper on Domain Seizures and Takedowns."
- Power, Michael. 1997. *The Audit Society: Rituals of Verification*. Oxford: Oxford University Press.
- Prakash, Aseem and Matthew Potoski. 2014. "Global Private Regimes, Domestic Public Law: ISO 14001 and Pollution Reduction." *Comparative Political Studies* 47:369-394.
- Raustiala, Kal and Christopher Sprigman. 2012. *The Knockoff Economy: How Imitation Sparks Innovation* Oxford: Oxford University Press.
- Reidenberg, Joel R. 1998. "Lex informatica: The formulation of information policy rules through technology." *Texas Law Review* 76:553-593.
- Rhodes, Rod A. W. 2012. "Waves of Governance." Pp. 32-48 in *The Oxford Handbook of Governance*, edited by D. Levi-Faur. Oxford: Oxford University Press.

- Ribisl, Kurt M., Rebecca S. Williams, HZIya Gizlice, and Amy H. Herring. 2011. "Effectiveness of State and Federal Government Agreements with Major Credit Card and Shipping Companies to Block Illegal Internet Cigarette Sales." *PLoS ONE* 6.
- Ricketson, Sam. 1994. *Intellectual Property: Cases, Materials and Commentary*. Sydney: Butterworths.
- Rimmer, Matthew. 2011. "'Breakfast at Tiffany's': eBay Inc, Trade Mark Law and Counterfeiting." *Journal of Law, Information & Science* 21:128-166.
- Robson, Stephani K. A. 1999. "Turning the Tables: The Psychology of Design for High-Volume Restaurants." *Cornell Hotel and Restaurant Administration Quarterly* 40:56-63.
- Rothacher, Albrecht. 2004. "Corporate Cultures and Global Brands." London: World Scientific Publishing Co.
- Rutter, Jason and Jo Bryce. 2008. "The Consumption of Counterfeit Goods: 'Here Be Pirates?'" *Sociology* 42:1146-1164.
- Sassen, Saskia. 2002. "The state and globalization." Pp. 91-112 in *The Emergence of Private Authority in Global Governance*, edited by R. B. Hall and T. J. Biersteker. Cambridge: Cambridge University Press.
- Schmitt, Bernd. 2012. "The consumer psychology of brands." *Journal of Consumer Psychology* 22:7-17.
- Scott, Colin. 2002. "Private Regulation of the Public Sector: A Neglected Facet of Contemporary Governance." *Journal of Law and Society* 29(1):56-76.
- Sell, Susan K. 2003. *Private Power, Public Law: The Globalization of Intellectual Property Rights*. Cambridge: Cambridge University Press.
- . 2010. "The Global IP Upward Ratchet, Anti-Counterfeiting and Piracy Enforcement Efforts: The State of Play." American University Washington College of Law, Washington, D.C.
- . 2011. "TRIPS was Never Enough: Vertical Forum Shifting, FTAs, ACTA, and TPP." *Journal of Intellectual Property Law* 18:448-478.
- . 2013. "Revenge of the 'Nerds': Collective Action against Intellectual Property Maximalism in the Global Information Age." *International Studies Review* 0:1-19.
- Seng, Daniel. 2014. "The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices." *Virginia Journal of Law and Technology*.
- Sheet, The Green. 2005. "Card Companies Agree to Ban Transactions From Online Cigarette Sales." in *The Green Sheet*: Assistant Chief Counsel, Bureau of Alcohol, Tobacco and Firearms.

- Shen, Anqui, Georgios A. Antonopoulos, and Kalus Von Lampe. 2010. "The Dragon Breathes Smoke": Cigarette Counterfeiting in the People's Republic of China." *British Journal of Criminology* 50:239-258.
- Sheptycki, James. 1997. "Insecurity, Risk Suppression and Segregation: Some Reflections on Policing in the Transnational Age." *Theoretical Criminology* 1:303-315.
- . 2000. *Issues in Transnational Policing*. London: Routledge.
- . 2001. "Accountability Across the Policing Field: Towards a General Cartography for Post-Modern Policing." in *Democratic Control of Policing and Security Sector Reform*. Geneva, Switzerland: Geneva Centre for the Democratic Control of Armed Forces.
- Smith, Leigh. 2011. "European Commission publishes Memorandum of Understanding on the sale of counterfeit goods over the internet." *Journal of Intellectual Property Law & Practice* 6:770-771.
- Spink, Amanda, Bernard J. Jansen, Chris Blakely, and Sherry Koshman. 2006. "A study of results overlap and uniqueness among major web search engines." *Information Processing and Management* 42:1379-1391.
- Strange, Susan. 1997. "The Retreat of the State: The Diffusion of Power in the World Economy." *International Journal* 52:366-369.
- Suchman, Mark C. 1995. "Managing Legitimacy: Strategic and Institutional Approaches." *The Academy of Management Review* 20:571-610.
- Swami, Viren, Tomas Chamorro-Premuzic, and Adrian Furnham. 2009. "Taking it: Personality and individual difference predictors of willingness to buy counterfeit goods." *The Journal of Socio-Economics* 38:820-825.
- Swire, Peter P. 2005. "Elephants and Mice Revisited: Law and Choice of Law on the Internet." *University of Pennsylvania Law Review* 153:1975-2001.
- Teddlie, Charles and Fen Yu. 2007. "Mixed Methods Sampling: A Typology with Examples." *Journal of Mixed Methods Research* 1:77-100.
- Underhill, Geoffrey R. D. 2003. "States, markets and governance for emerging market economies: private interests, the public good and the legitimacy of the development process." *International Affairs* 79:755-781.
- Urban, Jennifer M. and Laura Quilter. 2006. "Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act." *Santa Clara Computer and High Technology Law Journal* 22:621-693.
- Urbas, Gregor. 2005. "Criminal Enforcement of Intellectual Property Rights: Interaction Between Public Authorities and Private Interests." Pp. 303-322 in *New Frontiers of Intellectual Property Law*, edited by C. Heath and K. A. Sanders. Oxford: Hart Publishing.
- Vandenbergh, Michael P. 2007. "The New Wal-Mart Effect: The Role of Private Contracting in Global Governance." *UCLA Law Review* 54:913-970.

- Vixie, Paul. 2012. "Refusing REFUSED." in *CircleID: Internet Infrastructure*.
- Wall, David S. and Joanna Large. 2010. "Jailhouse Frocks: Locating the Public Interest in Policing Counterfeit Luxury." *British Journal of Criminology* 50:1094-1116.
- Watters, Paul A. 2013. "Measuring Online Advertising Transparency in Singapore: An Investigation of Threats to Users."
- . 2014. "The prevalence of High-Risk and Mainstream Advertisements Targeting Canadians on Rogue Websites."
- Weatherall, Kimberlee. 2012. "The New (Old) War on Copyright Infringement, and How Context is Opening New Regulatory Possibilities." *Media International Australia* 143:110-121.
- Whimster, Sam, ed. 2004. *The Essential Weber Reader*. New York: Routledge.
- Wilks, Stephen. 2013. *The Political Power of the Business Corporation*. Cheltenham, UK: Edward Elgar Publishing.
- Woo, Elaine Lee Hee. 2010. "Online Auction Sites and Inconsistencies: A Case Study of France, China, and the United States " *American University Intellectual Property Brief* 1:50-57.
- Woodiwiss, Michael. 2001. *Organized Crime and American Power: A History*. Toronto: University of Toronto Press.
- Zittrain, Jonathan. 2006. "A History of Online Gatekeeping." *Harvard Journal of Law & Technology* 19:253-298.
- . 2008. "Perfect Enforcement on Tomorrow's Internet." Pp. 125-156 in *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, edited by R. Brownsword and K. Yeung. Portland, Oregon: Hart Publishing.

III) Government

- Chesnut, Robert. 2007. "Testimony of Robert Chestnut, Senior Vice President, Rules, Trust and Safety, eBay, Inc." SubCommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary.
- City of London Police. 2014. "City of London Police call on advertising and brand sectors to help tackle cyber crime." April 28. Retrieved May 3, 2014 (<http://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/City-of-London-Police-call-for-help-tackle-cyber-crime.aspx>).
- Commission, European. 2004. "Directive 2004/48/EC of The European Parliament and of the Council on the enforcement of intellectual property rights - 29 April 2004." *Official Journal of the European Union*.
- . 2009. "Communication From the Commission to the Council, the European

Parliament and the European Economic and Social Committee. Enhancing the enforcement of intellectual property rights in the internal market." Brussels.

- . 2011. "Memorandum of Understanding." European Commission, Brussels.
- . 2012. "Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet - 2nd Quarterly Meeting Summary." Directorate General Internal Market and Services.
- . 2012a. "A European Consumer Agenda - Boosting confidence and growth. Commission from the Commission to the European Parliament, The Council, The Economic and Social Committee and the Regions." Brussels.
- . 2013. "Report from the Commission to the European Parliament and the Council on the Functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet."

Goodlatte 2011. "The Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Member, Committee on the Judiciary." Hearing on H.R. 3261, The "Stop Online Piracy Act". Before the Committee of the Judiciary, U.S. House of Representatives, November 16, 2011. Washington, DC.

House of Commons. 2013. "Supporting the Creative Economy." United Kingdom House of Commons, Culture, Media and Sport Committee. September 11. Retrieved February 2, 2014 (<http://www.publications.parliament.uk/pa/cm201314/cmselect/cmcumeds/674/674.pdf>).

DOJ. 2011. "Google Forfeits \$500 Million Generated by Online Ads & Prescription Drug Sales by Canadian Online Pharmacies." Department of Justice. Retrieved November 12, 2013 (<http://www.justice.gov/opa/pr/2011/August/11-dag-1078.html>).

Espinel, Victoria. 2011. "Remarks of Victoria Espinel, White House Intellectual Property Enforcement." *Marielle Gallo "IP Forum."* Brussels, Belgium. November 22. Retrieved November 5, 2013 (<http://www.ipforum.eu/medias/The%20US%20perspective%20of%20IPR%20enforcement%20by%20Victoria%20Espinel.pdf>).

- . 2011a. "Hearing Before the Subcommittee on Intellectual Property, Competition, and the Internet of the Committee on the Judiciary, House of Representatives." Washington, DC.
- . 2012. "Spoken Testimony - Testimony of Victoria A. Espinel, U.S. Intellectual Property Enforcement Coordinator, Office of Management and Budget, Before the U.S. Senate Committee on the Judiciary." May 9, 2012. Washington, DC.
- . 2012a. "Testimony of Victoria A. Espinel, U.S. Intellectual Property Enforcement Coordinator, Office of Management and Budget, Before the U.S. House of Representatives, Committee on the Judiciary, Subcommittee on Intellectual Property, Competition, and the Internet." September 20, 2012. Washington, DC.
- . 2012b. "Intellectual Property and the U.S. Economy." *White House Blog*. April 11. Retrieved November 3, 2013

(<http://www.whitehouse.gov/blog/2012/04/11/intellectual-property-and-us-economy>).

- . 2013. "Coming Together to Combat Online Piracy and Counterfeiting." *White House Blog*. July 15. Retrieved July 15, 2013 (<http://www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting>).

Espinell, Victoria, Aneesh Copra, and Howard Schmidt. 2012. "Combating Online Piracy While Protecting an Open and Innovative Internet." *The White House Blog*. January 14. Retrieved February 3, 2013 (<http://www.whitehouse.gov/blog/2012/01/14/obama-administration-responds-we-people-petitions-sopa-and-online-piracy>).

GAO. 2013. "Internet Pharmacies: Federal Agencies and States Face Challenges Combating Rogue Sites, Particularly Those Abroad." Government Accountability Office. Washington, DC.

Interpol. 2012. "Global crackdown on illicit online pharmacies." *Interpol Media release*, October 4. Retrieved December 12, 2012 (<http://www.interpol.int/News-and-media/News/2012/PR077>).

- . 2013. "International operation targets online sale of illicit medicines." *Interpol Media release*, June 27. Retrieved September 3, 2013 (<http://www.interpol.int/News-and-media/News/2013/PR077>).

IPEC. 2011. "Counterfeit Pharmaceutical Inter-Agency Working Group Report to the Vice President of the United States and to Congress." Washington, DC.

- . 2012. "2011 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement." March 20. Office of the Intellectual Property Enforcement Coordinator. Washington, DC.

