Abstract

The digital persona is a model of the individual established through the collection, storage and analysis of data about that person. It is a very useful and even necessary concept for developing an understanding of the behaviour of the new, networked world. This paper introduces the notion, traces its origins and provides examples of its application. It is suggested that an understanding of many aspects of network behaviour will be enabled or enhanced by using the notion.

The digital persona is also a potentially threatening, demeaning, and perhaps socially dangerous phenomenon. One area in which its more threatening aspects require consideration is in data surveillance, the monitoring of people through their data. Data surveillance provides an economically efficient means of exercising control over the behaviour of individuals and societies. The manner in which the digital persona contributes to an understanding of particular dataveillance techniques such as computer matching and profiling is discussed, and risks inherent in monitoring of digital personae are outlined.

Contents

- Introduction
- Introduction to the Digital Persona
- The Passive Digital Persona
- The Active Digital Persona
- Potential Applications
- Dataveillance
- The Digital Persona and Dataveillance
- Computer Matching
- Profiling
- Flaws in the Dataveillance of the Digital Persona
- More Sophisticated Applications of the Digital Persona to Dataveillance
- Implications
- Conclusions
- References

Introduction

The marriage of computing and telecommunications brought us networks. This had led to connections among networks, most importantly the Internet. With the networks has come a new working environment, popularly called 'the net', 'cyberspace' or 'the matrix'. Individuals communicate with others, particularly by addressing electronic messages to one another, and by storing messages which other, previously unknown, people can find and access. For a review of applications of the Internet to the practice of research, see Clarke (1994a).

People exhibit behaviour on the network, which other people recognise. Some of it is based on name; for example someone who uses a pseudonym like 'Blackbeard' creates a different expectation in his readers from someone who identifies themselves using a normal-sounding name like 'Roger Clarke'. Other aspects of the profile of people on the net are based on the promptness, frequency and nature of their contributions, and the style in which they are written.

Over a period of time, the cumulative effect of these signals results in the development of something which approximates 'personality'. It is a restricted form of personality, because the communications medium is generally restricted to standard text; at this early stage of developments, correspondents generally do not see pictures or sketches, or even hand-writing, and do not hear one another's voices. The limitations of the bare 26 letters, 10 digits and supplementary special characters of the ASCII character-set have spawned some embellishments, such the commonly-used 'smiley' symbol :-) , the frowning symbol :-( and the winking :-(. Some variations are of course possible; for example (:-|} could imply a boring, bald person with a beard, and (}&(- the wish:-).
the wink ;-) Some variations are of course possible; for example {:-|} could imply a boring, bald person with a beard, and {&-()} someone with a hangover. Generally, however, the symbol-set is anything but expressively rich. Moreover, its use originated in and is by and large limited to particular net subcultures.

Net-based communications give rise to images of the people involved. These images could be conceptualised in many different ways, such as the individual's data shadow, or his or her alter ego, or as the 'digital individual'. For reasons explained below, the term 'digital persona' has some advantages over the other contenders. This paper's purpose is to introduce and examine the notion of the 'digital persona'.

Introduction to the Digital Persona

In Jungian psychology, the anima is the inner personality, turned towards the unconscious, and the persona is the public personality that is presented to the world. The persona that Jung knew was that based on physical appearance and behaviour. With the increased data-intensity of the second half of the twentieth century, Jung's persona has been supplemented, and to some extent even replaced, by the summation of the data available about an individual.

The digital persona is a construct, i.e. a rich cluster of inter-related concepts and implications. As a working definition, this paper adopts the following meaning:

*the digital persona is a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual.*

The ability to create a persona may be vested in the individual, or in other people or organisations, or in both. The individual has some degree of control over a projected persona, but it is harder to influence imposed personae created by others. Each observer is likely to gather a different set of data about each individual they deal with, and hence to have a different gestalt impression of that person. In any case, the meaning of a digital persona is determined by the receiver based on their own processing rules. Individuals who are aware of the use of data may of course project data selectively, in order to influence the imposed digital persona that is formed (e.g. on arriving in the United States, they may take out an unnecessary loan simply to create a credit record).

