“PLEASED TO MEET YOU…WON’T YOU GUESS MY NAME?”

REDUCING IDENTITY FRAUD IN THE AUSTRALIAN TAX SYSTEM *

HENRY PONTELL
UNIVERSITY OF CALIFORNIA, IRVINE

VISITING PROFESSOR
CENTER FOR TAX SYSTEM INTEGRITY
RESEARCH SCHOOL OF SOCIAL SCIENCES
THE AUSTRALIAN NATIONAL UNIVERSITY

* Paper presented at the Centre for Tax System Integrity, The Australian National University. *“Identity Fraud and Illegal Tobacco: An Absence of Integrity,”* Sponsored by the Australian Taxation Office. October 29, 2002.

"Regard your good name as the richest jewels you can possibly be possessed of; for credit is like fire. When once you have kindled it you may easily preserve it, but if you once extinguish it, you will find it an arduous task to rekindle it again."

Socrates

Since it is not at all likely that Socrates could have envisioned the state of the world thousands of years after he wrote this, he most certainly couldn’t have fathomed that his words would ring more true today than at any other time in history.

Identity fraud is primarily a tool used to facilitate some other criminal act. Stealing another person's identity (i.e., identity theft) does not even have to enter into the picture. As the September 11th terrorists proved, identity theft was not necessary in the commission of one of the most heinous acts in history. About a month before the attack on the World Trade Center, Abdul Azziz Alomari and Ahmed Saleh Alghamdi, two of the terrorists who crashed planes into the north and south towers, used an accomplice to approach a secretary of a Virginia lawyer.[1] The secretary was paid to complete false Virgina affidavits and residency certifications. The documents indicated that Alomari and Alghamdi lived in Virginia, when in fact they were residing in motels in the state of Maryland. The two men later used these false documents, which were notarized by the secretary, to obtain official identification papers from the state of Virginia. These documents allowed them to board the doomed planes.[2] They did not need to steal another's identity, or commit what is known as "true person fraud." The two men simply used false documents to misrepresent their own. The September 11th hijackers made wholesale use of fictitious social security numbers, false identities and fraudulent identification documents in their attack on the United States.[3]

Identity fraud, or the use of false identities or fraudulent identification documents has been the subject of much discussion, debate and legislation in recent years. In the United States prior to September 11th attention focused primarily on financial fraud, and retail and consumer crime matters. It has now been substantially broadened. No longer simply the tool of the con artist or organized criminal, identity fraud has the potential to change the world we live in forever. It is central to almost any criminal enterprise, including a number of cyber crimes, terrorism, drug trafficking, alien smuggling, and common theft.

Identity fraud is one of the fastest growing, and insidious crime problems in the world today. It's myriad forms and use in facilitating a number of crimes poses unique and unprecedented challenges that require not only greater planning, coordination, and cooperation within and among government agencies, but with those across national borders as well. Identity fraud is an effective crime tool employed by individuals, organized crime groups, and terrorists. It generally involves a person falsely representing him or herself as either another person or a fictitious person. It may also take the form of a person fraudulently representing themselves through the misrepresentation of crucial facts regarding their own identity. These misrepresentations of same, stolen, or fictitious identities are made possible by either obtaining (through theft or fraud) documents and/or personal data of another individual, or by the production of false documents themselves. "Identity fraud" is a much more inclusive crime category than "identity theft," where one uses the identity of another to enact a criminal offense. By taking advantage of weak or ineffective identification and authentication systems, criminals have victimized consumers, credit card companies, government agencies, businesses, and entire nations.

Numerous accounts link the growth in such offenses to the increased use of computers and the Internet. Given the accelerated pace of these crimes in recent years, one could easily surmise that computers have done for identity fraud what the microwave has done for popcorn. Information is more freely and widely available, and databases containing private information exist at numerous commercial and government sites. In too many instances, the security of these data has been compromised, or the information has been stolen, or improperly used. This can result from criminal activities by individuals both within and outside of the agencies and businesses that are charged with their protection. Adding to the mix is the fact that the anonymity afforded by cyberspace, along with technological advances associated with it, have both outpaced effective regulatory and enforcement schemes, and broadened the scope and possibilities for crime in general. Many of these cyber crimes are associated with e-commerce and involve the use of false or stolen identities. A number of academic studies, presentations, and official reports in Australia attest to the importance, scope, and nature of identity fraud, and various strategies for dealing with it.[4]

It is clear from both the U.S. and Australian experience at least, that identity fraud poses serious challenges and policy choices that generally center on issues of cost and control. While seemingly separate concerns, I will argue from a white-collar crime perspective, that they are inexorably intertwined and dependent upon each other.