- . 2013. "2013 Joint Strategic Plan on Intellectual Property Enforcement." Office of the Intellectual Property Enforcement Coordinator. Washington, DC.

Johnson, Travis. 2013. "Request of the United States Patent and Trademark Office for Public Comments: Voluntary Best Practices Study. 78 Fed. Reg. 37210 (June 20, 2013)." Comments Regarding USPTO's Joint Strategic Plan for Intellectual Property Enforcement Voluntary Best Practices Study. International Anti-Counterfeiting Coalition, Washington, D.C. Retrieved September 15, 2013 (http://www.uspto.gov/ip/officechiefecon/comments_joint_strategic_plan.jsp).

Jones, Christine N. 2011. "Statement of Christine N. Jones, Executive Vice-President, General Counsel & Corporate Secretary, The GoDaddy Group, Inc., Hearing on "Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II," Before the United States House of Representatives Committee on the Judiciary, Subcommittee on Intellectual Property, Competition and the Internet. April 6, 2011. Washington, DC.

Kirkpatrick, Linda. 2011. "Testimony of Linda Kirkpatrick, Group Head, Franchise Development / Customer Performance Integrity, MasterCard Worldwide, Hearing on H.R. 3261, The "Stop Online Piracy Act". Before the Committee of the Judiciary, U.S. House of Representatives, November 16, 2011. Washington, DC.

- OECD. 2011. "OECD Council Recommendations on Principles for Internet Policymaking." Organization for Economic Cooperation and Development. December 13. Retrieved June 3, 2012 (<http://www.oecd.org/sti/ieconomy/49258588.pdf>).
- OHIM. 2013. "The European Citizens and Intellectual Property: Perception, Awareness and Behaviour." Office for the Harmonization in the Internal Market. Programme of the European Observatory on Infringements of Intellectual Property Rights. Retrieved March 7, 2014 (https://oami.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IPContributionStudy/25-11-2013/european_public_opinion_study_web.pdf).
- Oyama, Katherine. 2011. "Testimony of Katherine Oyama, Copyright Counsel, Google Inc." Hearing on H.R. 3261, The "Stop Online Piracy Act". Before the Committee of the Judiciary, U.S. House of Representatives, November 16, 2011. Washington, DC.
- Sheffner, Benjamin. 2013. "Comments of the Motion Picture Association of America, Inc." Motion Picture Association of America. Comments Regarding USPTO's Joint Strategic Plan for Intellectual Property Enforcement Voluntary Best Practices Study. Washington, D.C. Retrieved September 15, 2013 (http://www.uspto.gov/ip/officechiefecon/comments_joint_strategic_plan.jsp).
- Smith, Lamar. 2011. "Opening Statement: The Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Chairman, Committee on the Judiciary." Hearing on H.R. 3261, The "Stop Online Piracy Act". Before the Committee of the Judiciary, U.S. House of Representatives, November 16, 2011. Washington, DC.
- U.S. Department of Commerce. 2012. "Intellectual Property and the U.S Economy: Industries in Focus." Prepared by the Economics and Statistics Administration and the United States Patent and Trademark Office. March 2012. Retrieved March 12, 2013 (http://www.uspto.gov/news/publications/IP_Report_March_2012.pdf).
- Walker, Kent. 2011. "Testimony of Kent Walker, Senior Vice President and General Counsel Google Inc." Hearing on "Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II." House Judiciary Subcommittee on Intellectual Property, Competition, and the Internet. Washington, DC.
- Weatherley, Mike. 2014. "Debate over the intellectual property bill." House of Commons Hansard Debates for 20 Jan 2014. U.K. House of Commons. Retrieved February 2, 2014 (<http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm140120/debtext/140120-0002.htm>).
- Wishart, Peter. 2014. "Debate over the intellectual property bill." House of Commons Hansard Debates for 20 Jan 2014. U.K. House of Commons. Retrieved February 2, 2014 (<http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm140120/debtext/140120-0002.htm>).

Wyden, Ron. 2011. "Wyden SOPA Statement Warns of Severe Repercussions to a Free and Open Internet if Bills are Passed." November 16. Retrieved June 21, 2013 (<http://www.wyden.senate.gov/news/press-releases/wyden-sopa-statement-warns-of-severe-repercussions-to-a-free-and-open-internet-if-bills-are-passed>).

Yee, Denise. 2011. "Testimony of Denise Yee, Senior Trademark Counsel, Visa Inc., Targeting Websites Dedicated to Stealing American Intellectual Property, Hearing Before the Committee on the Judiciary, United States Senate." February 16, 2011. Washington, DC.

IV) Industry

2011. "Responsible Practices for Search Engines in Reducing Online Infringement Proposal for a Code of Practice." U.K. Search Engine Roundtable. November 15. Retrieved March 13, 2013 (<https://www.openrightsgroup.org/assets/files/pdfs/proposals%20to%20search%20engines.pdf>).

2012. "UK search: the way ahead." February 28. U.K. Search Engine Roundtable. Retrieved March 13, 2013 (<https://www.openrightsgroup.org/assets/files/files/pdfs/UK%20Search%20Engine%20Code%20of%20Practice%20%281%29.pdf>)

Ad Networks. 2013. "Best Practices Guidelines for Ad Networks to Address Piracy and Counterfeiting." Retrieved July 15, 2013 (<http://www.2013ippractices.com/bestpracticesguidelinesforadnetworkstoaddresspiracyandcounterfeiting.html>).

Alibaba Group. 2012. "Alibaba Annual Report 2011." March 12. Retrieved September 13, 2013 (img.alibabacom/ir/download/.../Full_2011_Annual_Report_ENG.pdf).

Alibaba Group. 2013. "It's Official? Alibaba Doing More Business Than Amazon + eBay." Alibaba.com. June 30. Retrieved September 9 2013 (<http://news.alibabacom/article/detail/insight/100902240-1-it%2527s-official%253F-alibaba-doing-more.html>).

American Express. 2011. "Notice Form Regarding Sales over the Internet of Illegitimate Products." Retrieved September 19, 2013 (<http://www.americanexpress.com/us/content/pdf/legal-disclosures/website-rules-and-regulations/Antipiracy%20Notice%20Form%20-%20Updated%20Oct%202011w.pdf>)

—. 2013. "American Express Merchant Reference Guide U.S." Retrieved November 3, 2013 (https://www209.americanexpress.com/merchant/singlevoice/singlevoiceflash/USSEng/pdf/merchant/PolicyPDFs/US_%20RefGuide.pdf).

ANA. 2012. "Statement of Best Practices to Address Online Piracy and Counterfeiting." Association of National Advertisers. May 3. Retrieved May 5, 2012.

(<http://www.ana.net/content/show/id/23417>).

- Apple. 2014. "Supplier Responsibility 2014 Progress Report." Retrieved May 16, 2014 (https://www.apple.com/au/supplier-responsibility/pdf/Apple_SR_2014_Progress_Report.pdf).
- BAE Systems Detica. 2012. "The Six Business Models for Copyright Infringement." June 27. Retrieved November 7, 2013 (<http://www.baesystemsdetica.com/resources/the-six-business-models-for-copyright-infringement/>)
- Bainbridge, Julie. 2012. "IACC Rooting Out Rogue Merchants: The IACC Payment Processor Portal Mid-Year Review and Vision for the Future." Presented at the International Anti-Counterfeiting Coalition Spring Conference, 2-4 May, Washington, DC.
- Barchiesi, Bob. 2011. "Message from the President IACC Portal Program: Letter from Bob." Get Real. August 18. Retrieved May 28, 2013 (http://4356049642aa3c99a6e91c99180a8219894d6198.gripelements.com/pdf/archive/get_real_newsletter_volume_5.pdf).
- Barchiesi, Bob. 2012. "IACC Payment Processor Portal Training Workshop." Presented at the International Anti-Counterfeiting Coalition Spring Conference, 2-4 May, Washington, DC.
- BASCAP. 2009. "Research Report on Consumer Attitudes and Perceptions on Counterfeiting and Piracy." Business Action to Stop Counterfeiting and Piracy. Retrieved May 7, 2012 (<http://www.iccwbo.org/advocacy-codes-and-rules/bascap/bascap-research/consumer-attitudes-and-perceptions/>).
- Bing. N.d. Intellectual Property Guidelines. Bing ads. Retrieved June 13, 2013 (<http://advertise.bingads.microsoft.com/en-us/editorial-intellectual-property-guidelines>).
- BSA. 2013. "BSA Appoints Victoria Espinel to be President and CEO." Business Software Alliance. August 29. Retrieved September 3, 2013 (<http://ww2.bsa.org/country/News%20and%20Events/News%20Archives/global/08282013-BSAsNewPresidentCEOEspinel.aspx>).
- Caldwell, Robert. 2012. "IACC Rooting Out Rogue Merchants: The IACC Payment Processor Portal Mid-Year Review and Vision for the Future." Presented at the International Anti-Counterfeiting Coalition Spring Conference, 2-4 May, Washington, DC.
- Digital Strategy Consulting. 2013. "Third of UK brands 'have no idea where display ads appear online.'" November 22. Retrieved February 3, 2014 (http://www.digitalstrategyconsulting.com/intelligence/2013/11/third_of_uk_brands_have_no_idea_where_display_ads_appear_online.php)
- Dougherty, Dan. 2011. "Combating Counterfeits: eBay's Global Approach." *Landslide* 4(2):1-3.
- eBay. 2013. *Annual Report 2012, Form 10-K*. eBay, Inc. Retrieved November 7, 2013 (<http://www.sec.gov/Archives/edgar/data/1065088/000106508813000004/ebay2>)

[012_10k.htm](#)).

- eBay. 2013a. "eBay User Agreement." Retrieved May 17, 2013 (<http://pages.ebay.com.au/help/policies/user-agreement.html>).
- eBay. 2008. "eBay Vows to Fight Following Overreach by LVMH." *eBay, Inc. Blog*. June 30. Retrieved May 6, 2013 (<http://blog.ebay.com/ebay-vows-to-fight-following-overreach-by-lvmh/>).
- Elliott, Martin, Director of Corporate Risk Management, Visa International. 2012. "Rooting out Rogue Merchants." Presented at the International Anti-Counterfeiting Coalition Spring Conference, 2-4 May, Washington, DC.
- GoDaddy. 2013. "GoDaddy Universal Terms of Service Agreement." Retrieved November 11, 2013 (au.godaddy.com/legal-agreements.aspx).
- Google. N.d. "Transparency Report." Retrieved March 7, 2013 (<http://www.google.com/transparencyreport/removals/copyright/faq/>).
- . 2012. "Annual Report 2012, Form 10-K." Retrieved June 5, 2013 (https://investor.google.com/pdf/20121231_google_10K.pdf).
- . 2013. "Counterfeit goods." Retrieved November 13, 2013 (https://support.google.com/adwordspolicy/answer/176017?hl=en&ref_topic=1346942).
- . 2013. "How Google Fights Piracy." September 10. Retrieved September 15, 2013 (<https://docs.google.com/file/d/0BwxyRPFduTN2dVFqYml5UeUeUE/edit?pli=1>).
- . 2014. "Busting Bad Advertising Practices - 2013 Year in Review." *Google Inside AdWords*. January 17. Retrieved February 2, 2014 (<http://adwords.blogspot.com.au/2014/01/busting-bad-advertising-practices-2013.html>).
- Guthrie, Robert. 2012. "Taking the fight to intermediaries." *Anti-Counterfeiting 2012 - A Global Guide*. Retrieved October 7, 2013 (www.worldtrademarkreview.com/issues/Article.ashx?g=7efd5982-f7f4-42ad-8765-92ffc01bec31).
- IAB. 2013. "Quality Assurance Guideline, Version 2.0." *Interactive Advertising Bureau*. July 25. Retrieved September 3, 2013 (http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-072513).
- IACC. 2011. "IACC Has New Tools to Cut Off Money to Bad Sites." *International Anti-Counterfeiting Coalition*. September 27. Retrieved May 3, 2012 (<http://www.iacc.org/announcements/iacc-has-new-tools-to-cut-off-money-to-bad-sites>).
- . 2012. "IACC Announces Collaborations with Taobao and DHGate to Fight Counterfeiting." *International Anti-Counterfeiting Coalition*. Retrieved September 25, 2013 (<http://members.iacc.org/news/104807/IACC-Announces-Collaborations-With-Taobao-DHgate-to-Fight-Counterfeiting.htm>).

