Public Interests on the Electronic Frontier Their Relevance to Policy-Formation for IT Security Techniques

Roger Clarke

Abstract

This paper identifies and discusses some key freedoms that are important in the information society. IT security is demonstrated to be both protective of, and threatening to, these freedoms.

Because new IT security techniques are bringing about major change, are likely to have significant impacts, and may have significant second-order effects, it is inevitable that changes in the law will be necessary. Policy-makers therefore need to develop a strong understanding of the techniques.

In addition, the policy-formation process needs to be informed about the diversity of impacts and effects, and the concerns of the various interested parties. That in turn implies broad, public consultation processes.

Contents

Introduction

The idea of 'security' generates many different emotions in people, depending on the context in which it is used. For example, security can imply warmth and comfort, particularly if it is associated with children or the home; it can invoke images of locks, bank-vaults and barbed-wire; and when qualified by 'national', it can excite feelings of patriotism, xenophobia, distrust of left-wing zealots, and distrust of right-wing zealots, all at once.

The subject of this Conference, IT Security, inherits all of the multi-facetedness of the word 'security'; and, on top of that, it is highly dynamic. New information technologies are rapidly begetting new needs, and IT security techniques are being rapidly invented and innovated in order to address those needs. These techniques have implications for many different kinds of people and organisations.

Laws are used as a means of expressing the balance-points among the various interests, in such a manner that an arbiter can decide the difficult boundary-cases. The new IT security techniques require changes in laws, to facilitate their exploitation, and to regulate their use.

Changes in laws are a matter of public policy. The purpose of this paper is to examine some important aspects of the context within which policy formation about new security techniques is taking place.

When public interests are discussed, many people like to talk in terms of human rights. There are claims that some rights are innate, and that some are absolutely necessary, and more important than other interests. Appendix 1 provides a checklist of the broad human rights area. For an examination of rights in cyberspace, see Clarke (1995e), and the associated references.

Rather than asserting rights, this paper has taken the gentler approach of identifying interests that people have in various freedoms. It confronts the difficulty that, in relation to many of these freedoms, security is a pre-condition; but it is also a threat.

The paper commences with a brief review of some of the new IT security techniques. It then examines a series of freedoms that people are interested in. The conclusions are drawn that the policy-formulation process must be well-informed, not only about the new IT security techniques, and the risks they address, but also about the many freedoms that people are seeking to protect, and the varying perspectives of the many different stakeholders.

Background

The imminent explosion in electronic commerce and electronic services delivery has created the need for ways of keeping participants' risk exposure within bounds. This is best addressed

through authentication, which takes various forms, appropriate to different circumstances. These include:

- value authentication, to provide assurance that the consideration proffered by the other party measures up to expectations.

  'Consideration' includes cash; payment instructions; promises of delivery of physical goods or performance of physical services; and the delivery of digital goods or the performance of digital services;

- eligibility authentication, to provide assurance that people claiming a particular capability actually have it. Examples of settings in which this is applicable include the signing of contracts; the application of advantageous tariffs and discounts; and the granting of concessions; and

- person authentication (often referred to as 'user authentication'), to ensure that a person is who they claim themselves to be. This is necessary for some classes of transactions, in particular those that only the person in question should be permitted to perform (such as access to personal data), and those that necessarily involve an ongoing relationship between the parties (such as health care, and the advancing of credit).

During the last decade or so, advances in information technology have presented a substantial set of new opportunities, and challenges. Some that are relevant to the present discussion are:

- cryptography (for a primer, see Clarke 1996), including:
  - asymmetric cryptography;
  - digital signatures, certificates and certification authorities;
- secret-sharing;
  - key escrow; and
  - key-cracking initiatives using virtual farms of workstations;
- surveillance techologies (for a primer, see Clarke 1988), including:
  - biometric identifiers (for a primer, see Clarke 1995a);
  - front-end verification, data-matching and profiling;
  - identifier-based; and
  - pattern-based; and
- intrusion and counter-intrusion technologies, including:
  - viruses and worms;
  - JavaScript, cookies and Java applets; and
  - firewalls.

Policy-makers need to act in relation to modern security technologies. In doing so, they need to appreciate that a range of different interests exists, and to seek a balance among them. The following section identifies some of these important interests.

Freedoms

Some years ago, I developed a set of mini-cases of what I referred to as 'dysfunctional behaviour' on the Internet. One of the most interesting aspects of the discussions that were stimulated by that document were disputes as to whether the behaviours really were dysfunctional; for example, 'anonymous remailers' are 'a bad thing' (because they enable people to avoid taking responsibility for their statements); but also 'a good thing' (because they protect whistle-blowers, and hence ensure that 'truth will out').