Finally I will offer some overarching concepts that bear directly on prevention strategies and means of control currently underway here in Australia, and elsewhere.

The Identity Fraud Problem in the U.S. and Australia: Questions of Numbers and Prevalence

The numbers associated with identity fraud have become staggering in recent years, and continue to increase. The United States Secret Service, which along with other agencies has jurisdiction over financial crimes, reported in 1997 that of the nearly 10,000 arrests its agents made, that 94% involved identity fraud.[5] Similarly, along with the U.S. Postal Inspectors, they have ascertained that organized crime groups have made identity fraud a major part of their international operations in the commission of financial crimes, drug shipments, immigration violations, and violent crimes.[6] The victimization of individuals and corporations through identity fraud has also been documented. For example, one recent study notes that almost all (96%) of the approximate $407 million in fraud losses reported by Master Card in 1997 involved identity theft.[7] The Secret Service also reported that the losses due to identity theft in 1997 for which arrests were made totaled almost three-quarters of a billion dollars, which represented twice the figure of the previous two years.[8]

A study issued by the U.S General Accounting Office in March, 2002 reports findings regarding systematic data on identity frauds. The report notes numerous problems in the collection of pertinent information throughout government agencies and businesses. It deals with identity theft only, and with the victimization of consumers and e-commerce, not government entitlement programs, which are enormous, and cover such areas as social security, health care, and welfare. This narrow focus on consumer identity theft, can only lead to a vast underestimate of the true prevalence and cost of identity fraud. The GAO found no systematic data to test assumptions regarding non-reporting or whether those who made reports were actual victims, or "preventative" callers (those who had lost documents, or had them physically stolen in wallets or purses). Using anecdotal data, the GAO concluded that the problem seemed to be increasing in both prevalence and cost.

More than anything stated in the report, perhaps, the GAO findings speak to the rather dismal state of affairs in the U.S. regarding efforts to prevent and control identity fraud. Coordination efforts of various agencies are not specified, nor are they likely to be optimal given past history. Moreover, the FBI and Secret Service have adopted the "back-end enforcement stance" that identity fraud is not a "stand alone" crime, but rather a component of white-collar and financial crimes, such as bank, credit card or electronic device frauds or counterfeiting. As I'll discuss in a few moments, for a number of reasons a proactive and preventative is needed to deal effectively and more efficiently with the problem of identity fraud.

Australia

In August 2000, the House of Representatives Standing Committee on Economics, Finance and Public Administration of the Parliament of Australia published a study entitled, *Numbers on the Run*, which reviewed the findings of the Australian National Audit Office (ANAO) Report (No. 37 1998-99) on the Management of Tax File Numbers (TFN). The ANAO study of the TFN system had found that: 3.2 million more TFNs than people in Australia at the last census; 185,000 potential duplicate tax records for individuals; 62 percent of deceased clients not recorded as such in a sample match; and 40 percent of deregistered companies still recorded as active.[9] These findings, along with the estimate of almost half a billion dollars in uncollected tax revenue led to the Committee's report and its overall finding that, "…what we found was an organization that is reactive rather than proactive; where emphasis is placed on strategies that return a short term financial gain rather than ensuring the long term integrity of the system; and where management philosophies are not well translated through the organization."[10] While this unflattering description undoubtedly applies in varying degrees to many, if not most public bureaucracies and large corporations in the world today, it was indeed a call to clean up and ensure the integrity of the nation's TFN system. The Parliamentary inquiry provided 26 recommendations, covering the areas of ATO data and systems quality, data matching, TFN registration, tax treatment and work rights of non-residents, identity fraud and proof of identity processes, extending the TFN quotation, and the implications for the Australian business number. Most of the recommendations relate to improving data integrity and quality, improving internal processes, proactive links with other agencies, additional audits, preventing frauds, and providing better proof of identity processes and assessing the problems of identity fraud.