- . 2013. "IACC and Taobao Marketplace Sign Agreement to Combat Counterfeiting Online." International Anti-Counterfeiting Coalition. Retrieved September 25, 2013 (<http://members.iacc.org/news/136452/IACC-and-Taobao-Marketplace-Sign-Agreement-to-Combat-Counterfeiting-Online.htm>).
- . 2014, "IACC Payment Processor Initiative (RogueBlock)." Retrieved 14 January 2014 (<http://www.iacc.org/payment-processor-portal.html>).
- ICANN. 2012. ".com Registry-Registrar Agreement." Internet Corporation for Assigned Names and Numbers. Retrieved June 3, 2013 (<https://www.icann.org/resources/pages/appendix-08-2012-12-07-en>).
- . 2013. "2013 Registrar Accreditation Agreement." Internet Corporation for Assigned Names and Numbers. Retrieved November 21, 2013 (<https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>).
- IFPI. 2013. "IFPI Digital Music Report: Engine of digital world." International Federation of the Phonographic Industry. Retrieved September 4, 2012 (http://www.ifpi.org/downloads/dmr2013-full-report_english.pdf).
- NTA. 2009. "Addressing the Sale of Counterfeits on the Internet." International Trademark Association, New York City. September. Retrieved May 13, 2012 (<http://www.inta.org/Advocacy/Documents/INTA%20Best%20Practices%20for%20Addressing%20the%20Sale%20of%20Counterfeits%20on%20the%20Internet.pdf>).
- JICWEBS. 2013. "DTSG: UK Good Practice Principles for the Trading of Digital Display Advertising." Joint Industry Committee for Web Standards. Retrieved December 30, 2013 (<http://www.jicwebs.org/digital-trading-standards-group-good-practice-principles/good-practice-principles>).
- Kirkpatrick, Linda. 2012. "Rooting Out Rogue Merchants: The IACC Payment Processor Portal Mid-Year Review and Vision for the Future." Presented at the International Anti-Counterfeiting Coalition Spring Conference, 2-4 May, Washington, DC.
- Linggo, Colin T. 2012. "Rooting Out Rogue Merchants I: Online Advertising's Response to Counterfeiting." Presented at the International Anti-Counterfeiting Coalition Spring Conference, 2-4 May, Washington, DC.
- MasterCard. N.d. "MasterCard Anti-Piracy Policy." Retrieved June 9, 2013 (http://www.mastercard.com/us/wce/PDF/MasterCard_Anti-Piracy_Policy.pdf).
- MasterCard. 2013. "Security Rules and Procedures – Merchant Edition." MasterCard Worldwide. February 22. Retrieved July 23, 2013 (http://www.mastercard.com/us/merchant/pdf/SPME-Entire_Manual_public.pdf).
- MPAA. 2013. "Understanding the Role of Search in Online Piracy." Motion Picture Association of America. September 18. Retrieved December 16, 2013 (<http://www.mpa.org/wp-content/uploads/2014/03/Understanding-the-role-of-search-in-online-piracy.pdf>).

- Montanaro, Kristina. 2012. "IACC Payment Processor Portal Program: First Year Statistical Review: Executive Summary." October 2012. Retrieved December 2012
(<http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf>).
- . 2012. "IACC Payment Processor Portal Training Workshop." Presented at the International Anti-Counterfeiting Coalition Spring Conference, 2-4 May, Washington, DC.
- Singhal, Amit. 2012. "An Update to our search algorithms." *Google Inside Search: The official Google Search blog*. October 8. Retrieved November 9, 2012
(<http://insidesearch.blogspot.com.au/2012/08/an-update-to-our-search-algorithms.html>).
- Spelich, John W. 2012. "Comments by Taobao for Special 301 Review (2012 Special 301 Review)." *TechLawJournal*. February 10. Retrieved May 5 2012
(<http://www.techlawjournal.com/topstories/2013/20130920.asp>).
- Taobao. N.d. "How to Submit an IPR Infringement Complaint." Retrieved August 9, 2013 (<http://qinquan.taobao.com/report/operation.htm>).
- Visa. 2013. "Visa International Operating Regulations." October 15. Retrieved November 9, 2013 (<https://usa.visa.com/.../visa-international-operating-regulations-main.pdf>).
- Walker, Kent. 2010. "Making Copyright Work Better Online." *Google Public Policy Blog*. December 2. Retrieved January 28, 2013
(<http://googlepublicpolicy.blogspot.com.au/2010/12/making-copyright-work-better-online.html>).

V) Media

- Alizila staff. 2013. "Taobao's Fight Against Piracy Expands." *Alizila*. August 16. Retrieved September 9, 2013 (<http://www.alizila.com/taobaos-fight-against-piracy-expands>).
- Anderson, Nate. 2010. "Senator: Web Censorship Bill a 'Bunker-Busting Cluster Bomb'." *Wired*, November 20. Retrieved March 13, 2012
(<http://www.wired.com/2010/11/senator-web-censorship-bill-a-bunker-busting-cluster-bomb/>).
- Ball, James, Julian Border, and Glenn Greenwald. 2013. "Revealed: how US and UK spy agencies defeat internet privacy and security." *The Guardian*. September 6. Retrieved September 7, 2013
(<http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>).
- Bason, Tamlin H. 2012. "IP Czar: Voluntary Industry Agreements Could be Key to Combatting IP Infringement." *Bloomberg BNA*. May 17. Retrieved September

- 18, 2012 (<http://www.bna.com/ip-czar-voluntary-industry/>).
- BBC. 2013. "UK piracy warning letters delayed until 2015." *BBC*. June 6. Retrieved August 12, 2013 (<http://www.bbc.com/news/technology-22796723>).
- Berkens, Michael. 2011. "Here Is GoDaddy's Statement In Support of the Stop Online Piracy Act House Hearing Tomorrow." *The Domains*. November 15. Retrieved November 25, 2013 (<http://www.thedomains.com/2011/11/15/here-is-godaddys-statement-in-support-of-the-stop-online-privacy-act-house-hearing-tomorrow/>).
- Bertram, Theo. 2013. "Follow the Money: Can the Business of Ad-Funded Piracy Be Throttled?" *Musictank.co.uk*. May 28. Retrieved May 30, 2013 (<http://www.musictank.co.uk/events/follow%20the%20money>).
- Biddle, Ellery Roberts. 2014. "Advocates Hail Brazil's 'Bill of Rights for the Internet.'" *Global Voices Advocacy*. March 26. Retrieved March 27, 2014 (<http://advocacy.globalvoicesonline.org/2014/03/26/advocates-hail-brazils-constitution-for-the-internet-marcocivil/>).
- Bradwell, Peter. 2011. "Government and private policing." *Open Rights Group Blog*. December 14, 2011. Retrieved March 1, 2012. (<https://www.openrightsgroup.org/blog/2011/private-copyright-policing-update>).
- . 2012. "The Spirit of 'Transparency' Haunts Copyright Roundtables." *Open Rights Blog*. May 3, 2012. Retrieved May 10, 2012. (<https://www.openrightsgroup.org/blog/2012/the-spirit-of-transparency-and-the-copyright-roundtables>).
- Carlson, Nicholas 2013. "A Single Chinese Company Dwarfed All of America's Black Friday and Thanksgiving Sales in One Day." *Business Insider*, December 4. Retrieved December 21, 2013 (<http://www.businessinsider.com.au/alibaba-dwarfs-americas-black-friday-2013-12>).
- Charman-Anderson, Suw 2012. "PayPal Forced into Erotica U-Turn." *Forbes*, March 14. Retrieved November 13, 2013 (<http://www.forbes.com/sites/suwcharmananderson/2012/03/14/paypal-forced-into-erotica-u-turn/>).
- Clifton, Marjorie. 2012, "The Fight to Combat Illegal Online Pharmacies", Retrieved (<http://www.biotech-now.org/health/2012/08/the-fight-to-combat-illegal-online-pharmacies#>).
- The Economist*. 2014. "Alibaba's IPO: From bazaar to bonanza." *The Economist*, May 10. Retrieved May 25, 2014. (<http://www.economist.com/news/business/21601869-chinas-e-commerce-giant-has-just-revealed-details-its-long-awaited-flotation-america-it>).
- Ellison, David. 2012. "UK advertisers grasping nettle of online brand protection " *News ISBA: The Voice of British Advertisers*. August 9. Retrieved June 15, 2013 (<http://isba.org.uk/news/2013/08/09/uk-advertisers-grasping-nettle-of-online-brand-protection>).
- eMarketer. 2013. "Mobile Pushes US Digital Ad Market Higher." *eMarketer*. August 21. Retrieved August 20, 2013 (<http://www.emarketer.com/Article/Mobile-Pushes->

[US-Digital-Ad-Market-Higher/1010149](#)).

- Enigmax. 2013. "PayPal Demands Invites to Private BitTorrent Trackers." *TorrentFreak*, January 8, 2013. Retrieved January 13, 2013 (<https://torrentfreak.com/paypal-demands-invites-to-private-bittorrent-trackers-130108/>).
- Erickson, Jim. 2011. "Alibaba.com Unveils New Anti-fraud Plan." *Alizila*. May 12. Retrieved May 20, 2011 (<http://www.alizila.com/alibabacom-unveils-new-anti-fraud-plan>).
- . 2012. "U.S. Removes Taobao from "Notorious" List of Pirate Markets." *Alizila*. December 14. Retrieved October 26, 2013 (<http://www.alizila.com/us-removes-taobao-notorious-list-pirate-markets>).
- . 2012a. "Taobao Marketplace to Name and Shame Shady Online Merchants." *Alizila*. March 8. Retrieved July 11, 2012 (<http://www.alizila.com/taobao-marketplace-name-and-shame-shady-online-merchants>).
- Ernesto. 2011. "BitTorrent.com and Archive.org Blacklisted as Pirate Sites by Major Advertiser" *TorrentFreak*, June 10. Retrieved June 14, 2011 (<https://torrentfreak.com/bittorrent-com-and-archive-org-blacklisted-as-pirate-sites-110610/>).
- . 2012. "PayPal Bans BitTorrent Friendly VPN Provider." *TorrentFreak*. June 22. Retrieved March 2, 2013 (<https://torrentfreak.com/paypal-bans-bittorrent-friendly-vpn-provider-120622/>).
- . 2013. "Google Refuses to Delete Pirate Websites from its Search Results." *TorrentFreak*. July 12. Retrieved July 22, 2013 (<https://torrentfreak.com/google-refuses-to-delete-pirate-websites-from-its-search-results-130712/>).
- . 2014. "UK Police Launch Pirate Site Blacklist for Advertisers." *TorrentFreak*. March 31. Retrieved April 10, 2014 (<https://torrentfreak.com/city-of-london-police-launches-pirate-site-blacklist-for-advertisers-140331/>).
- . 2014a. "Google Asked to Remove 100 Million Pirate Search Results in 2014." *TorrentFreak*. May 5. Retrieved May 15, 2014 (<http://torrentfreak.com/google-asked-remove-100-million-pirate-search-results-140505/>).
- Efrati, Amir. 2013. "In Online Ads, There's Google—and Then Everybody Else." *The Wall Street Journal*. July 13. Retrieved July 24, 2013 (<http://blogs.wsj.com/digits/2013/06/13/in-online-ads-theres-google-and-then-everybody-else/>).
- Fae, Jane. 2014. The internet censorship programme that you're not allowed to know about. *Politics.co.uk*. March 27. Retrieved March 28, 2014 (<http://www.politics.co.uk/comment-analysis/2014/03/27/the-internet-censorship-programme-you-re-not-allowed-to-know>).
- Firth, James. 2011. "Live tweets from Ed Vaizey round table on content protection and web blocking." *SROC: Slightly Right of Centre*. December 7, 2011. Retrieved November 13, 2013 (<http://www.sroc.eu/2011/12/live-tweets-from-ed-vaizey-round-table.html>).