It is useful to distinguish between informal digital personae based on human perceptions, and formal digital personae constructed on the basis of accumulations of structured data. The data-intensity of contemporary business and government administration results in vast quantities of data being captured and maintained, and hence considerable opportunity to build formal digital personae. These data range from credit and insurance details, through health, education and welfare, to taxation and licensing. The extent of interchange of data-holdings among organisations is increasing, both concerning groups (e.g. census and other statistical collections) and about identified individuals (e.g. credit reference data and ratings, insurance claims databases, consumer marketing mailing lists, telephone, fax and email address directories, electoral rolls and licence registers).

Later sections of this paper also distinguish between passive, active and autonomous digital personae. A schematic representation of the formal, passive digital persona is at Exhibit 1.

### Exhibit 1: The Passive Digital Persona
There is something innately threatening about a persona, constructed from data, and used as a proxy for the real person. It is reminiscent of the popular image of the voodoo doll, a (mythical) physical or iconic model, used to place a magical curse on a person from a distance. Similar ideas have surfaced in ‘cyberpunk’ science fiction, in which a ‘construct’ is “a hardwired ROM cassette replicating a ... man's [sic] skills, obsessions, knee-jerk responses” (Gibson, 1984, p.97).

Some people may feel that it is demeaning, because it involves an image rather than a reality. Others may regard it as socially dangerous. This is because the person's action is remote from the action's outcome. This frees the individual's behaviour from his or her conscience, and hence undermines the social constraints which keep the peace.

The digital persona offers, on the other hand, some significant potential benefits. Unlike a real human personality, it is digitally sense-able, and can therefore play a role in a network, in real-time, and without the individual being interrupted from their work, play or sleep. Leaving aside the normative questions, the notion has descriptive power: whether we like it or not, digital personae are coming into existence, and we need the construct as an element in our understanding of the emerging network-enhanced world. The following sections investigate the nature of the digital persona, commencing with a simple model, and progressively adding further complexities in order to build up a composite picture of the notion.

The Passive Digital Persona

A digital persona is a model of an individual, and hence a simplified representation of only some aspects of the reality. The efficacy of the model depends on the extent to which it captures those features of the reality which are relevant to the model's use. As with any modelling activity, it suffers the weaknesses of the reductionist approach: individuals are treated not holistically, but as though a relatively simple set of data structures was adequate to represent their pertinent characteristics.

Some aspects of the person's digital persona, and of the transactions which create and maintain it, can be represented by structurable data, such as the times of day when the person is on the net, the frequency and promptness with which he or she communicates, and the topics they discuss. Other aspects are more subjective, and depend on interpretation by message recipients of such factors as the degree of patience or tolerance shown, the steadiness of expression, the appreciation of the views of others, and the consistency of outlook. There is a trade-off between the syntactic consistency with which structured data can be processed, and the semantic depth and tolerance of unusual cases associated with less formal communications.

An individual may choose to use more than one projected digital persona. People may present themselves differently to different individuals or groups on the net; or at different times to the same people; or at the same time to the same people. One projection may reflect and provide close insight into the person's 'real personality', while other personae may exaggerate aspects of the person, add features, omit features, or misrepresent the personality entirely.

Reasons why people may wish to adopt multiple personae include:

- the maintenance of a distinction between multiple roles (e.g. prison warder, psychiatrist or social worker and spouse/parent; employed professional and spokesperson for a professional body; and scout-master and spy);
- the exercise of artistic freedom;
- the experimental stimulation of responses (e.g. the intentional provocation of criminal acts, but also the recent instance of a male impersonating a physically impaired female);
- willing fantasy (as in role-playing in multi-user dungeons and dragons or MUDDs);
- paranoia (i.e. to protect against unidentified and unlikely risks); and
- fraud and other types of criminal behaviour.

There are many instances in which multiple projected personae may be used constructively. In conventional email, recipients may be unaware that multiple user-names are actually projections of the same person, but the sender may thereby feel free to express a variety of ideas, including mutually contradictory ones. Anonymity is particularly useful in alleviating problems associated with power differentials, such as the fear of retribution by one's superiors, or of derision by one's peers.

Even where the mapping of digital personae to person is known to the recipients, the sender's choice of persona enhances the semantic richness of the conversation. In contexts beyond email, the idea has even greater power. In the decision support literature, techniques such as brain-storming and delphi encourage the pooling of know-how and the stimulation of new ideas. The existing choice among comments being anonymous, temporarily anonymous or identified can be supplemented by participation in the event of more personae than people. This enables advantage to be taken of the power and complexity of intellectually prodigious individuals.