The committee notes that there are numerous agencies and groups that are investigating ways to get their arms around the problem of identity fraud, with the goals of providing for better data integrity and document processing in public agencies. These include the Office of Strategic Crime Assessments, a working group chaired by AUSTRAC, the Australian Registrars Conference, the Heads of Fraud Conference, and the Australian Bureau of Criminal Intelligence.[11]

Regarding the extent of identity fraud, the ANAO report noted the ease with which it could be committed through obtaining false documents, and the associated problems for government agencies involved in the verification of PoI. It also found that identity fraud posed a significant and growing problem especially with the development of new technology related to electronic commerce. This was indicated by the estimate that 25 percent of frauds reported to the Australian Federal Police involved the theft of identity, the availability of "identity kits" to generate high quality false documents, and that fabricated documents for a false identity are for sale, including via the Internet.[12] They recommended that: government agencies work with industry to develop statistics regarding the extent and cost of identity fraud; that the ATO improve internal processes for both establishing identity and preventing identity fraud; that the government begin a formal process for assessing PoI risks and reform; and that the government develop a process for working with official agencies and industry to develop strategies for reducing and preventing identity fraud, including the possibility of a national electronic gateway for verifying documents. These efforts are currently underway. It is also important to note that the Inquiry's report and recommendations highlight that the problem of identity fraud is a "community problem."

Inherent Problems in Measuring Cost and Prevalence: Identity Fraud as White-Collar Crime

The government's efforts to produce more data, cost and prevalence estimates, and to quantify the economic impact of identity fraud as providing "a powerful step toward ensuring support for reform across all levels of government, business and the community," is not likely to be all that "powerful" given what is already known about it in the U.S., Australia, and elsewhere, and what a rather substantial body of research has already established regarding the hidden and costly nature of white-collar criminality in general.

White-collar crimes, especially financial frauds, generally remain undetected unless victims report them, systematic investigation leads to discovery, or serendipitous events lead to their recognition. Financial crimes are enacted through a number of mechanisms such as identity frauds, accounting frauds, and insider control frauds, resulting in massive losses to both organizational and individual victims. There is much evidence that has already been amassed to establish this as fact.[13] How much crime "actually exists" is determined by the organizational resources available to uncover, investigate, and prosecute it, and more generally, enforce what most experts already regard as inadequate laws aimed at its control.

The irony of course is that the capacity to do this in an effective manner is itself determined by the political will to take fraud seriously enough to devote such investigative resources in the first place. If that same political will is dependent on "proving" through the production of numbers that enough of a problem exists, then the cycle of non-discovery and non-recognition remains intact. This is central to understanding the cost and prevalence of white-collar crime, which is apt to be neither reported nor recorded in a timely or accurate manner.

In fact, as we have witnessed over the past two decades, the most consequential white-collar crimes such as the savings and loan debacle and the recent corporate scandals in the U.S. which have affected not only national but international markets, are brought to public attention only *after* massive losses are realized, and even then, the actual cost, nature, and causes of fraud continue to be debated.

These two cases also illuminate the operational definition of cost. Should the "cost" be calculated based upon: the specific transactions that were fraudulent?; only those activities that bring criminal charges?; only those criminal activities that end up being adjudicated?; fraud costs cited in actual convictions?; the cost of the bankruptcies and failures caused by fraudulent activity?; costs of investigation and prosecution?; investor and taxpayer losses?; or some combination of these? All of them represent true "costs" of fraud.

Simply put, studies can never fully recognize the cost of fraud because of its hidden and unreported nature, and the inability or unwillingness of agencies and businesses to discover, or record it in a timely manner. Rather, they are bound to arrive at figures that under represent the true extent of the problem.[14] Thus, any extrapolation from existing reported figures, or those gained through surveys will necessarily produce an absolutely conservative estimate of identity fraud. Moreover, given the rapidly increasing number of identity fraud cases, its growth curve will need to be taken into account as well. These are manifest considerations for future policy, especially in regard to realistic resource allocations.