- Forbes*. 2013. "Why American Express is Growing its Third Party Issued Cards Business." *Forbes*, March 1. Retrieved March 24, 2013 (<http://www.forbes.com/sites/greatspeculations/2013/03/01/why-american-express-is-growing-its-third-party-issued-cards-business/>).
- Forbes*. 2013. "Fortune 500", Retrieved March 13, 2013 (<http://money.cnn.com/magazines/fortune/fortune500/>).
- Franzen, Carl 2012. "How the Web Killed SOPA and PIPA." *Talking Points Memo*, January 20. Retrieved January 20, 2012 (<http://talkingpointsmemo.com/idealab/how-the-web-killed-sopa-and-pipa>).
- Gabbatt, Adam. 2014. "Protesters rally for 'the day we fight back' against mass surveillance." *The Guardian*. February 11. Retrieved February 15, 2014 (<http://www.theguardian.com/world/2014/feb/11/day-fight-back-protest-nsa-mass-surveillance>).
- Glanz, James and Andrew W. Lehren. 2013. "N.S.A. Spied on Allies, Aid Groups and Businesses." *The New York Times*. December 20. Retrieved December 22, 2013 (<http://www.nytimes.com/2013/12/21/world/nsa-dragnet-included-allies-aid-groups-and-business-elite.html>).
- Goldman, Eric. 2009. "Making Sense of the \$32M Contributory Trademark Infringement Judgment Against a Web Host-Louis Vuitton v. Akanoc." in *Technology & Marketing Law Blog*. September 18, 2009. Retrieved January 12, 2013 (http://blog.ericgoldman.org/archives/2009/09/making_sense_of.htm).
- . 2012. "Celebrating (?) the Six-Month Anniversary of SOPA's Demise." *Forbes*. July 18. Retrieved July 18, 2012 (<http://www.forbes.com/sites/ericgoldman/2012/07/18/celebrating-the-six-month-anniversary-of-sopas-demise/>).
- Goodwin, Danny. 2014. "Google, Bing Gain Search Share to End 2013." *Search Engine Watch*. January 16. Retrieved March 12, 2013 (<http://searchenginewatch.com/article/2323499/Google-Bing-Gain-Search-Share-to-End-2013>).
- Greenwald, Glenn and Ewen MacAskill. 2013. "NSA Prism program taps in to user data of Apple, Google and others." *The Guardian*. June 7. Retrieved June 23, 2013 (<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>).
- Guglielmo, Connie 2013. "Apple's Supplier Labor Practices In China Scrutinized After Foxconn, Pegatron Reviews." *Forbes*. December 12. Retrieved February 3, 2014. (<http://www.forbes.com/sites/connieguglielmo/2013/12/12/apples-labor-practices-in-china-scrutinized-after-foxconn-pegatron-reviewed/>)
- Hamburger, Tom and Matea Gold. 2013. "Google, once disdainful of lobbying, now a master of Washington influence." *The Washington Post*. April 13. Retrieved March 13, 2014 (http://www.washingtonpost.com/politics/how-google-is-transforming-power-and-politicsgoogle-once-disdainful-of-lobbying-now-a-master-of-washington-influence/2014/04/12/51648b92-b4d3-11e3-8cb6-284052554d74_story.html).

- Healey, Jon. 2013. "A non-SOPA broadside aimed at online piracy hotbeds." in *Daily Press*. July 15. Retrieved August 23, 2013 (<http://www.dailypress.com/topic/la-ol-online-advertising-movie-music-piracy-20130715,0,6652526.story>).
- Humphries, Fred. 2013. "Microsoft applauds release of Best Practice Guidelines for Ad Networks to Address Piracy and Counterfeiting." *Microsoft on the Issues*. July 15, 2013. Retrieved January 11, 2014 (http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/07/15/microsoft-applauds-release-of-best-practice-guidelines-for-ad-networks-to-address-piracy-and-counterfeiting.aspx).
- Interbrand. 2013. Interbrand Best Global Brands 2013. Retrieved March 7, 2014 (<http://www.interbrand.com/en/>).
- Jabour, Bridie and Martin Pengelly. 2014. "Australia spied on Indonesia talks with US law firm in 2013." *The Guardian*. February 16. Retrieved February 16, 2013 (<http://www.theguardian.com/world/2014/feb/16/australia-spied-indonesia-talks-us-firm>).
- Jackson, Eric. 2012. "The US Government Just Gave Alibaba The Green Lights to IPO, Helping Yahoo." *Forbes*. December 14. Retrieved April 2, 2014 (<http://www.forbes.com/sites/ericjackson/2012/12/14/the-us-government-just-gave-alibaba-the-green-light-to-ipo-helping-yahoo/>).
- 2014. "How Much Could Alipay Add to the Value of Alibaba IPO?" *Forbes*, May 5. Retrieved May 10, 2014 (<http://www.forbes.com/sites/ericjackson/2014/05/05/how-much-could-alipay-add-to-the-value-of-alibaba-ipo/>).
- Karaganis, Joe. 2012. "Meganomics: The Future of "Follow-the-Money" Copyright Enforcement." *Torrent Freak*. January 24. Retrieved February 13, 2014 (<https://torrentfreak.com/meganomics-the-future-of-follow-the-money-copyright-enforcement-120124/>).
- Kharif, Olga. 2013. "Go Daddy CEO Mulls 2014 IPO, Joining Wave of Cloud Deals." *Bloomberg*. July 26. Retrieved September 9, 2013 (<http://www.bloomberg.com/news/2013-07-24/go-daddy-ceo-mulls-2014-ipo-joining-wave-of-cloud-deals.html>).
- Kirsner, Scott 2003. "How eBay Fights Fraud." *Fast Company*. July 2. Retrieved December 13, 2011 (<http://www.fastcompany.com/46858/how-ebay-fights-fraud>).
- Lee, Mark. 2012. "Alibaba Hires Ex-U.S. Official to Aid Washington Lobbying." *Bloomberg*. April 17. Retrieved June 19, 2013 (<http://www.bloomberg.com/news/2012-04-17/alibaba-hires-ex-u-s-official-to-aid-washington-lobbying.html>).
- Levy, Steven 2014. "How the NSA Almost Killed the Internet." *Wired*, January 7. Retrieved February 12, 2014 (<http://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/>).

- Masnick, Mike. 2011. "Class Action Lawsuit Filed Against Coach Over Bogus Takedowns, Trademark Bullying." *Techdirt*. February 14. Retrieved August 8, 2012 (<http://www.techdirt.com/articles/20110211/21555413069/class-action-lawsuit-filed-against-coach-over-bogus-takedowns-trademark-bullying.shtml>).
- Masnick, Mike. 2014. "White House Withholds Details of its Role in 'Voluntary' Agreement Between Payment Processors and Copyright Industries." *TechDirt*. February 21. Retrieved February 23, 2014 (<https://www.techdirt.com/articles/20140220/16152426303/white-house-withholds-details-its-role-voluntary-agreement-between-payment-processors-copyright-industries.shtml>).
- McCullagh, Declan. 2012. "Protect IP, SOPA protests knock senate websites offline." *c/net*, January 19. Retrieved January 20, 2012 (<http://www.cnet.com/au/news/protect-ip-sopa-protests-knock-senate-web-sites-offline/>).
- McIntyre, T.J. 2010. "Home Office terrorist material report site – some thoughts." *IT Law in Ireland*. February 9. Retrieved November 2, 2013 (<http://www.tjmcintyre.com/2010/02/home-office-terrorist-material.html>).
- Miller, Claire Cain. 2014. "Revelations of N.S.A. Spying Cost U.S. Tech Companies." *The New York Times*. March 21. Retrieved March 23, 2014 (<http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html>).
- Millward, Steven. 2013. "By 2016, China Will Have 423 Million E-Commerce Shoppers Spending \$457 Billion." *TechInAsia*. February 12. Retrieved July 21, 2013 (<http://www.techinasia.com/china-ecommerce-shoppers-in-2016/>).
- . 2013a. "China's 'Cyber Monday' ends with \$5.7 billion spent in 24 hours on Alibaba's e-stores." *TechInAsia*. November 12. Retrieved February 2, 2014 (<http://www.techinasia.com/china-online-sales-shopfest-sees-alibaba-tmall-sales-nearly-6-billion-dollars/>).
- Mitchell, Russ. 2010. "As a CEO, Meg Whitman has had her ups and downs." *The Bay Citizen*. July 5. Retrieved August 15, 2013 (<https://groups.yahoo.com/neo/groups/QueerCaliforniaState/conversations/topics/855>).
- Moncau, Luiz Fernando and Pedro Nicoletti Mizukami. 2014. "Brazilian Chamber of Deputies Approves Marco Civil Bill." *InfoJustice.org*. March 25. Retrieved March 27, 2014 (<http://infojustice.org/archives/32527>).
- Netburn, Deborah. 2014. "Google says 4.5 million people signed its anti-SOPA petition today." *Los Angeles Times*. January 18. Retrieved January 20, 2012 (<http://latimesblogs.latimes.com/technology/2012/01/google-anti-sopa-petition.html>).
- Newswire, PR. 2013. "LegitScript Shuts Down 6,700 Rogue Internet Pharmacies." PR Newswire. June 28. Retrieved July 5, 2013 (<http://www.prnewswire.com/news-releases/legitscript-shuts-down-6700-rogue-internet-pharmacies->

[213544321.html](#)).

Newsire, PR. 2007. "Microsoft, Google, & Yahoo! Pay Millions to U.S. for Their Past Promotion of Illegal Gambling." PR Newsire. December 19. Retrieved July 3, 2013 (<http://www.prnewswire.com/news-releases/microsoft-google--yahoo-pay-millions-to-us-for-their-past-promotion-of-illegal-gambling-58808842.html>).

Owles, Eric. 2014. "5 Questions for Alibaba's I.P.O." *The New York Times*. May 9. Retrieved May 11, 2014 (<http://dealbook.nytimes.com/2014/05/09/weekend-reading-5-questions-for-alibabas-i-p-o/>)

Perlroth, Nicole, Jeff Larson, and Scott Shane. 2013. "N.S.A Able to Foil Basic Safeguards of Privacy." *The New York Times*. September 5. Retrieved October 3, 2013 (<http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all>).

Policy Team, Access. 2014. "A bill of internet rights for Brazil." *Access*. March 26. Retrieved March 29, 2014 (<https://www.accessnow.org/blog/2014/03/26/a-bill-of-internet-rights-for-brazil>).

PR Newswire. 2007, "Microsoft, Google, & Yahoo! Pay Millions to U.S. for Their Past Promotion of Illegal Gambling." PR Newswire. December 19. Retrieved February 15, 2013 (<http://www.prnewswire.com/news-releases/microsoft-google--yahoo-pay-millions-to-us-for-their-past-promotion-of-illegal-gambling-58808842.html>).

—. 2013, "LegitScript Shuts Down 6,700 Rogue Internet Pharmacies", June 28. Retrieved August 28, 2013 (<http://www.prnewswire.com/news-releases/legitscript-shuts-down-6700-rogue-internet-pharmacies-213544321.html>

Reuters. 2014. "Brazilian Congress Passes Internet Bill of Rights." *The New York Times*. April 22. Retrieved April 29, 2014 (http://www.nytimes.com/reuters/2014/04/22/technology/22reuters-internet-brazil.html?partner=rss&emc=rss&_r=0).

RogueFinder. 2012. "Study of Rogue Websites Selling Counterfeit Goods." Gioconda Law Group. May 15. Retrieved June 23, 2012 (<http://roguefinder.com/wp-content/uploads/2012/05/RogueFinder-Study.pdf>).

Rothenberg, Randall. 2011. "Letter to the Congressional International Anti-Piracy Caucus." November 1. Retrieved August 22, 2013 (<http://www.iab.net/media/file/Rothenberg-Reply-to-CAPC.pdf>).

Samuels, Julie and Mitch Stoltz. 2012. "Google's Opaque New Policy Lets Rightsholders Dictate Search Results." Electronic Frontier Foundation. August 10. Retrieved 30 March 2013 (<https://www.eff.org/deeplinks/2012/08/googles-opaque-new-policy-lets-rightsholders-dictate-search-results>).

Sandoval, Greg. 2011. "Lawmakers ask advertisers for Web-piracy crackdown." *C/net*. October 11. Retrieved December 2, 2012 (<http://www.cnet.com/au/news/lawmakers-ask-advertisers-for-web-piracy-crackdown/>).