**The Active Digital Persona**

In the preceding section, the digital persona has been described as a passive notion, comprising data alone. It is important to relax that simplification. The concept of an 'agent' has been current in computer science circles for some years. This is a process which acts on behalf of the individual, and runs in the individual's workstation and/or elsewhere in the net. A trivial implementation of this idea is the 'vacation' feature in some email servers, which returns a message such as 'I'm away on holidays until <date>' to the senders of messages. (Where the sender is a mailing list, this may result in broadcast of the message to hundreds or thousands of list-members).

More useful applications of projected active digital personae are mail filterers (to intercept incoming mail and sort it into groups and priority sequences), news gatherers (to search newsgroups, bulletin boards and electronic journals and newsletters, in order to identify items of interest to the individual and compile them into personal news-bulletins), and 'knowbots' (to undertake relatively intelligent searches of network sources in order to locate and fetch documents on a nominated topic). For a review of some of these capabilities, see Loch & Terry (1992).

The 'agent' concept derives from two ideas. One is the long-standing, spookily-named 'daemon', i.e. a program which runs permanently in order to perform housekeeping functions (such as noticing the availability of files to be printed, and passing them in an orderly manner to the printer). The other ancestor idea is the 'object', which refers to the combination of data with closely associated processing code. Although this term should be understood in its technical sense, it is unavoidable that people who are fearful of the impacts of ubiquitous networking will draw attention to how the very word underlines the mechanistic dangers inherent in the idea.

The active digital persona has all of the characteristics of the passive: it can be projected by the individual, or imposed by others; and it can be used for good or ill. The difference is in the power which the notion brings with it. It enables individuals to implement filters around themselves, whereby they can cope with the bombardment of data-flows that are increasingly apparent in the networked world. These need not be fixed barriers, because they can self-modify according to feedback provided by the person or compiled from other sources; and they can contain inbuilt serendipity, by letting through occasional lowly-weighted communications, and hence provide the network equivalent of book-shop browsing.

A person's digital behaviour may be monitored (e.g. their access to their mail and the location they accessed it from, and their usage of particular databases or records). This may be done with the agreement of the individual, as a contribution to community welfare and efficiency (see, for example, Hill & Hollan 1994), or without the individual's knowledge or consent, in which case it may be used sympathetically or aggressively.

In extreme case, an active agent may be capable of autonomous behaviour. It may be unrecallable by its originator (as was the case with the Cornell worm). It may, by accident or design, very difficult to trace to its originator. A familiar analogy is to short-duration nuisance telephone and fax calls.

**Public Personae**

Individuals can exercise a degree of control over their projected passive and active personae, but much less influence over those personae imposed by others upon them. Although there are likely to be considerable differences among the various personae...
personae imposed by others upon them. Although there are likely to be considerable differences among the various personae associated with an individual, there are also commonalities. With some individuals, there is so much in common among the images that it is reasonable to abstract a shared or public persona from the many individual personae.

Examples abound of public personae developed through conventional media. The public images of Zsa Zsa Gabor, Elizabeth Taylor, Pierre Trudeau, Donald Trump and Ross Perot are public property. The idea of any of them successfully suing in defamation a person who criticised their public image, on the grounds that this misrepresented their real personality, seems ludicrous. Similar limitations confront personalities of the Internet, such as Cliff Stoll, Peter Neumann, Richard Stallman and Phiber Optik.

A public persona may arise in and be restricted to a particular context. For example, a person's digital shadow may be well-known within an electronic community such as that associated with a mailing list or bulletin board. Archetypal public personae include the inveterate sender of worn-out jokes and clichés, the practical joker, the sucker who always takes practical jokers' bait, the 'wild idea' generator, the moral crusader, and the steadying influence who calls for calm and propriety when the going gets rough.

With the immediacy of the net, many people play these roles without the realisation that they are predictable. But they can be adopted quite conscientiously and constructively, e.g. where a respected persona reinforces the need for appropriate behaviour, and conversely, where a normally placid respondent replies vigorously, implying that their patience is stretched to the limit. In such contexts, there is once again no reason why an individual should be restricted to a single public persona.