Ethnographic and qualitative study of actual behaviors of official agencies regarding the treatment and processing of identity fraud, their potential conflicts and disparate interests, as well as of the attitudes and behaviors of private industry and consumers would provide important information for properly grounding cost estimates, as well as for prevention and control strategies. These factors speak to organizational capacities for generating the information upon which such cost and prevalence estimates are ultimately based. In the case of tax system efforts to reduce identity fraud, specific information regarding the state of current state of IT systems, intra-agency coordination, available resources to accomplish required tasks, and other organizational and legal issues need serious evaluation. This simply cannot be accomplished in an effective manner without all necessary organizational elements in place, and, perhaps most importantly, without systems and data integrity being given equal prominence to other necessary functions within the ATO. This means that adequate resource allocation, internal planning, and coordination across the entire agency -- not just the offices involved with data integrity-- need to be prioritized. Having internal data that are valid, reliable, protected, and integrated is a cornerstone of any healthy organization, especially one as vulnerable to both non-compliance and political attack as a nation’s tax system. Unfortunately, the world’s governments have a long journey ahead in this regard.

In the U.S., for example, even the most rudimentary steps to protect identity information are seriously lacking. In August, 2002, an audit of the Internal Revenue Service reported that it was unable to account for an unknown number of 6,600 computers lent to volunteers who assist low income, disabled, non-English-speaking and older citizens with their tax returns.[15] An audit of other IRS programs found that 2,300 computers were missing. The computers contained private taxpayer data that constitute a prime source for identity thieves. The audit followed previous reports that the U.S. Customs Service lost track of 2,000 computers and that the Justice Department could not find 400 of their machines. One U.S. Senator commented that this “latest disclosure cries out for a ‘government-wide effort’ to prevent computers from being lost or stolen.” He further laments, “I’m worried that just as dryers have a knack for making socks disappear, the federal government has discovered a core competency of losing computers.”[16] In response to the audit results, an IRS official noted that its management “recognized that inadequate internal controls and accountability over computers were areas that needed dramatic improvement.”[17] The obvious question that arises is how many other “dramatic improvements” need to be accomplished given the complexities of effective response to the problem of identity fraud.

Responses

Trying to deal with identity fraud through criminalization alone, cannot serve as an effective means of control. The agencies that might best foster this do not involve law enforcement, but the documentation and authentication of identity itself.

Professor Gary Marx, one of the world's leading authorities on surveillance, technology and social control mechanisms, points out that in complex settings in democratic societies, "relying primarily on technology to control human behavior has clear social and ethical limitations."[18] Simply put, regardless of how ideal a technical control system may appear in the abstract, it is inevitably subject to the harsh realities of implementation and actual practice. "The perfect technical solution is akin to the donkey incessantly chasing a carrot suspended before it."[19] Larger systemic contexts, consequences and alternatives may be ignored. As Marx notes, "The complexity, and fluidity of human situations makes this a rich area for the study of trade-offs, irony and paradox. There are some parallels to iatrogenetic medical practices in which one problem is cured, but at the cost of creating another. Technical efforts to insure conformity may be hindered by conflicting goals, unintended consequences, displacement, lessened equity, complacency, neutralization, invalidity, escalation, system overload, a negative image of personal dignity and the danger of the means determining, or becoming the ends."[20] All of these concerns need to be fully examined before implementing technological “solutions.” Moreover, the lack of privacy concerns and awareness in various sectors of society as well as the careless use of personal information provide structural gaps in the social control of personal identity that criminals continue to exploit. As seen by the example of missing computers, the government may itself inadvertently contribute to the escalation of the same fraud that it wishes to suppress.