- Schneier, Bruce. 2013. "Surveillance as a Business Model." *Schneier on Security*. November 25. Retrieved February 23, 2014 (https://www.schneier.com/blog/archives/2013/11/surveillance_as_1.html).
- 2014. "Don't Listen to Google and Facebook: The Public-Private Surveillance Partnership is Still Going Strong." *The Atlantic*, March 25. Retrieved April 2, 2014 (<http://m.theatlantic.com/technology/archive/2014/03/don-t-listen-to-google-and-facebook-the-public-private-surveillance-partnership-is-still-going-strong/284612/>).
- Stuart, Keith. 2013. "Xbox One DRM restrictions dropped after gamer outcry." *The Guardian*. June 20. Retrieved February 17, 2014 (<http://www.theguardian.com/technology/2013/jun/19/xbox-one-drm-second-hand-restrictions-abandoned>).
- Su, Sail. 2014. "China Search Engine Market Update for Q4 2013." *China Internet Watch*. March 11. Retrieved April 3, 2014 (<http://www.chinainternetwatch.com/6527/china-search-engine-market-update-q4-2013/>).
- Suchman, Evan. 2013. "New stats have Visa almost cornering the debit market, with a 72.7 percent marketshare." *FierceRetail*. April 1. Retrieved May 9, 2013 (<http://www.fierceretail.com/story/new-stats-have-visa-almost-cornering-debit-market-727-percent-marketshare/2013-04-01>).
- Tabuchi, Hiroko. 2014. "Alibaba to acquire Chinese Mapping Firm as Buying Spree Continues." *The New York Times*. April 11. Retrieved April 18, 2014 (http://dealbook.nytimes.com/2014/04/11/alibaba-continuing-buying-spree-to-acquire-chinese-mapping-firm/?_php=true&_type=blogs&ref=technology&_r=0).
- Thompson, Derek 2010. "Google's CEO: 'The Laws Are Written by Lobbyists'." *The Atlantic*, October 1. Retrieved November 6, 2013 (<http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/>).
- Timm, Trevor. 2012, "How PIPA and SOPA Violate White House Principles Supporting Free Speech and Innovation." January 16. Retrieved March 13, 2013 (<https://www.eff.org/deeplinks/2012/01/how-pipa-and-sopa-violate-white-house-principles-supporting-free-speech>).
- Wang, Helen H. 2010. "How eBay Failed in China." *Forbes*, September 12. Retrieved June 2, 2013 (<http://www.forbes.com/sites/china/2010/09/12/how-ebay-failed-in-china/>).
- WPP. 2013. "Global internet ad spend hit \$99bn in 2012, almost 20% of total investment." *WPP*. March 27. Retrieved July 12, 2013 (<http://www.wpp.com/wpp/press/2013/mar/27/global-internet-ad-spend-hit-99bn-in-2012/>).

Appendix A – List of Interviews

I) United States

Bainbridge, Julie, Senior Brand Protection Manager, PayPal, 1 July 2012, interview by telephone.

Barchiesi, Bob, President, International Anti-Counterfeiting Coalition (trade association), Washington, D.C., 24 April 2012, in-person interview.

Brand-protection manager, U.S. apparel company (rights holder), 31 May 2012, interview by Skype.

Brenner, Brett, Electrical Safety Foundation International (trade association), Arlington, VA, 24 April 2012, in-person interview.

Brokate, Brian, Partner, Gibney Anthony & Flaherty (law firm), New York City, 30 March 2012, in-person interview.

Courtney, Kurt, Director, Government Relations, American Apparel and Footwear Association (trade association), Washington, DC, 30 April 2012, in-person interview.

Elings, Roxanne, Co-Chair, Global Trademarks/Brand Management Practice, Greenberg Traurig LLP (law firm), New York City, 20 March, 2012, in-person interview.

Evert-Burks, Leah, Director of Brand Protection, Deckers Outdoor Corporation (rights holder), 12 June 2012, interview by Skype.

Faulconer, David, Consultant, TeleSolv Consulting, LLC (investigative firm), Washington, DC, 27 April 2012, in-person interview.

Feinberg, Eric, Owner, Fans Against Kounterfeit Enterprise (brand-monitoring firm), 2 August 2012, interview by Skype.

Flynn, Sean, Associate Director, Program on Information Justice and Intellectual Property (non-governmental organisation), Washington, DC, 14 May 2012, in-person interview.

Forgione, Joseph, Director of Trademark Enforcement, Gioconda Law Group (law firm), New York City, 3 April 2012, in-person interview.

Gaines, Rudy Manager, Marksmen (investigative firm), 19 April 2012, interview by Skype.

Garner, Tracy, Anti-Counterfeiting & Unauthorised Distribution, Schneider Electric (rights holder), 9 May 2012, interview by Skype.

Gioconda, Joseph, Founder, Gioconda Law Group & Founder, RogueFinder LLC (law firm), New York City, 22 August 2012, interview by Skype.

Global Head of Security, Pharmaceutical company (rights holder), 27 March 2012, interview by Skype.

Government official, Senior Policy Advisor, Office of the U.S. Intellectual Property Enforcement Coordinator, Washington, DC, 18 May 2012, in-person interview.

Government official, National Intellectual Property Rights Coordination Centre, Arlington, VA, 16 May 2012, in-person interview.

Holmes, Rob, Owner and CEO, IPCybercrime (investigative firm), Texas, 2 May 2012, in-person interview (in Washington, DC).

Investigative firm, California, 19 April 2012, interview by Skype.

Investigative firm, Georgia, 23 April 2012, interview by Skype.

Jamar, Steven D., Associate Director, Institute for Intellectual Property and Social Justice (non-governmental organisation), Washington, DC, 26 April 2012, in-person interview.

Karaganis, Joe, Vice-President, The American Assembly (non-governmental organisation), New York City, 28 March 2012, in-person interview.

Kubic, Tom, CEO, Pharmaceutical Security Institute (trade association), Arlington, VA, 10 May 2012, in-person interview.

Lawyer, Hong Kong Law Firm, Washington, DC, 7 May 2012, in-person interview.

Li, Candice, External Relations Manager, Anti-counterfeiting, International Trademark Association (trade association), New York City, 3 April 2012, in-person interview.

Loaiza, Mario, Owner, Mario Loaiza & Associates Inc. (investigative firm), 16 July 2012, interview by Skype.

Love, Andrew, Brand Security, Global Investigations, Legal Enforcement, Specialised Bicycles (rights holder), US, 24 August 2012, interview by Skype.

Montanaro, Kristina, Associate Counsel, Director Special Programs, International Anti-Counterfeiting Coalition (trade association), 24 April 2012, Washington, D.C., in-person interview.

Rogan, Lisa, Director of Trademarks & Brand Protection, Acushnet and coordinator of U.S. Golf Manufacturers' Anti-Counterfeiting Working Group (rights holder), Washington, DC, 2 May 2012, in-person interview.

Senior Policy Advisor, Office of the Intellectual Property Enforcement Coordinator, Executive Office of the President, Washington, DC, 18 May 2012, in-person interview.

Silcox, Clark, Counsel, National Electrical Manufacturers' Association (trade association), Arlington, VA, 13 April 2012, in-person interview.

Siy, Sherwin, Deputy Legal Director, Public Knowledge (non-governmental organisation), Washington, DC, 11 May 2012, in-person interview.

Sohn, David, General Counsel, Centre for Democracy and Technology (non-governmental organisation), Washington, DC, 15 May 2012, in-person interview.

Smith, Te, Vice President, Communications, MarkMonitor (brand-monitoring firm), 6 April 2012, interview by Skype.

Tarbutton, Tamara, Investigator, Vaudra Ltd. (investigative firm), Washington, DC, 2 May 2012, in-person interview.

Thomson, Tom, Executive Director, Coalition for Intellectual Property Rights (trade association), Washington, DC, 10 May 2012, in-person interview.

Trainer, Timothy, President, Global Intellectual Property Strategy Centre (trade association), Washington, DC, 11 April 2012, in-person interview.

Volpi, Vincent CEO, PICA Corporation (investigative firm), 25 June 2012, interview by Skype.

Walling, Daniel, Founder, LevelPlay (brand-monitoring firm), 14 August 2012, interview by Skype.

Weinstein, Maxim, President & Executive Director, StopBadware (non-governmental association), Cambridge, MA, 1 August 2012, interview by Skype.

Westerfield, Allen, President, Imaging Supplies Coalition for International Intellectual Property Protection Inc. (trade association), 10 July 2012, interview by Skype.

Zewers, Kirsten, Government Relations, Counsel, Intellectual Property Owners Association (trade association), Washington, DC, 23 April 2012, in-person interview.

Australia

Arnold, Phill, Director, Counterfeiting Intelligence Services, Brisbane, 2 May 2012, in-person interview (in Washington, DC).

Australian Customs, Canberra, 23 February 2012, in-person interview.

Australian Federal Police, Canberra, 23 January 2012, in-person interview.

Bosland, Jason, Senior Lecturer, Intellectual Property Research Institute of Australia (non-governmental organisation), Melbourne, 31 January 2012, in-person interview.

Douglas, Craig, Owner, Nationwide Research Group, Melbourne (investigative firm), 1 February 2012, in-person interview.

Gamble, Ken, CEO, Gamble Investigations International (investigative firm), Sydney, 5 December 2011, in-person interview.

Hutley, Vanessa, Music Industry Piracy Investigations (trade association), Sydney, 16 December 2011, by email.

Kitschke, Brad, Executive Director, Australian Sporting Goods Association (trade association), Melbourne, 2 February 2012, in-person interview.

Managing Director, Investigative firm, Australia, 8 November 2011, in-person interview.

Manders, Karl CEO, Continental Enterprises Inc. (investigative firm), 9 May 2012, interview by Skype.

Robson, Julie, Investigator, Victorian Detective Service, Melbourne, 6 February 2012, in-person interview.

Rumore, Michael, Owner, Rumore Investigations, Sydney, (investigative firm), 30 November 2012, in-person interview.

Stern, Stephen, Partner, Corrs, Chambers and Westgarth (law firm), Sydney, 1 February 2012, in-person interview.

United Kingdom

Baker, Steve, Co-Owner, Intellectual Property Management Services (investigative firm), UK, 9 September 2012, in-person interview.

Croker, Damian, CEO, BrandStrike Limited (brand-monitoring firm), London, UK, 25 September 2012, in-person interview.

Croxon, Siân Partner, DLA Piper (law firm), London, UK, 14 September 2012, in-person interview.

Cumming, Robert, Solicitor, Walker Morris (law firm), UK, 21 September 2012, interview by Skype.

Government official, National Intellectual Property Rights Coordination Centre, 16 May 2012, Arlington, VA, in-person interview.

Government official, Homeland Security Investigations, U.S. Embassy, London, UK, 4 October 2012, in-person interview.

Gray, Alastair, Head of London Cerberus Investigations (investigative firm), London, UK, 4 September 2012, in-person interview.

Guthrie, Robert, Associate, SJ Berwin (law firm), 5 October 2012, London, UK, in-person interview.

Harrison, Clive, Export Sales & Brand Protection Manager, Acushnet Europe (rights holder), 2 October 2012, interview by Skype.

Hyde-Blake, Gavin, Director of Research and Investigation (investigative firm), Eccora, London, UK, 19 September 2012, in-person interview.

Investigations manager, computer technology firm (rights holder), 9 October 2012, interview by Skype.

Investigative firm, UK, 14 May 2012, interview by Skype.

Kotecha, Amit, Senior Mobile & Networks Manager, Internet Advertising Bureau (trade association), London, UK, 8 October 2012, in-person interview.

Mee, Duncan, Co-owner, Cerberus Investigations (investigative firm), London, UK, 4 September 2012, in-person interview.

Newman, Jeremy, Partner, Rouse Legal (law firm), London, UK, 10 September 2012, in-person interview.

Orchard, Ruth, Director, Anti-Counterfeiting Group (trade association), England, 17 September 2012, by Skype.

Ramm, James, Director, Commercial Security International (investigative firm), London, UK, 10 October 2012, in-person interview.

Robinson, Graham, Managing Director, Farncombe International (investigative firm), London, UK, 28 September 2012, in-person interview.

Sharp, Kieron, Director General, Federation Against Copyright Theft (trade association), UK, 9 October 2012, by Skype.

Simmons, Adrian, Managing Director, Total Brand Security (brand-monitoring firm), London, UK, 21 September 2012, in-person interview.

Smith, Keith, Deputy Director, British Electrotechnical Allied Manufacturing Association (trade association), London, UK, 3 September 2012, in-person interview.

Starr, Ian, Partner, D Young & Co. (law firm), London, UK, 7 September 2012, in-person interview.