**Potential Applications**

There is a range of uses to which an individual might put projected, passive digital personae. It may simply be to express their personality, or a facet of it, or an exaggeration of some feature of it, or a feature that the person would like to have. It may be a desire to free themselves of normal constraints, in order to express different thoughts or the same thoughts differently. There is the well-known activity of 'flaming' on the net, in which people express themselves to others with a vigour that would be socially and perhaps physically risky if done on a face-to-face basis. The freedom to project a digital persona can be used creatively, constructively, entertainingly, interpersonally, in a defamatory manner, or criminally.

Projected, active digital personae are, on the other hand, a relatively recent development, and it is too early to be able to appreciate and analyse the scope of the potential applications. There is no reason, however, why an agent has to run on one's own workstation, nor be limited to input-filtering; for example, so-called 'program trading' agents can issue buy/sell orders if the price of nominated commodities fall/rose beyond a nominated (or computed) threshold; and updates to key records in remotely-maintained statistical databases can be monitored. It is also possible to conceive of the 'active' role being extended to, for example, conducting a nuisance campaign against an opponent, by bombarding their email and/or fax letter-box; or countering such a campaign which has been directed against oneself.

Passive digital personae may be imposed by other individuals and organisations for a variety of reasons. Typical among these is the construction of a consumer profile, in order to judge whether or not to promote the sale of goods, services or ideas to each particular individual, and if so, then to indicate the suitability of each a palette of promotional media and devices should be used.

Similarly, imposed, active digital personae offer considerable prospects. People's interests or proclivities could be inferred from their recent actions, and appropriate goods or services offered to them by the supplier's computer program using program-selected promotional means. Another application might be a network 'help desk’ program to detect weak or inefficient database search strategies, and offer advice as a service to network users. A network control mechanism could provide warnings to subscribers when they use foul language, or exceed traffic or storage quotas. As with other forms of monitoring of the workplace and the public, questions of law, of contract, of image and of morality arise.

Afficionados of science fiction are aware of ample sources of inspiration for more futuristic uses of the concept. In John Brunner's 'The Shockwave Rider' (1974), personae are used primarily by the State as an instrument of repression, but secondarily also by the few individuals capable of turning features of the net against the ruling clique, as a means of liberation. In 'cyberpunk' literature, people adopt pre-programmed personae in a manner analogous to their usage of psychotropic drugs (see, in particular, Gibson's 'Neuromancer', 1984; and the collection of short stories edited by Sterling, 1986). In Bear's 'Eon' (1985), digital personae have become so comprehensive that they are routinely detached from individuals: disembodied 'partials' are created to perform specific tasks on their owners' behalf, and 'ghosts' of biologically dead people are rejuvenated from the city databank.

As with all imaginative fiction, plugging into the net, partials and ghosts should not be understood as predictions, but as investigations of extreme cases of contemporary ideas, as speculations of what might be, and as inspiration for more practicable, restricted applications. As 'virtual reality' graduates from the laboratory, the digital persona idea will doubtless be embodied in some of its applications.
In order to provide a deeper appreciation of the power of the digital persona, the remaining sections of the paper investigate its application to one specific area: the monitoring of people.

**Dataveillance**

Dataveillance is usefuly abbreviated to dataveillance, is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons. In the past, the monitoring of people's behaviour involved physical means, such as guards atop observation towers adjacent to prison-yards. In recent decades, various forms of enhancement of physical surveillance have become available, such as telescopes, cameras, telephoto lenses, audio-recording and directional microphones. In addition, electronic surveillance has emerged in its own right, in such forms as telephone bugging devices and the interception and analysis of telex traffic.

Dataveillance differs from physical and electronic surveillance in that it involves monitoring not of individuals and their actions, but of data about them. Two classes need to be distinguished:

- **personal dataveillance**, in which a previously identified person is monitored, generally for a specific reason; and
- **mass dataveillance**, which is of groups of people, generally to identify individuals of interest to the surveillance organisation.

Dataveillance is much cheaper than conventional physical and electronic surveillance. The expense involved in physical and even electronic monitoring of the populace acted as a constraint on the extent of use. This important natural control has been undermined by the application of information technology to the monitoring of data about large populations. The development is perceived by philosophers and sociologists as very threatening to freedom and democracy.