The body of this paper examines a series of 'freedoms' that people are interested in. It draws out the inherent tensions that exist between people with different world-views, and even between different roles of the same individual: IT security is generally found not on one, but on both, sides of each discussion.

Freedom to communicate in ways that preclude interception

It is a hallmark of civilisation that people have a considerable degree of freedom to say what they think, without living in fear of reprisals from powerful individuals and institutions. Americans have this embedded in their constitution, and set great store by it; and their attitudes permeate the Internet. In practice, there are constraints on freedom of speech, in the form of laws relating to defamation, negligent mis-statement, deceptive conduct, confidence, censorship, and a wide range of other rules and regulations.

Closely associated with this is the freedom to 'speak' without being able to be 'overheard'. Conversations are often held such that overhearing is difficult, eg in a closed office, in noisy surroundings, or in the middle of a large open space where eavesdroppers would be obvious. Mail interception and telephone monitoring are illegal, except in very particular circumstances. Reflecting the expectation of security of communications, netizens demand the freedom to use 'strong' encryption to ensure that their net-based communications are not intercepted or monitored.

In the name of security, government agencies responsible for law enforcement and national security seek, and in some cases have actually achieved, the technical and legal capability to compromise the freedom to communicate without interception. Telephone calls may be tapped. Moreover, new carrier technologies are required to be interceptible; for example, the implementation of GSM digital telephony in Australia was delayed because of the strength of the encryption used, and the lack of a 'trap-door' to enable interception.

The US National Security Agency, in an unsustainable attempt to retain its cold-war dominance over the White House, continues to fight for the outlawing of encryption techniques that it cannot crack. There has, however, been no apparent attempt by Australian law enforcement and

national security agencies to have such controls applied to the use of cryptography in this country.

Freedom to conduct most transactions anonymously

Consumer marketing organisations are greeting Internet-based electronic commerce with enthusiasm. Current examples of rampant commercialism include:

- email addresses are perceived as public property, and used for unsolicited communications, commonly known as 'spam';
- e-lists are being treated as channels for unsolicited promotional materials;
- cookies are being appropriated to the task of gathering information about web-surfers' interests and style into consumer profiles;
- data about individuals is being merged with geodemographics; and
- the user-pull configuration of the world-wide web is being subverted, and adapted towards a push-technology.

Small wonder, then, that people are actively seeking countermeasures against invasive applications of net-technology.

Some of these countermeasures are as direct and aggressive as the behaviour of the marketer. Others seek to deny information to the privacy-invader, in particular by not providing an identifier. Security specialists have mixed feelings about this approach: on the one hand, investigations are made much more difficult if transaction trails are obscured; and on the other, denial of information is one of the fundamental tenets of security practice.

Freedom to conduct most other transactions pseudonymously

There are cases where anonymity precludes achievement of the objectives of either or both of the parties to a transaction. This does not, however, necessarily mean that such transactions have to be openly identified. Pseudonymous techniques can be applied, most commonly through the use of an indirect or 'pseudo-identifier', whose relationship to an individual is protected through technical, procedural and legal mechanisms. This prevents casual discovery of the identity of the person or persons concerned; but enables the security interests of the individual to be compromised by higher-order security interests, subject to control mechanisms.

An analysis of the concepts of identified, anonymous and pseudonymous transactions, and of the means of achieving balance between the interests of the various parties, is to be found in Clarke (1995b and 1996g).

Freedom from demeaning identification rites

After the scope for using anonymity and pseudonymity has been exhausted, there remain circumstances in which transactions need to be identified. Such situations include where the transaction is one episode in a long-standing relationship; where the data already held about the person is relevant to the current transaction; and/or where the person has an interest in misrepresenting their circumstances, and the identity is needed as a means of exercising control over that risk.

People have an interest in not being subjected to procedures that de-value their humanness. For people from some cultures or with particular religious beliefs, photographs that show the person's facial features are uncomfortable, or worse. Fingerprints have always been associated with suspicion of criminality. For many people, giving up samples of body fluids or tissue is at least unpleasant and even downright degrading. All forms of imposition of artificial identifiers (such as tattoos, anklets and micro-chips) represent the express denial of difference between humanity and items on a production-line.

This interest in what might reasonably be termed 'the security of the person' is in direct conflict with broader interests in 'public security'. People visiting prisoners in gaols in N.S.W. are now expected to submit to such indignities. Hand geometry and retinal patterns are in use in a variety of access-control settings. There are occasional proposals to apply fingerprinting beyond the field of criminal investigation. Despite the enormous complexities it involves, DNA testing is being crept into the mainstream.