Aside from the technological aspects of control, which can be compromised in any number of ways by competing technology and various other neutralization mechanisms, the *human context* of control also remains particularly vulnerable. This can be easily overlooked, as it exists in the long shadow of expensive and sophisticated technology and complex operational systems. Consider the following, which underscores the point that state-of-the-art control systems can be completely undermined through simple human interactions: “…a thief who could not break a manufacturer’s sophisticated encryption code, never-the-less managed to embezzle millions of dollars through generating fake invoices. He did this by having an affair with the individual who had the encryption codes.”[21]

The National ID Debate

It is of paramount importance that officials recognize that security and privacy issues associated with large government databases present major problems. As a result of the September 11th attacks, legislation was introduced before the United States Congress to initiate a standardized identification system that would link existing information in state motor vehicle databases to “create a standardized driver's license equipped with technology capable of uniquely identifying the cardholder.”[22] The promoters of the bill claimed that their goal was *not* to create a national ID, but simply to stop identity fraud and terrorism through the use of phony drivers licenses. The proposal, which was supported by the American Association of Motor Vehicle Administrators, would have allowed states to “share demographic and driving record information in real time, and would mandate the use of security features such as holograms, fingerprints or other biometric identifiers on all state-issued ID cards.”[23]

In response to this proposed legislation, an April 2002 report from the National Academies of Science argued against a national ID card due to concerns over privacy and security of personal data collected by official agencies. The study was endorsed by the National Research Council’s Computer Science and Telecommunications Board, which is comprised of a number of private sector and academic institutions including Microsoft, AT&T, MIT and Stanford, among many others. It warned that current efforts to establish a national identification system could produce more harm than good, unless policymakers first paid serious attention to a vast array of privacy, security, and logistical matters.[24] It also noted that the “costs of abandoning, correcting or redesigning a system after broad deployment might well be extremely high."[25]

The study concluded that, "Given the wide range of technological and logistical challenges, the likely direct and indirect costs, the serious potential for infringing on the rights and freedoms of ordinary citizens, and the gravity of the policy issues raised, any proposed nationwide identity system requires strict scrutiny and significant deliberation well in advance of design and deployment."[26] Besides the conservative cost estimate of $100 million to make changes to the country's 200 million existing drivers' licenses, the report also warned of "function creep" or future uses of a national ID in ways not originally intended. This phenomenon is well illustrated by the current use of Social Security numbers, which were created solely for administering Social Security benefits, but are now used as the major national identifier. Moreover, securing against the misuse of information becomes more difficult as the system of users expands beyond original boundaries, and the system itself becomes a larger and more attractive target for malicious hackers.

The ATO is no different from many other tax systems in its vulnerability to constant criticism no matter what it attempts to accomplish in areas such as compliance, audit or collections. Having issues discussed openly, especially involving the use of personal information, serves an important educative and disclosure function that can mitigate much misunderstanding. For example, if tax officers do their job effectively, they may be seen as overbearing and unfair.[27] If they are not enforcing rules, they may be viewed as incompetent in the collection of taxes. Fostering mechanisms to promote voluntary compliance is an important goal, and that can be better accomplished through public education as to the importance of the protection of identity information, and what the ATO is doing to help in this regard.

Self-Monitoring and Surveillance

Just as important as ensuring the accuracy and security of data and systems, is evaluation on an ongoing basis. Identity fraud has many forms, and can affect operational systems and commerce in myriad ways. One mechanism that can be employed to monitor system integrity involves the use of government agents posing as persons trying to compromise it using known techniques.[28] In discussing ideas regarding the detection of "dirty data," for example, some researchers have pointed to the use of deceptive techniques to allow access to information that would not otherwise be available or known to others. Officials using deceptive techniques on their own agencies, should raise no major ethical concerns. It also allows for constant system monitoring, and the identification of weak spots in need of immediate improvement. It involves proactive enforcement and regulation of identity fraud rather than simply reacting to system weaknesses on a case-by-case basis after the fact. Such monitoring could take the form of sophisticated and controlled field experiments that would provide substantial systematic data regarding organizational weaknesses upon which necessary organizational changes could be based. These system vulnerabilities are, after all, the crux of the identity fraud problem. This approach also entails working forward towards increased system integrity at both the human and technological levels, versus simply working backwards from actual reported crimes as “trace elements” which lead to the discovery of identity frauds and how they took place. Moreover, there is variability in the visibility of these trace elements that make them less than ideal for plugging gaps in the system. For example, Marx notes, “Trace elements involving victims are likely to become publicly known to the extent that (a) the gap between victimization and its discovery is short, (b) the victim is personally identifiable, (c) the victim is aware of the victimization, and (d) does not fear retaliation for telling others about it. There is a parallel here to the ease of discovering victim as against victimless crimes. The former are much more likely to be known about.”[29]