The increasing information intensity of modern administrative practices has been well described by Rule (1974, 1980). Foucault (1975) used the concept of the 'panopticon' to argue that a prison mentality is emerging in contemporary societies. Smith (1974 et seq), Laudon (1986b), OTA (1986) and Flaherty (1989) deal with dataveillance generally. The role of information technology in dataveillance is discussed in detail in Clarke (1988). A political history of dataveillance measures in one country are in Clarke (1987, 1992a).

**The Digital Persona and Dataveillance**

To be useful for social control, data must be able to be related to a specific, locatable human being. Organisations which pursue relationships with individuals generally establish an identifier for each client, store it on a master file and contrive to have it recorded on transactions with, or relating to, the client. The role of human identity and identification in record systems is little-discussed, even in the information systems literature (see, however, Clarke 1989).

The notion of the digital persona is valuable in understanding the process of dataveillance. The data which is monitored is implicitly assumed by the monitoring organisation to provide a model of the individual which is accurate in all material respects. Organisations' data collections typically comprise basic data provided by clients at the time the relationship with the organisation is established, supplemented by data arising as a byproduct of transactions between them. This gives rise to a digital persona which is far from complete, but generally adequate for the purposes implied by the relationship. Secondary uses not contemplated within that relationship result in greater risk of misinterpretation of the limited model inherent in the data, e.g. through misunderstanding of the varied meanings of such data-items as marital status, number of dependants and income.

The following two sections discuss the role of the digital persona in two particular dataveillance techniques which involve secondary use of data, and which transcend organisational boundaries.

**Computer Matching**

Computer matching is a computer-supported process in which personal data records relating to many people are compared in order to identify cases of interest. Since it became economically feasible in the early 1970s, the technique has been progressively developed, and is now widely used, particularly in government administration and particularly in the United States, Canada, Australia and New Zealand. A description and analysis are in Clarke (1992b, pp.24-41). See Exhibit 2 for an overview of the process.

Computer matching brings together data which would otherwise be isolated. It has the capacity to assist in the detection of error, abuse and fraud in large-scale systems (Clarke 1992b, pp.41-46). It may, in the process, jeopardise the information privacy of everyone whose data is involved, and even significantly alter the balance of power between consumers and corporations (see Larsen 1992, Gandy 1993), and citizens and the State (see Rule 1974, Laudon 1986). Of particular concern is the extent to which the digital persona which arises from the matching process may be a misleading image of the individual and their behaviour.

---

and their behaviour.

There are three means whereby a digital persona can be constructed from multiple sources:

- a common identifier;
- correlation among multiple identifiers; and
- multi-attributive matching.

Virtually all computer matching undertaken by agencies of the U.S. Federal Government appears to be based on a common identifier, the Social Security Number or SSN (Clarke 1993, pp.9-19). In Canada the Social Insurance Number (SIN) plays a similar role. In European countries it has been the practice for many years for a single identifier to be used for a limited range of purposes, in particular taxation, social security, health insurance and national superannuation. In Australia, an originally single-purpose identifier (the Tax File Number) has recently been appropriated to serve as a social security identifier as well (Clarke 1992a). These codes are used because they are widely available, and their integrity is regarded by the agencies concerned as being adequate. Some agencies, in order to address acknowledged quality problems, use additional data-items to confirm matches.

Exhibit 2: The Computer Matching Process

There are alternatives to a government-assigned number. Physiologically-based identifiers (sometimes referred to as 'positive' identifiers) have the advantage of being more reliably relatable to the person concerned. Many forms have been proposed.

identifiers) have the advantage of being more reliably relatable to the person concerned. Many forms have been proposed, including thumbprint, fingerprints, voiceprints, retinal prints and earlobe capillary patterns. There is also the possibility of a non-natural identifier being imposed on people, such as the brands and implanted chips already used on animals, the collars on pets, and the anklets on prisoners on day-release schemes and on institutionalised patients.

Where a single common identifier is not available, two or more organisations can establish cross-references between or among separate identifiers. This can be achieved by the supply by each individual of their identifier under one scheme to the operator of one or more other schemes. This may be mandated by law, or sanctioned under law (i.e. not prohibited) and required under contract (which if applied consistently by all operators in an industry such as credit or insurance is tantamount to mandating).