Because of their substantial and intrusive impact, biometrics should be used sparingly, and only where economically and socially justified, taking into account all of the various interests involved.

Even where biometrics are not involved, people are confronted with challenges to produce documents. The so-called '100-point' scheme, originally developed in the context of the issue of passports, has been extended by law into the banking sector, and is showing signs of being applied in further areas. Despite the fact that there is no such thing as 'proof of identity', documentary evidence is treated as though it were proof; and lack of such evidence is, by inference, disproof of identity. People who have difficulty producing such documents are marginalised (in many cases, further marginalised), and humiliated.

These matters are examined at length in Clarke 1995a.

Freedom from centralised storage of identification details

Where biometrics is used, a further design consideration is of great importance. If the 'measure of a person' is under the control of that person alone, then the extent of the threat to the person's humanity is diminished.

Individuals can retain control over their biometric measures through its capture onto a chip that they carry, provided that it is stored in no other location, or at least only in other locations that are secured by the person's private key. Authentication of the person would then be conducted by a device that takes a measure of the person presenting themselves, and compares it with the measure pre-stored on the chip; and

that keeps no record other than that the two measures were sufficiently consistent that the person was accepted as being the one associated with the identifier stored on the chip.

Such procedures may seem complex to someone who is focusing simply on the public security interest (such as a Police Minister or a Corrective Services Minister). It can be confidently anticipated that law enforcement and national security interests will conceive of schemes that embody an Australia-Card-style register (Clarke 1987) containing not merely personal data and a unique identifier, but also biometrics of suspect segments of the population.

Freedom to adopt multiple identities to reflect multiple roles

To people brought up on a diet of law enforcement, national security, or even just too many crime-novels, terms like 'multiple identities', 'aliases' and 'aka's' (also-known-as) seem to directly imply criminality.

The simple fact is that many people have multiple identities, and most of them do not have criminal intent. Artists present many faces, and may have a nom de plume associated with each of them. People in security-sensitive roles (there's that word again), such as prison-warders and staff in psychiatric hospitals, live in the suburbs under different names from those that they use at work. Professional women may sustain their maiden name, or a prior married name. People who have abandoned a life of crime change their names. Whistle-blowers (who, for example, pass on evidence of unlawful, unreasonable or hypocritical behaviour by their employer) are well-advised to do so under an assumed name.

The State is a major peddler in multiple identities. Law enforcement and national security operatives use them in order to protect themselves from likely physical harm. Protected witness schemes depend on them. A related matter is the issue by the Passports Office, under particular circumstances, of duplicate official passports.

A further consideration is that individuals play multiple roles, and have varying competencies depending on which role they are playing at the time. For example, a company employee may have company as well as personal credit-cards; and the same individual may be capable of signing cheques, or committing to contract, a company, and one or more associations, as well as themselves and their spouse.

In the face of realities like these, automatic responses by authorities to the effect that multiple identities should not be countenanced, ring hollow, and are ineffective. Of course people with criminal intent abuse multiple identities. But, for very good reasons, the law does not render criminal the act of having multiple identities, or even of misrepresenting one's identity.

The complexities of the information society and the information economy make it essential that people be recognised as having multiple identities. The Australian Taxation Office, for example, should already cope with multiple Tax File Numbers registered as being associated with one another, and relating to a single taxpayer.

Trust based on networks, not on government-imposed hierarchies

One view of the world perceives all authority as emanating from above. Diagrams of social governance originating in Eastern European countries, for example, are a simple hierarchy, with an ultimate authority (although words like 'king' seldom appear any more).

Social governance in democracies, on the other hand, is circular. Parliaments, governments and the court system are subject to constitutional and electoral control mechanisms. Indeed, the more mature models include not just a loop from the nominally top-end societal institutions back to 'the people', but also cross-checks within the system. These include tribunals, ombudsmen, advocacy groups (industry, professional and consumer associations, and special interest groups), and the media.

The current draft Public Key Authentication Framework (PKAF) subscribes to the hierarchical notion that there is a font of all trust, prosaically referred to as a Root Authority. In the information society and information economy, the practice is more likely to be that certificate authorities will cross-certify one another, generating trust through a network of information, rather than depending on the old-fashioned presumption that there is an ultimate authority.

Freedom from appropriation of identity

On the net, as the saying goes, "no-one knows you're a dog". But the inverse also holds: no-one knows if you're a person pretending to be a dog, because the absence of any inbuilt authentication mechanism means that anyone can purport to be anyone else.

This is upsetting to many netizens, but in fact it parallels real life, where similar difficulties arise when people pretend to be other people, or forge signatures. Beyond being psychologically unsettling, the inability to be sure who one is communicating with will inhibit some kinds of transactions, in both electronic commerce and electronic service delivery settings.