Conclusion

Much remains to be done both within ATO as well as other public agencies, the private sector, and the general population in terms of awareness and education regarding issues of identity fraud. Before various technologies are introduced, an inventory of existing organizational capacities to employ them effectively, necessary intra- and inter-agency agreements, private sector regulation of the use of personal data, consumer awareness and education, and an airing of the ethical and moral issues associated with third party uses of personal data need to be accomplished if efforts to reduce identity fraud are to be successful. The difficulty with quick fixes, or silver bullets when it comes to complex social problems is that they never deliver the results promised, and often create new problems. Understanding how and why the social system itself encourages identity fraud, and making persons aware of the need to protect their personal information are important factors in reducing its frequency.

Organizational capacity issues loom large in effectively dealing with identity fraud within public bureaucracies such as tax and criminal justice.[30] Their external environments must also be taken into account insofar as they affect organizational workloads. These capacity issues must be taken into account when government policies are developed regarding enforcement and compliance responses. A primary reliance on enforcement strategies inevitably results in system overload and the inability to respond effectively. This is akin to a sprinkler system shutting off when the fire gets hottest. Identity frauds in the U.S are growing by leaps and bounds, and now include an increasing number of “inside jobs” which involve the theft of identity of family members.[31] The retiring commissioner of the U.S. Internal Revenue Service, Charles Rossotti, recently highlighted the stunning lack of capacity to deal with cheating due to increasingly sophisticated schemes. He noted the “huge gap” between those cheating the system in numerous ways and the agency's "capacity to require them to comply."[32] "The IRS is simply outnumbered when it comes to dealing with the compliance risks."[33] He pointed to the fact that the IRS would need to hire almost 35,000 workers just to keep pace with increasing demands by the year 2010, and claimed, "If these problems and conditions are left un-addressed, we could face an enormous crisis in confidence in the tax system."[34] This not only points to an important irony of current control efforts (i.e., the potential escalation of non-compliance and de-legitimization of the system itself), but underscores the simple truth that the ability of any system to undertake new initiatives in an effective way, depends on its baseline capacity to deal with current issues. That baseline capacity does not currently exist in the largest voluntary tax system in the world.

Technology alone, no matter how politically expedient, cannot provide an effective solution. In a list of what he terms "techno-fallacies" Marx illustrates the uncritical use of technology to provide control and order through surveillance in modern society. A sampling of those most related to identity fraud include: The fallacy of perfect containment or non-escalation (or the Frankenstein fallacy that technology will *always* remain the solution rather than become the problem); the fallacy of permanent victory; the fallacy of the 100% fail-safe system; the fallacy of assuming that personal information on customers, clients and cases in the possession of a company is just another kind of property to be bought and sold the same as office furniture or raw materials; and the more general fallacy of re-arranging the deck chairs on the Titanic instead of looking for icebergs.[35] Someone needs to be on deck paying attention to the horizon ahead.

NOTES

[1] United States v. Zacarias Moussaoui, U.S.D.C., E.D. Va., Dec. 2001 term, Indictment, Paragraphs 104-107.

[2] Krim, Jonathan and O'Harrow, Robert Jr., "National ID Cards Gaining Support," *Washington Post*, December 17, 2001.

[3] *Ibid.*

[4] See Russell G. Smith. "Identity-related Economic Crime: Risks and Countermeasures." Australian Institute of Criminology, Report No. 129, September, 1999; Ringlin, Shane. "Identity Related Crime – A Rapidly Growing Problem." Unpublished manuscript; Main, Geoff and Robson, Brett. *Scoping Identity Fraud.* Attorney-General's Department, Commonwealth of Australia, September, 2001; Smith, Russell G. "Traveling in Cyberspace on a False Passport: Controlling Transnational Identity-related Crime." Paper presented at the British Society of Criminology Conference, Keele, U.K., July 17-20, 2002; Marsden, Chris. Presentation at the NSW Fraud Co-ordination Group's National Fraud Conference, Sydney, August 1, 2001; NSW Registry of Births, Deaths and Marriages. *Fraud Minimization Strategy*, 1992-2002, Internal document; and Office of Strategic Crime Assessments. "The Criminal Exploitation of Identity." Occasional Paper No. 2/00.