An alternative approach is to construct a matching algorithm based on pairs of similarly-defined fields. Typically this involves names, date-of-birth, some component(s) of address and any available identifiers (such as drivers' licence number). Data collection, validation, storage and transmission practices are such that dependence on equality of content of such fields is impracticable (Laudon 1986a). Instead, the data generally needs to be re-formatted and massaged (‘scrubbed’) and/or algorithms devised to identify similarity.

Considerable progress has been made in supporting technologies for multi-attributive matching, including sophisticated algorithms, high-speed processors, storage, vector- and array-processing, associative processing (such as CAFS) and software development tools expressly designed to enable multi-attributive matching (such as INDEPOL) (Clarke 1992b, pp.39-40).

Profiling

Profiling is another dataveillance technique which is attracting increasing usage. A set of characteristics of a particular class of person is inferred from past experience, and data-holdings are then searched for digital personae with a close fit to that set of characteristics. The steps in the profiling process can be abstracted as shown in Exhibit 3.

Profiling is used by government agencies to construct models of classes of person in whom they are interested, such as terrorists, drug couriers, persons likely to commit crimes of violence, tax evaders, social welfare frauds, adolescents likely to commit suicide, and children with special gifts. It is also used by corporations, particularly to identify consumers likely to be susceptible to offers of goods or services, but also staff-members and job-applicants relevant to vacant positions (Clarke 1993).

Exhibit 3: Steps in the Profiling Process

- describe the class of person sought
- use existing experience to define a profile of that class of person
- express the profile formally
- acquire data concerning a relevant population
- search the data for digital personae whose characteristics comply with the profile
- take action in relation to those individuals

Flaws in the Dataveillance of the Digital Persona

There are substantial weaknesses in the digital persona used in computer matching and profiling. These arise in respect of the identification basis used, and the data and processing characteristics.

As regards human identification schemes, the deficiencies of universal schemes such as the SSN as a basis for digital identification have been well-documented (FACFI 1976, Clarke 1989, Hibbert 1992). All such identifiers depend on a seed document, most commonly a birth certificate. Such documents generally have no direct association with the persons to whose birth they attest. They are therefore capable of appropriation by multiple people as a nominal basis for identities. Other documentary evidence of identity (driver's licence, passport, credit card, club membership, etc.) derive from the primary document and from one another.

Such a pattern of inter-locking documents is therefore a highly insecure means of identifying people, especially where they have incentives to avoid identification, or to otherwise mislead. Yet this is the dominant means of identification used in administrative systems, and people act as though it were reliable, as attested to by the prevalence of the term 'proof of identity' to refer to documents. As a result of the unreliability of identification, it is inevitable that, in respect of some proportion of the data subjects, matching creates pseudo-personae, which purport to relate to a specific individual, but may be a composite of several.

In relation to data and process quality, Neumann (1976-) has catalogued manifold problems. An analysis in Clarke (1992b, pp.52-61) distinguishes a number of different areas in which problems arise, and is reproduced in Exhibit 4.

The composite digital persona that computer matching produces comprises data from different sources, gathered and processed in different ways. Flaws in this assembly of data can lead to pseudo-personae and other distortions.
maintained for different purposes. The definitions of such apparently common data-items as marital status, number of dependants and income vary a great deal among the various government agencies and private sector corporations that use them.

**Exhibit 4: Areas in which Data and Process Quality Problems Arise**

- data sources
- data meaning
- data quality
- data sensitivity and privileges
- matching quality
- context
- oppressive use of the results

In addition to definitional problems, the care taken to assure quality of data reflects the circumstances of use. This applies to the precision of the data, its completeness, and the extent to which it is amended to reflect change. Substantial efforts are necessary to control quality, and ensure comparability of multi-sourced items. In the absence of adequate controls, the composite image is a melange, and drawing inferences from the pooled data is fraught with risks. Who bears the risks depends on the circumstances. In some cases, the agency or corporation makes many mistakes and expends significantly greater resources than it anticipated. In others, the individual suffers, through delays, confusion and denial of services.