Waring, Tim, Director, Intelligence Technologies (brand-monitoring firm), UK, 3 October 2012, interview by Skype.

Watson, Allan, Director, Global Operations, Gamble Investigations International (investigative firm), London, UK, 12 September 2012, in-person interview.

Whitelaw, Valerie, President, Imaging Consumables Coalition Europe, 17 September 2012, interview by Skype.

Winter, Susie, Director General, Alliance for Intellectual Property (trade association), London, UK, 12 September 2012, in-person interview.

Wishart, Det./Supt. Bob, Head of National Operational Delivery, Regional Fraud Project, City of London Police, London, UK, 6 September 2012, in-person interview.

Wood, David, Director of Anti-Piracy, British Recorded Music Industry (BPI) Ltd. (trade association), London, UK, 12 September 2012, London, in-person interview.

Canada

Elliott, Barry, Criminal Intelligence Analytical Unit, Canadian Anti-Fraud Centre, North Bay, Ontario, 27 June 2012, interview by telephone.

Hunter, Beau, President, Global Intellectual Property Securities (investigative firm), 4 April 2012, interview by Skype.

Lipkus, Lorne, Partner, Kestenberg, Siegal, Lipkus LLP Toronto, (law firm) 1 May 2012, in-person interview (in Washington, DC).

Lipkus, David, Associate, Kestenberg, Siegal, Lipkus LLP Toronto, (law firm) 10 August 2012, in-person interview.

Representative from Nipissing University, North Bay, Ontario, 12 July 2012, interview by telephone.

Spreekmeester, Kevin, Vice President, Global Marketing, Canada Goose (rights holder), 9 August 2012, interview by Skype.

Appendix B

BEST PRACTICES TO ADDRESS COPYRIGHT INFRINGEMENT AND THE SALE OF COUNTERFEIT PRODUCTS ON THE INTERNET

Payment System Operators will voluntarily maintain clear and transparent procedures as set out below to address sales of Copyright-Infringing Products and Counterfeit Trademark Products over the Internet in which the payments with respect to such sales are processed or facilitated using the services provided by a Payment System Operator. These procedures are intended to reflect best practices and supplement, not replace, independent actions taken by Right-Holders to enforce their intellectual property rights.

- 1) Each Payment System Operator will maintain the following policies and procedures:
 - a) maintain a clearly identifiable complaint mechanism for Right-Holders on a website and post policies prohibiting the sale of Illegitimate Products using the Payment System Operator services; and
 - b) maintain one or more points of contact for receiving Requests from Right-Holders posted on the Payment System Operator's website.
- 2) The points of contact for Right-Holder Requests for each Payment System Operator are as follows:
 - a) **American Express:** antipiracy@aexp.com
 - b) **Discover:** RiskOperations@discover.com
 - c) **MasterCard:** ipinquiries@mastercard.com
 - d) **PayPal:** https://cms.paypal.com/us/cgi-bin/?&cmd=_render-content&content_ID=ua/InfringementRpt_full&locale.x=en_US
 - e) **Visa:** visa.com/ReportBrandAbuse
- 3) Each Payment System Operator requires that the Right-Holder provide the following (collectively, the "Request"):
 - a) a description of the alleged infringement, including the identity of the site allegedly engaged in the sale of Illegitimate Products and evidence proving the allegation. If only certain items on a website are alleged to be Illegitimate Products, the Request must clearly identify those specific products and their location on the website;
 - b) evidence that the Illegitimate Products could be purchased using a Payment System Operator's services, for example, by providing a screenshot of the Payment System Operator's logo appearing on the merchant website. Test transactions are helpful, but not required to submit a complete Request;

- c) a copy of the Right-Holder's cease & desist letter or DMCA notice notifying the website operator that it is engaging in infringing activity, or an attestation that, to the best of the Right-Holder's knowledge, the site is not licensed or otherwise authorized to sell the alleged Illegitimate Products in question;
 - d) evidence demonstrating that the Right-Holder owns a copyright or trademark in question; and
 - e) prompt responses to communications from Payment System Operators for additional information.
- 4) Upon receiving a Request in a Four-Party System, the Payment System Operator shall identify the acquiring entity in the system and transmit the Request to the appropriate acquiring entity with a request to conduct a prompt investigation. As part of that investigation, the merchant may provide written evidence that it has the right to legitimately sell the product in question. The Payment System Operator shall report the results of its investigation to the Right-Holder or shall require the acquiring entity to report the results of its investigation to the Right-Holder directly with a copy to the Payment System Operator. The Payment System Operator or acquiring entity will endeavor to provide an initial response to the Right-Holder in a reasonably expedient manner given the facts and circumstances of the investigation.
- 5) The Right-Holder may make further inquiries with the Payment System Operator directly if the acquiring entity does not address the Right-Holder's concern to its satisfaction.
- 6) Upon receiving a Request in a Three-Party System or the PayPal system, the Payment System Operator shall itself conduct the investigation and report the results of the investigation to the Right-Holder. As part of that investigation, the merchant may provide written evidence that it has the right to legitimately sell the product in question.
- 7) If the merchant fails to provide credible evidence as determined by the Payment System Operator or acquiring entity supportive of the merchant's position that it is not engaged in illegal conduct, or if the investigation by the acquiring entity (in a Four Party System) or the Payment System Operator (in a Three Party System or the PayPal system) determines in its reasonable opinion that the merchant is engaged in sales of Illegitimate Products, such acquiring entity or the Payment System Operator shall demand that the merchant prevent future improper transactions.
- 8) If the merchant persists in intentionally selling Illegitimate Products, the acquirer (in a Four-Party System) or Payment System Operator (in a Three-Party System) shall suspend or terminate payment services to that merchant with United States account holders. Other appropriate remedies may also be imposed if a merchant fails to respond in a timely manner or if a merchant fails to take appropriate action based on a valid complaint.

- 9) If an acquiring entity (in a Four-Party System) fails to follow the aforementioned procedures, the relevant Payment System Operator shall take appropriate remedial measures, which may include the imposition of fines and other disciplinary action, with respect to the acquiring entity terminating the merchant's access to the system.
- 10) Payment System Operators shall have a process in place to allow for prompt review of remedial measures imposed if the merchant in a Three-Party System or, a merchant or acquiring entity in a Four-Party System, disputes the allegations of infringement.
- 11) A Payment System Operator may request a written agreement by the Right-Holder to support the Payment System Operator fully in connection with a dispute where, in the Payment System Operator's reasonable opinion, the merchant provides credible evidence supportive of the merchant's position that it is not engaged in illegal conduct, including by defending, holding harmless and indemnifying the Payment System Operator for any costs, expenses (including legal fees) or liabilities arising in connection with such dispute.
- 12) Definitions:
 - a) A "Right-Holder" is a natural or legal person, or entity, having the legal standing and authority to assert a copyright or trademark right.
 - b) A "Payment System Operator" is an operator of payment networks or systems that process or facilitate payments for purchases of products over the Internet through the use of payment products such as credit cards, debit cards, or prepaid cards, or other methods of payment, and includes American Express, Discover, MasterCard, PayPal, and Visa.
 - c) A "Three-Party System" is a Payment System in which the company operating the network interfaces directly with merchants and cardholders, in addition to processing transactions, issuing cards and enlisting merchants to accept those cards.
 - d) PayPal is a system in which buyers and sellers establish accounts directly with PayPal and can utilize credit cards, bank accounts, or PayPal balances to send and receive payments.
 - e) "Four-Party System" is a Payment System in which issuing and acquiring entities have direct relationships with cardholders and merchants, respectively, and where the company operating the payment network provides services to the entities to process payment transactions. In a Four-Party System, the acquiring entities directly enroll merchants into programs that accept payment cards in exchange for products and services, and the issuing banks issue payment cards. The Payment System Operator in a Four-Party System does not hold merchant accounts, issue payment cards, or issue credit.

- f) "Illegitimate Products" includes Copyright-Infringing Products and Counterfeit Trademark Products sold over with Internet.
 - i) "Counterfeit Trademark Products" shall mean any products, including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such products, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the Right Holder of the trademark in question under the laws of the United States.
 - ii) "Copyright-Infringing Products" shall mean any products which are copies made without the consent of the Right Holder or person duly authorized by the Right Holder and which are made directly or indirectly from an article where the making of that copy would have constituted an infringement of a copyright or a related right under the laws of the United States.
- g) "Request" means a request by a Right-Holder to investigate Illegitimate Products in accordance with paragraph (3) above.

13) The policies and procedures of any individual Payment System Operator may vary in order to ensure that the most reasonable and effective mechanisms are put in place to prevent the sale of the Illegitimate Products utilizing their services, and based on the unique aspects and experience of each Payment System Operator, developments in technology, and further consultation with Right-Holders. It is the responsibility of each Payment System Operator to establish its own merchant acquisition policies and procedures appropriate to its respective business models, risk assessments, internal policies, and/or regulatory oversight.

These best practices are voluntary and not legally binding. Nothing herein shall impute knowledge, create or impose liability, rights, obligations or waiver of any rights or obligations for any parties. These best practices shall not replace, modify or interpret existing law or legal framework including without limitation defenses or limitations on liability. This document is not to be used in any way in any legal proceedings.

Appendix C

Best Practices for Rights-holders with Payment Processors

Good Faith. Any claim put forward by a rights-holders, their agents or associations will be made with a good faith belief in the accuracy and completeness of the details contained in the claim.

Notice Consolidation and Designated Points of Contact. Rights-holders who are active members of a participating association (hereinafter “channeling associations”), will channel all complaints through such association, unless not reasonably practicable, for example, if the activity complained of is not reasonably related to the competency of the trade association, if the rights-holder has a good-faith belief that direct notification is necessary due to the urgency of the circumstances, if there is a conflict of interest, or a prohibitive contractual obligation exists. Each channeling association shall endeavor to consolidate such claims made by its members prior to submission to the payment processors. Rights-holders and any channeling association engaged by one or more rights-holder shall also furnish a designated point of contact charged with responding expeditiously to inquiries from such channeling associations and/ or the payment processors.

Additional information requested by the payment processor. Channeling associations and/or rights-holders will respond expeditiously to reasonable requests for additional information that are made by a payment processor in connection with a claim or, within five business days of receiving the request, will explain the delay in providing the additional information. If in a particular case a payment processor identifies a specific need for additional information not appearing in the mutually agreed-upon standardized form described below, the channeling association or rights-holder will respond within a reasonable time period, either with the requested information or an explanation as to why the information requested is not reasonable.

Standardized Form. Channeling associations will develop and utilize a common form or system for notifying a payment processor about the use of its financial network to process transactions for activities that violate US intellectual property laws, including without limitation unauthorized sales, access to performances of, or distributions of its’ rights-holders’ intellectual property. Channeling associations will consult with rights-holders and payment processors as needed in developing such form or system.

Standardized Coding of Infringement Types. Active channeling associations will collaborate to develop a standardized coding for various infringement types (e.g., unauthorized copyright download, unauthorized copyright streaming, counterfeit goods, circumvention devices, etc.) to aid in categorization and response by payment processors. Channeling associations shall consult with the payment processors to develop such coding.

Concurrent Notification. Where a site accepts payment from multiple payment services, channeling associations will endeavor to provide notice of the request for investigation to multiple payment processors simultaneously so that each payment processor is aware of the pending investigation by a sister payment processor.

Training. Upon request from payment processors, channeling associations shall provide baseline training to payment processors on detecting counterfeit products or infringing works, or other related topics.

**Responsible Practices for Search Engines in Reducing Online Infringement
Proposal for a Code of Practice**

Executive Summary

Consumers rely on search engines to find and access entertainment content and they play a vital role in the UK digital economy. At present, consumers searching for digital copies of copyright entertainment content are directed overwhelmingly to illegal sites and services. This causes consumer confusion and significantly impedes the development of licensed digital entertainment markets in the UK. Search engines, as trusted intermediaries, should assist consumers in finding legal services and should not contribute to copyright infringement.

This paper proposes the introduction of a voluntary Code of Practice for search engines, overseen by Government, which would help to ensure that consumers are directed to safe and legal sources for entertainment content online and grow the UK digital economy.