[5] General Accounting Office, "Identity Fraud: Information on Prevalence, Cost and Internet Impact is Limited," May, 1998 p.29 (GAO/GCD-98-100BR).

[6] Identity Theft and Assumption Deterrence Act, S. Rep. No. 105-274 at 7 (1998).

[7] GAO, op. cit. p.44.

[8] *Ibid*. 28.

[9] House of Representatives Standing Committee on Economics, Finance and Public Administration, Parliament of the Commonwealth of Australia, *Numbers on the Run*, August, 2000, Canberra, AU.

[10] *Ibid*. Foreword.

[11] *Ibid.* p.65-66.

[12] *Ibid*. p. 67.

[13] See for example, Rosoff, Stephen, Henry Pontell, and Robert Tillman. *Profit Without Honor: White-Collar Crime and the Looting of America* (2nd Edition). Upper-Saddle River NJ: Prentice-Hall, 2002; Calavita, Kitty, Henry Pontell, and Robert Tillman. *Big Money Crime: Fraud and Politics in the Savings and Loan Crisis. Berkeley*: University of California Press, 1997; and Pontell, Henry and David Shichor (Editors). *Contemporary Issues in Crime and Criminal Justice: Essays in Honor of Gilbert Geis*. Upper-Saddle River NJ: Prentice Hall, 2001.

[14] Albert Biderman and Albert J. Reiss, Jr., *Data Sources on White-Collar Law-Breaking* Washington, D.C.: U.S. Gov't Printing Office, 1980

[15] *Associated Press.*"This Time the IRS is Missing Computers." *Los Angeles Times*. August 16,2002. p. A31.

[16] *Ibid.*

[17] *Ibid.*

[18] Marx, Gary T., "Technology and Social Control: The Search for the Illusive Silver Bullet." *International Encyclopedia of the Social and Behavioral Sciences*, 2001. p. 1.

[19] *Ibid.*
[20] *Ibid.*
[21] *Ibid*.
[22] Krebs, Brian. "National Academies Study Tempers Call for National ID." *Newsbytes*. April 11, 2002.
[23] *Ibid.*
[24] *Ibid*.
[25] *Ibid.*
[26] *Ibid.*
[27] Walters, Kath. "Do ATO Staff Know Their Stuff? Newly Hired Officers Are Being Criticised as Unfair, Untrained and Unable to Spot Real Problems." *BRW.* October 10-16, 2002. p. 74-75.
[28] See Marx, Gary T. "Let's Eavesdrop on Managers." *Computerworld*, April 20, 1992.
[29] Marx, Gary T. "Notes on the Discovery, Collection, and Assessment of Dirty Data." In J. Schneider and J. Kitsuse*, Studies in the Sociology of Social Problems*, Ablex, 1984.
[30] See Pontell, Henry. "Deterrence: Theory Versus Practice." *Criminology*, 16 (May, 1978) pp. 3-22; Pontell, Henry. "System Capacity and Criminal Justice: Theoretical and Substantive Considerations," in Harold E. Pepinsky (ed.), *Rethinking Criminology*. Beverly Hills: Sage Publications, 1982, pp. 131-143; Pontell, Henry, Kitty Calavita, and Robert Tillman, "Corporate Crime and Criminal Justice System Capacity: Government Response to Financial Institution Fraud," *Justice Quarterly* 11:3 (September, 1994) pp. 383-410.
31 Dreazen, Yochi J. "Identity Theft as an Inside Job is Increasing." *Wall Street Journal*, July 31, 2002. p. B1.
32 "IRS: Tax Cheats Get Sophisticated." *Associated Press*. September 24, 2002.
[33] *Ibid.*
[34] *Ibid.*
[35] *Ibid.*