Profiling may be based on data arising from matching procedures, in which case it is subject to the same risks. Alternatively, it may be undertaken on the basis of the holdings of a single personal data system, in which case a greater degree of confidence in the data quality may be justifiable. Even here, however, risks arise. The model against which the data is compared is derived from the experience of specialists, and reflects their biases. It also involves trade-offs between different factors which may be understood by the designers but not by the users. The result is that atypical, idiosyncratic and eccentric people, and extenuating circumstances, tend not to be catered for. Inferences are readily drawn that with careful review may be quite unreasonable. The first risk is that organisations may invest far too much effort in cases which provide them with no benefits; the second and much more serious risk is that individuals may be subjected to unreasonable treatment, and face significant difficulties in even understanding what is happening to them, let alone coping with the difficulties.

**More Sophisticated Applications of the Digital Persona to Dataveillance**

Beyond computer matching and profiling, there are many further ways in which the digital persona can be applied. In a networked world, individuals' behaviour can be monitored, and their attitudes inferred, on the basis of what they do on the net. The data-sources they access, the individuals they communicate with, and the contents of their messages will be of considerable interest to many organisations, ranging from law enforcement agencies to consumer marketing companies.

Some individuals are seeking ways to confound the attempts to monitor them, through, for example, message encryption and the adoption of multiple identities. Law enforcement agencies, meanwhile, are seeking to preclude the deployment of encryption tools other than those which they can crack, and will doubtless seek legal limitations on the freedom of individuals to express themselves through multiple network personae. When that fails, it is reasonable to expect that they will invest considerable sums in technology to establish and maintain mappings of personae onto persons. In the normal manner of things, the mere exercise of the freedom may be treated as sufficient cause for the person to be subjected to a higher than normal level of surveillance. Another plausible approach would be to match multiple personae, in order to generate suspicions of error, misdemeanour or crime.

There is evidence that real-time monitoring of electronic transactions is already being undertaken; for example, in 1989 an extortionist in the United Kingdom was arrested at an automated teller machine (ATM) while withdrawing money from an account into which the proceeds of his crime had been paid. He had made a succession of withdrawals from ATMs throughout the country, and this was the first occasion on which he had used that particular machine. The most likely means whereby the arrest could have been effected was through monitoring of all transactions at ATMs for the use of a particular card, with immediate communication to police on the beat. As with any privacy-intrusive technique, the first use is unarguably in the public interest. Regrettably, there must be considerable doubt about whether it will be subsequently constrained to such universally acceptable uses.

Profiles or templates of sought-after classes of people can be assembled, and databases of persona behaviour compared with them in order to identify potential terrorists, drug-runners, hackers and suicide-prone adolescents. Until now, this has been done occasionally, on the basis of existing data-holdings. The scope now exists for it to be done in real-time, with not only suspicious individual transactions being sought, but also the accumulation of transactions being monitored for suspicious combinations.

In the marketing arena, the promotion of goods, services and ideas could be automated. Active agents operating on behalf of
organisations could contain profiles, monitor transactions, recognise opportunities and initiate contact. Law enforcement agencies could extend beyond mere dataveillance to automated actions, such as pre-programmed warnings to individuals who were approaching the boundaries of the law, or even directly-implemented punishment, such as the levying of fines directly against the infringer's bank account, or the suspension of network privileges. There may be some circumstances in which such uses might be considered inappropriate, and many in which controls would be essential; but none of them would appear to be repugnant in their own right, and all of them seem likely to be put to use in some circumstances.

There are many further potential applications which are less salubrious; for example, the increased visibility of people's habits and movements creates opportunities for thieves seeking to enter premises when they are unattended, and for extortionists, kidnappers and assassins to be in the right place at the right time to perform their deed with a minimum of risk to themselves. False data can be infiltrated into the network, with the intent of rendering a digital persona misleading. This might be done by individuals seeking to escape detection, or to be interpreted as falling into some particular category. It might alternatively be done by some other person or organisation seeking to assist, or to harm, the individual concerned.