In particular, it proposes that search engines should:

- assign lower rankings to sites that repeatedly make available unlicensed content in breach of copyright;
- prioritise websites that obtain certification as a licensed site under a recognised scheme;
- stop indexing websites that are subject to court orders while establishing suitable procedures to de-index substantially infringing sites;
- continue to improve the operation of the ‘notice and takedown’ system and ensure that search engines do not encourage consumers towards illegal sites via suggested searches; related searches and suggested sites; and
- ensure that they do not support illegal sites by advertising them or placing advertising on them, or profit from infringement by selling key words associated with piracy or selling mobile applications which facilitate infringement.

Introduction

The growth of the UK digital economy is presently held back by the pervasive nature of online infringement of copyright, particularly for digital entertainment content. Innovation in new digital content services is hampered by the fact that such sites have to compete against large numbers of unlicensed, free competitors, some of which have become well-known brands themselves while continuing to evade the law. Investment in original content is undermined because it is difficult to get a fair return on investment. And consumers are faced with a confusing array of legal and illegal services, and may not always know for certain which are legitimate and which are not.

Private & Confidential

Much of the illegal activity in the digital economy is facilitated and encouraged by money making rogue sites. Intermediaries, unwittingly or by willfully turning a blind eye (or in some cases, by encouraging such activity), play a key role in enabling content theft and often even profit from it. Only a comprehensive approach can address this issue.

It is recognised that rights holders must be active in licensing new digital services, supporting innovation and offering the consumer flexibility and choice as to how they access digital entertainment. It must be as simple and as affordable as possible for consumers to access legal content online and legal services must be communicated to consumers.

However, it is also essential that other players in digital markets help create an environment that supports and promotes legality on the internet. The recent *Newzbin2* judgment confirms that service providers have a responsibility to cooperate in addressing sites that favour or encourage copyright infringement – so called structurally infringing sites. These are sites a substantial part of whose activities actively and knowingly encourage, induce, assist and/or are designed for infringement. The clear judgment rendered in this case should inform and give impetus to a codification of an effective and balanced approach to addressing such sites.

As recognised by DCMS in its recent announcement on *Next Steps for Implementation of the DEA*,¹ it is also appropriate for intermediaries, such as search engines, internet advertising networks, online payment services, domain registries etc, to play a greater role in promoting an environment of legality on the internet by adopting responsible practices and procedures.

In this paper, rightsholder organisations from the music, film, television, football and publishing sectors (BPI, Motion Pictures Association, PACT, The Premier League, Publishers Association) outline the main elements of a possible Code of Practice for search engines, which would have a significant impact in helping to grow the UK digital economy and in ensuring that consumers are not drawn into illegal behaviour online. These measures would:

- assist consumers in identifying and accessing legal entertainment content on the internet;
- encourage websites which host or facilitate access to illegal content towards improved online behaviour;
- ensure that consumers reduce their exposure to malware, viruses, insecure financial transactions; scams and other risks associated with illegal sites;
- ensure that the existing system of removing illegal content from search results works to optimum effect; and
- help ensure that search engines do not unwittingly profit from illegal content on the internet through the placement of advertising or the sale of mobile applications.

¹ <http://www.culture.gov.uk/images/publications/Next-steps-for-implementation-of-the-Digital-Economy-Act.pdf>

We believe that parallel Codes of Practice should be developed with (for example) internet advertising networks and online payment providers, so that all are contributing properly to grow the UK digital economy.

The role of search in online infringement

Major search engines such as Google, Yahoo and Bing are vital portals through which consumers access information and digital content. At present, it is trivially easy for UK consumers to find and access illegal entertainment content via search engines. Indeed, in many cases it is much more difficult for consumers to find and access *legal* services via search engines, since they are swamped in search results by illegal sites. As a result, a high percentage of the traffic that goes to illegal content sites is directed there from major search engines.

Research by Harris Interactive in September 2010 for BPI found that 23% of UK consumers regularly download music illegally using Google as their means to find the content - this is the same percentage of UK consumers that use P2P networks to download music illegally.

The scale of the problem is easily illustrated. For example, if one searches neutrally for digital music to download (i.e. without suggesting whether one wants it from a legal music store or an illegal free site), search results on the first few pages of major search engines direct consumers overwhelmingly to illegal websites in preference to legal websites. On 26 September 2011, BPI made test searches on Google for the name of each of the UK's top 20 singles and albums, followed in each case by the word "mp3" (the dominant legal and illegal file format for digital music). On average, 16 of the first 20 Google results for chart singles and 15 of the top 20 search results for chart albums linked to known illegal sites. These results were virtually the same as those obtained for the equivalent search undertaken a year earlier.²

Research undertaken by the Publishers Association, conducting free search on Google and Bing for the 50 bestselling books of the week 24.04.11 – 30.04.11 showed that:

- Google returned an average of 41% non-legal links in the top ten (first page) results;
- Bing returned an average of 21% non-legal links in the top ten (first page) results;
- Google's top ten free search results now contain 18% more non-legal links that were found in a comparable survey conducted by the PA in October 2010;
- the average position for the first non-legal link on Google was 3.48, whilst the same on Bing was 4.10; and
- the average position of the first legal link on Google was 1.32, with Bing coming in at 1.14.

Similar results can be demonstrated for films, TV programmes and highlights of Premier League football. For example, according to a June 2011 Envisional Briefing report, 77% of sites that commonly link to or host infringing film and television material get more traffic from Google than

² When the same test was conducted in November 2010, 17 of the first 20 Google results for singles and 14 of the top 20 search results for albums (on average) linked to known illegal sites.

Private & Confidential

any other site online, according to a sample of thirty key sites. Notorious pirate sites such as Pirate Bay and Isohunt continue to appear as search results.

As time goes on, the situation is getting worse rather than better. Illegal sites are proliferating and they are becoming increasingly sophisticated and convincing, so that consumers are lured into using them. Illegal sites now commonly carry fake logos, carry advertising from known and respected brands, and use 'trusted' payment processors which all inspire confidence in the user.

Consumers do not wish to be left in this position. An IPSOS Omnibus survey conducted in March 2011³ found a very high degree of consumer support for search engines directing users to legal sites over illegal ones. 84% of consumers surveyed said that they expect the sites their search engine identifies at the top of its results to be legal. The same percentage agreed with the statement that "search engines should direct consumers to legal sites rather than illegal ones". 85% also said that, when purchasing goods (including music) search engines should direct consumers towards legitimate websites.

These results are not surprising. Aside from the negative consequences for the consumer by potentially breaking the law - perhaps inadvertently - by acquiring content from or providing content to illegal websites, such websites also pose a number of other risks. Spyware, malware, and viruses are all common on sites featuring unlicensed entertainment content and the cost to consumers of repairing the damage that they unwittingly cause to their computer may be considerable or even irreparable in the case of identity theft or theft of personal information. Harris Research in September 2010 asked illegal file sharers to disclose unwanted problems that arose as a result of their use of unauthorised services. 41% of these respondents had downloaded spyware, 39% had downloaded a virus or Trojan. More worryingly, 17% said that their PC or laptop crashed and was unusable for a period of time, and nearly one in eight (12%) divulged that they had to have their PC or laptop repaired or replaced.

There are also not just risks to consumers, but to the integrity and security of networks. Computers infected by malware can be the source of Distributed Denial of Service Attacks – the method by which commercial services are attacked to ensure that legitimate services cannot be used by consumers and businesses. This is a source of financial loss to UK businesses and helps seed a lack of trust in online (particularly in financial services). Consumers that are guided towards illicit sites can unwittingly put networks at risk through downloading from those sites.

We believe that search engines have a role to play in protecting consumers and businesses by directing users to sites which comply with the law and do not propagate illegal content, host viruses and other damaging or inappropriate content.

While it will remain necessary for rightsholders to send takedown notices to illegal sites, and to continue to work with search engines to improve the procedures for de-listing sites and individual content items in search results, it is clear that the current regime will not be sufficient to ensure that search engines direct consumers first and foremost to legal places to acquire digital content. To achieve that, search engines will need to do more.

³ BPI Music Online Omnibus 11th to 14th of March 2011, based 1009 adults 16-64.

Potential elements of a Code of Practice

A. Search rankings

i. De-ranking sites that persistently make available unlicensed content in breach of copyright

Proprietary search algorithms rank web pages according to “relevance” to the user; search companies have confirmed to content owners that they currently do not take into account the legality or illegality of content on a web page as a factor in determining its ranking.

At times search engines have sought to present the outcome of their algorithms, in the ranking of search listings, as something over which they does not exert control. In fact, search engines are well placed to influence the outcome of search results since they control the algorithm that produces them. They also directly control which sites they choose to crawl, index, and link. Google’s own “Web History” service learns a consumer’s preferences and re-lists sites according to individual preferences. Moreover, there are several documented instances of search engines intervening to modify their search rankings to achieve a commercial or policy goal.

For example, in February 2011, Google is reported to have taken action against JC Penny over alleged ‘gaming’ of search results.⁴ Google has also reportedly reordered search on suicide to guide users towards sources of advice, such as the Samaritans.⁵

Google is taking action against content farms, as reported widely in January 2011 and confirmed by Google itself⁶. In this example Google makes a subjective judgement about the quality of sites it is linking to and “absolutely takes action on sites that violate our quality guidelines regardless of whether they have ads powered by Google”. Given Google makes such value judgements, it should be easy to do so in the face of objective evidence. The other element of this of note is that Google is making an assessment of the quality of the entertainment content. We believe that this is particularly relevant when considering content on sites on the basis of legality.

We propose that in order to further protect consumers and to encourage responsible behaviour among websites, the extent of illegal content on a website should become a factor influencing the ranking of that website in search results returned to consumers. In addition, where a site has been found by a court to be substantially infringing, it should no longer be crawled, indexed or linked at all.

⁴ http://www.nytimes.com/2011/02/13/business/13search.html?_r=1 These, and other aspects search ranking, were investigated by Congress at the House of Representatives Subcommittee on Intellectual Property, Competition and the Internet *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II* 6 April 2011.

⁵ http://www.samaritans.org/media_centre/latest_press_releases/google_one_box.aspx

⁶ <http://googlepublicpolicy.blogspot.com/2011/09/making-copyright-work-better-online.html>

We should explore simple and objective mechanisms to enable a search engine to take account of these factors. Search engines already respond to valid de-listing requests from copyright owners.⁷ One proposal would be that the number of URLs that the search engine has de-listed as a result of takedown requests from right holders, in respect of a particular website, should be reflected in the ranking accorded to that website.

Another factor to consider might be the type of infringing content – i.e. if a site consistently gives access to particularly damaging content such as pre-release material - that might be a factor that would lead to increased de-ranking. There may also be a threshold of serious repeated or egregious infringement beyond which a site should be de-listed entirely or at least for a period of time, to allow the copyright infringement issues to be properly addressed.

The ability of websites to serve counter-notice for URL de-listing under US DMCA procedures, and the fact that URL de-listing is routinely publicised by Google on the Chilling Effects website, ensure both that sites are able to challenge de-listing requests that could have an impact on their ranking, and that there is transparency about the alleged infringements that may impact on a site's ranking.

Given that Google already de-ranks and de-lists sites that do not meet its own “quality guidelines” or otherwise violate its policies, we do not believe that search engines would face significant legal exposure if they were to de-rank or de-list sites using an objective measure, based on their actions in response to legal DMCA complaints, in pursuit of the legitimate objective of preventing their service being used to facilitate copyright infringement.

ii. Prioritising legal sites in searches for content

The group of rights holders believes that, where content owners are able to objectively and reliably certify websites as providing legal access to digital content, those sites should be prioritised by search engines in their search rankings above sites which are not so certified, for certain specific types of search. Industry could take the lead on this by ensuring there are appropriate certification programmes in place. Rigorous care would have to be taken to ensure that any such schemes would be transparent, open and non-discriminatory.⁸

We recognise that the purpose of consumers' searches relating to digital content may be quite diverse and that it would not be appropriate for prioritisation to be implemented for every type of search. Rather, prioritisation should be focused on searches where the consumer is clearly trying to access digital content to download or stream, rather than simply looking for information.

⁷ As reflected in Google's policy statement of November 2010, see <http://googlepublicpolicy.blogspot.com/2010/12/making-copyright-work-better-online.html>

⁸ One example of such a certification programme is the *Music Matters* scheme <http://www.whymusicmatters.org>. This scheme, which is open to any website to join at zero or nominal cost, awards Music Matters certification to sites making available recorded music that satisfy objective criteria, in terms of having appropriate procedures in place to ensure that the content they make available is properly licensed.