Implications

Broader social impacts of dataveillance are identified and discussed in Clarke (1988), as shown in Exhibit 5. See also Rule (1974), Laudon (1986b) and Flaherty (1989). Clearly, many of these concerns are diffuse. On the other hand, there is a critical economic difference between conventional forms of surveillance and dataveillance. Physical surveillance is expensive because it requires the application of considerable resources. With a few exceptions (such as Romania, East Germany under the Stasi, and China during its more extreme phases), this expense has been sufficient to restrict the use of surveillance. Admittedly the selection criteria used by surveillance agencies have not always accorded with what the citizenry might have preferred, but at least its extent was limited. The effect was that in most countries the abuses affected particular individuals who had attracted the attention of the State, but were not so pervasive that artistic and political freedoms were widely constrained.

Dataveillance changes all that. It is relatively very inexpensive, and getting cheaper all the time thanks to progress in information technology. The economic limitations are overcome, and the digital persona can be monitored with thoroughness and frequency, and surveillance extended to whole populations. To date, particular populations have attracted the bulk of the attention, because the State already possessed substantial data-holdings about them, viz. social welfare recipients, and employees of the State. Now that the techniques have been refined, they are being pressed into more general usage, in the private as well as the public sector.

The primary focus of government matching programmes has been 'evildoers'. This is not intended in a sarcastic or cynical sense - the media releases do indeed play on the heartstrings, but the fact is that publicly known matching programmes have been mostly aimed at classes of individual who are abusing a government programme, and thereby denying more needy individuals of the benefits of a limited pool of resources. Nonetheless, these programmes have a 'chilling effect' on the population they monitor. Moreover, they have educated many employees in techniques which are capable of much more general application.

Conclusions

In basing its analysis on models and their incompletenesses, this paper has adopted a 'materialist' ontological perspective, and a 'critical realism' standpoint. Alternative philosophical standpoints might lead to a rather different analysis, but this paper has argued that widespread networking is bringing with it many new developments. The ability for individuals to project one or more models of themselves outwards, and for individuals and organisations to impose digital personae upon others has the potential to create valuable new opportunities, and to impinge upon established and important values.

Exhibit 5: Social Impacts of Dataveillance

- personal dataveillance
  - low data quality decisions
  - lack of subject knowledge of, and consent to, data flows
  - blacklisting
  - denial of redemption
- mass dataveillance
  - dangers to the individual
    - arbitrariness
    - acontextual data merger
    - complexity and incomprehensibility of data
    - witch hunts
    - ex-ante discrimination and guilt prediction
    - selective advertising
Application and articulation of the idea should enable the descriptive and explanatory power of models of network behaviour to be enhanced. After the coming period of turbulence, it should play a role in improving the predictive power of those models.

The digital persona raises questions about the appropriateness of various legal notions. Inter-networking exacerbates the already apparent inadequacies of privacy, data protection and intellectual property laws. The tort of appropriation provides qualified protection to Elvis Presley's heirs and Madonna against profit-making based on those public personae; but in the networked world it may be less able to protect people from having actions and utterance of others attributed to them.

Dataveillance is an inevitable outcome of the data-intensity of contemporary administrative practices. The physical persona is progressively being replaced by the digital persona as the basis for social control by governments, and for consumer marketing by corporations. Even from the strictly social control and business efficiency perspectives, substantial flaws exist in this approach. In addition, major risks to individuals and society arise.

If information technology continues unfettered, then use of the digital persona will inevitably result in impacts on individuals which are inequitable and oppressive, and in impacts on society which are repressive. European, North American and Australasian legal systems have been highly permissive of the development of inequitable, oppressive and repressive information technologies. Focussed research is needed to assess the extent to which regulation will be sufficient to prevent and/or cope with these threats. If the risks are manageable, then effective lobbying of legislatures will be necessary to ensure appropriate regulatory measures and mechanisms are imposed. If the risks are not manageable, then information technologists will be left contemplating a genie and an empty bottle.

References


Brunner J. (1975) 'The Shockwave Rider' Methuen, 1975


Hibbert C. (1992) 'What To Do When They Ask You for Your SSN' Comp. Prof'l for Social Resp., various electronic versions


Laudon K.C. (1986a) 'Data Quality and Due Process in Large Interorganisational Record Systems' Commun. ACM 29,1 (Jan 1986) 4-11


Neumann P. (1976 -) 'RISKS Forum', Software Engineering Notes since 1,1 (1976), and in Risks.Forum on UseNet


Navigation

Go to Roger's Home Page

Go to the contents-page for this segment.

Send an email to Roger

Last Amended: 12 October 1996