To use the example of music, we would propose that prioritisation be enabled for searches that contain any of the following key search terms: "mp3", "flac", "wma", "aac", "torrent", "download", "rip", "stream" or "listen", "free", when combined with an artist name, song or album title contained on a list to be regularly updated and provided to a search engine by a recognised and properly mandated agency representing rights holders for a particular sector, such as BPI.

Such a measure should not be complex to implement from a technology perspective and would go a long way towards ensuring that consumers are directed towards legal sites on the Internet rather than falling, sometimes initially unwittingly, into content piracy.

iii. Making the existing process work better

Google has announced some recent welcome improvements to its processes for receiving and acting on DMCA notices submitted by rightsholders. In our experience, average takedown times have improved and the process of submitting notices has been made easier. Google has also removed from Autocomplete a number of terms that encouraged consumers towards infringing sites.⁹ However, these steps do not go far enough. There is more that can and should be done to improve this process:

- Artificial limits on the ability of rightsholders to search for infringing content should be removed;¹⁰
- infringing links should be removed within a maximum of 4 hours of being reported by an authorised agent. Once removed, there should be effective measures to prevent re-appearance of infringing links and of pirate sites and blog spots;
- if a website is subject to a blocking order or has been adjudicated by a court to be a structurally infringing site, the sites in any case should be automatically de-listed and removed from the cache, without any time delay while appropriate procedures and criteria should be implemented to delist sites that are persistent offenders;
- to ensure an expedited process, rights holders should be able to take advantage of automated tools, which should be implemented by search engines to allow rapid removal and disabling of infringing links; and
- Autocomplete or "suggested searches" should not in any instance direct consumers towards illegal sources for content. Search engines should continuously review autocomplete/suggested search terms and should respond expeditiously to requests from rights holders to remove terms that direct consumers to illegal sites.

⁹ <http://googlepublicpolicy.blogspot.com/2011/09/making-copyright-work-better-online.html>

¹⁰ Google currently limits the number of de-listing submissions that a rights holder can make to 10k per day.

B. Advertising

Search itself is a form of advertising and the ranking and listing of sites is affected by search engines through the sale of words from search terms to advertisers to help serve adverts. Some search engines go further, and have operations that serve adverts such as Google's DoubleClick, AdSense and AdMob and Microsoft's AdCenter. Such adverts generate revenue for providers of websites that are based on illegal use of content. Meanwhile reputable firms find themselves as banner ads on sites in the UK and abroad that are set up to infringe copyright.

A Code of Practice for search engines should include measures to ensure that search engines do not support the business models of substantially infringing sites by supporting them with advertising and that they do not themselves profit from online infringement. To that end, we propose that search engines should:

- implement active, ongoing, effective screening procedures for ad partners (both those that buy ads on the search engine's website or run ads from the search engine's ad network on their third party sites);
- eliminate all adverts on substantially infringing sites and on search results pages that contain links to substantially infringing sites;
- establish an effective and simple complaints procedure so third parties can notify the search engine/ad network of ad placement on sites that facilitate infringement, or search result pages that do so;
- continuously review key search words;
- ensure that it does not place advertisements for Google products and services on substantially infringing sites;
- end the practice of selling key words that are closely associated with piracy; and
- prevent re-registration of terminated ad partners through active, effective internal procedures.

As indicated above, we believe that a separate track of the roundtable process should be established to develop and agree a Code of Practice for internet advertising networks generally.

C. Mobile Applications

In addition to its search and advertising activities, Google also operates an applications platform for Android devices. Given Google's direct financial interest in applications sold through its Android Market, Google (or any search engine that operates an apps platform) should:

- effectively screen applications to see if they are likely to substantially facilitate or encourage infringement or otherwise designed to facilitate infringement;

Private & Confidential

- take down mobile apps where it is aware that they are designed or known to be used to illegally download entertainment content, either via p2p applications or unauthorized lockers;
- prevent apps from being reposted, or “copycat apps” being posted, once an app has been removed as above; and
- terminate the accounts of developers that repeatedly post apps that facilitate infringement and prevent them registering new accounts.

D. Governance

We believe that a Code of Practice could be administered and overseen on a voluntary basis, with DCMS in attendance, so that Government remains well informed about the functioning of the Code. It will also give strength to the process if Government maintains its role.

Moreover to ensure transparency, accountability and democratic scrutiny, we would suggest that DCMS prepare an annual report to the parliamentary Select Committee on Culture, Media & Sport on the functioning of the Code of Practice. This would help to ensure that, while meeting its objective of ensuring that search engines play a more responsible role in reducing online infringement of copyright, the Code of Practice would act proportionally within a wider public policy objective of freedom of general access to information online and healthy competition and access to online markets.

UK search: the way ahead Appendix E: Search Engines' Proposed Code

The UK internet economy:

(Obtained by U.K. Open Rights Group)

The UK internet economy now accounts for over 7.2 per cent of UK GDP and is forecast to grow to over 10 per cent by 2015. The UK leads the world at e-commerce: online, the UK now exports three times more than it imports. We have become a nation of digital shopkeepers, with small businesses online growing over four times faster than those offline. This rapid growth in the digital economy continues to create jobs – with some estimates suggesting 350,000 jobs over the next five years.

The Coalition Government has made clear that it both recognises the value of the UK economy and is committed to nurturing its growth.

"I am committed to making the UK the best place in the world to start, run and grow a hi-tech company." Prime Minister, 29 September 2011

In his September 2011 speech to the Royal Television Society, the Secretary of State for Culture, Media and Sport echoed the Government's commitment to hi-tech growth and described how, with the right conditions, this could create huge opportunities for the creative content industries in the UK:

"The first priority must be to capitalise on the extraordinary opportunity presented by our digital and creative industries. It is an opportunity that is probably bigger for this country than any in the world except the United States. That is because we are the second largest producer of digital content in the world and the internet makes it possible to distribute that content worldwide at close to zero cost."

However just as the internet creates fantastic opportunities to distribute UK creative content worldwide, it also brings with it new and disruptive challenges, and the Secretary of State is seeking to help strengthen copyright enforcement in order to support those who create content.

Supporting the Secretary of State's multi-stakeholder approach:

UK internet users are world leaders in their use of innovative digital content and online e-commerce services. At the same time, the UK creative industries are world leaders in innovative, commercially successful content of all kinds.

The UK can continue holding both of these leadership positions if the right solutions to online copyright infringement can be agreed, which truly focus on the root causes of piracy, and target enforcement in a proportionate way. Disproportionate measures would deter inward investment, stifle legitimate innovation, and make it harder for new artists to break through. We therefore support the Secretary of State's efforts to facilitate cross-industry dialogue to address industrial-scale piracy. In addition, Google, Microsoft and Yahoo! will continue to help audiences find high-quality content online.

According to the latest figures from the BPI, digital revenues grew by 24.7 per cent in 2011 to account for 35.4 per cent of overall sales – in particular, digital albums were up 43.2 per cent year-on-year. "It is highly encouraging for the long-term prospects of the industry that the pace of digital growth continues to accelerate," says chief executive Geoff Taylor. More needs to be done but we are confident that we are on the right track with respect to the development of legal services for entertainment content online.

Google, Microsoft and Yahoo! continue to explore and conclude innovative partnerships with the creative industries – built around providing access to more content for more users.

Tackling copyright infringement on the internet:

As search engines, we put our users first. Our policies are built around that principle. It is vital that as we seek to work with the Secretary of State and the rightsholders to tackle online copyright infringement that this principle of putting users first is not overturned.

Search engines play a vital role in free speech, creativity, expression, and innovation by organising billions of web pages in a way that they can be more easily discovered by internet users. Search engines benefit creators and rightsholders by helping connect users to artists and content producers.

Search engines are not the source of infringing content. Removing links from a search engine does not remove illicit content from the internet.

Rightsholders have the primary responsibility for protecting their intellectual property, and are in the best position to identify their intellectual property and evaluate potential infringement.

The violation of intellectual property rights is an issue search engines take seriously and have policies and practices in place to address. However, without specific, reliable notices from rightsholders, search engines lack the knowledge and capability to identify and address infringement without inadvertently disrupting the free flow of information on the internet.

Search engines aid rightsholders in their efforts to enforce their rights by providing robust and effective copyright notice and takedown systems which allow for the expeditious removal of problematic links and advertisements from the search engine's database. Rightsholders must participate fully in the notice and takedown system for it to be maximally effective and expeditious in addressing the shared goal of reducing infringement.

To that end, this document sets out general principles rightsholders and search engines should follow to address online infringement effectively.

1. Principles for ensuring effective and expeditious copyright notice and takedown – search engines:

- Search engines should have a method to allow rightsholders to provide notice regarding links to infringing materials indexed by the search engine;
- Search engines should have procedures for expeditiously processing valid takedown notices from rightsholders;
- To further free speech, creativity, expression, and innovation online, it is appropriate for search engines to consider counter-notices from those affected by takedown requests and who seek to challenge the basis of those requests;
- Search engines will continue to work with rightsholders to improve notice and takedown practices and systems to eliminate inefficiencies in the processing of takedown notices.

2. Principles for ensuring effective and expeditious copyright notice and takedown – rightsholders:

- Rightsholders should seek removal of infringing content directly from the infringing actor or from the online hosting service before seeking remedies from search engines;
- Rightsholders should limit their removal request to links actually offered by a search engine in its results or advertisements;
- Rightsholders should substantiate their ownership of allegedly infringing IP and their claims of infringement of their IP;
- Rightsholders should narrowly and specifically identify infringing content in their takedown notices and must issue such notices only after assessing their impact on any non-infringing uses and concluding that the takedown would not have an adverse effect on such non-infringing uses;
- Rightsholders should agree to a reasonable procedure for sites or advertisers to file counter-notices that contest the takedown demand, allow for restoration of the content under appropriate circumstances, and eliminate liability of search engines for restoring content in response to counter-notices;
- Rightsholders should be accountable for improper notices, e.g. through the failure to properly identify infringing material or limit the negative effect on non-infringing uses;
- Rightsholder should support transparency in the takedown process, by ensuring that notices be made publicly available with only minimal redactions to protect privacy interests;
- Rightsholders should not pursue legal action against search engines for content that they link to unless they have first submitted takedown notices meeting the standards described above, and the search engine has refused to remove the specific noticed links.

3. Leading industry efforts to protect advertisers from association with infringing content:

- Our businesses are also damaged by misplacement of advertising against inappropriate content. The advertising networks and exchanges we own operate in highly competitive spaces, and rely on building and maintaining the trust of our advertiser clients. We already have strong commercial incentives to avoid placing advertising against copyright infringing material, so where instances do occur, they are rectified swiftly.
- Along with our own efforts, all three companies are active members of the Internet Advertising Bureau, and are involved in the evolving system for online self-regulation. Our advertising networks are all IASH signatories, and we take our responsibilities in this respect very seriously. We are constantly vigilant to the dangers of misplacement of advertising online, as this fundamentally affects our ability as businesses to maintain the trust of our valued advertiser clients.
- The online advertising world is constantly changing, and now involves a bewildering array of different players and technologies. The self-regulatory system must, and will, evolve to encompass these changes.

Ongoing, multi-stakeholder engagement:

We appreciate the role the Secretary of State has played in engaging all stakeholders in meaningful dialogue.

The interconnected nature of the internet means that a well-intended but narrowly focused effort to address problems can have serious unintended consequences on the integrity of the internet and the rights of its users. Crafting effective action requires a holistic approach that includes the engagement of diverse stakeholders, especially those with deep understanding of both technical and human rights considerations.

Over the last few years in the UK, there has been steady and welcome growth in understanding between the creative industries and internet companies.

This document is written to play a part in furthering that understanding and providing a foundation for a progressive partnership with the creative industries that will reduce rates of copyright infringement.

We therefore commit to ongoing dialogue in the UK – in parallel with global efforts – with copyright owners and other stakeholders. In our view, this dialogue should focus on:

- Assessing and sharing insights into the changing nature of piracy and its technologies;
- Gathering intelligence about the effectiveness of all of the current interventions (injunctions, notice and takedown procedures etc.) and providing a forum to discuss their evolution.

This dialogue would inform, and be informed by, other dialogue at European level and beyond. The aim would be a steady progression of our commercial and policy responses to piracy in the UK, which takes due account of global developments.

February 2012