A practical solution may be to leave the majority of communications unauthenticated, and therefore unreliable as to their source; but to create an additional class of communications, used only in circumstances where authentication of the originator is of consequence. Digital signatures appear to be capable of providing varying degrees of confidence in the origin of a message, depending on the design of the certification scheme, the certificates that are available, and the set of brand-names on the certificates.

Freedom from cancellation of identity

Anti-utopian literature contains vivid examples of concern about a person being denied their identity by the State. Examples include '1984' (which used the notion of an 'unperson'), and sci-fi author John Brunner's 'The

Shockwave Rider'.

In pre-information societies, denying a person their identity would have been very difficult, because one's identity derived from many sources, both formal and informal. One interpretation of the information society involves a register of citizens, biometrics, irrefutable evidence of identity, and efficient, production-line-inspired case-management. If this dream were to be achieved, security would exist at a public level, but there would be no private sphere left within which the concept of security could be applied at an individual level.

A more likely path than that kind of dystopia is ongoing tension between aspirants to such a society, and people who value the unstructuredness, unplannedness and diversity that are part and parcel of humanity.

Freedom to hide

Finally, it is vital that an uncomfortable fact be confronted. People want to retain a private space; and sometimes they want that space to be sufficiently large that they can get lost in it.

Some instances of a person 'getting lost' involve psychological instability, and the mainstream view is that such people are in need of treatment. Some instances are criminal, or at least financially irresponsible, eg people who 'start a new life' in a far-flung location in order to avoid the consequences of crime, or the need to keep paying for the ex-wife and the kids (in practice most such people are male).

Meanwhile, some are normal people who are overwhelmed by current circumstances, and just 'need a break'. And others are 'celebrities' who need protection from their fans; and still others are 'stirrers' who've stirred up a bigger hornet's nest than they expected, and need protection from a fatwa, or its equivalent in other cultural terms.

The same features of a society that will protect the security of 'good' individuals can be exploited to protect 'bad' ones. And the same 'security' measures needed to protect society from 'bad' people impose themselves in equal measure on 'good' ones. There are no simple answers; every decision about appropriate security measures is an exercise in balance.

Conclusions

Security is multi-headed, in that it nurtures freedoms, and it also threatens them. Policy-formation processes must reflect these complexities. Approaches must be constructed that balance both the direct impacts and the second-order effects on the various interests.

That in turn implies that the people involved in policy-making processes must be technically well-informed, and must also represent the various stakeholders who have an interest in the outcome. The making of new policy and law about IT security is a public matter, not one that can be conducted within clubs, behind closed doors.

Appendix 1: The Victorian Council for Civil Liberties' Draft Bill of Rights

Note: The list has been resequenced and restructured.

Rights in Relation to Physical Safety

- Life and Liberty
- Freedom from Cruel, Inhuman or Degrading Punishment
- Dignity

Rights in Relation to the State

- Nationality
- Participation in Government
- Equality and Equal Protection of the Law
- Freedom from Arbitrary Arrest
- Recognition as a Person Before the Law
- Effective Remedy
- Fair Hearing
- Presumption of Innocence
- Freedom from Retrospectivity
- Asylum
- Behavioural Rights
- Freedom from Slavery
- Freedom of Assembly and Association
- Freedom of Movement
- Family

Information Rights

- Freedom of Thought and Conscience
- Freedom of Access to Information [omitted from the Draft Bill, or
- perhaps assumed to be implicit]
- Freedom of Access to the Information Infrastructure [also omitted]
- Freedom of Opinion and Expression
- Privacy

Social and Economic Rights

- Adequate Standard of Living
- Education
- Work
- Social Security
- Leisure
- Participation in Cultural Life
- Social Order
- Property
- Copyright [or 'intellectual property' more generally]
- Saving

Equality

- Entitlement to Rights and Freedoms Without Distinction

References

Clarke R. (1987) 'Just Another Piece of Plastic for Your Wallet: The Australia Card' Prometheus 5, 1 (June 1987) 29–45. Republished in Computers & Society 18, 1 (January 1988), with an unrefereed Addendum in Computers & Society 18, 3 (July 1988), at http://www.anu.edu.au/people/Roger.Clarke/DV/OzCard.html

Clarke R. (1988) 'Information Technology and Dataveillance', Commun. ACM 31,5 (May 1988), At http://www.anu.edu au/people/Roger.Clarke/DV/CACM88.html

Clarke R. (1992) 'The Resistible Rise of the National Personal Data System' Software Law Journal V, 1 (January 1992) 29–59, at http://www.anu.edu.au/people/Roger.Clarke/DV/SLJ.html

Clarke R.A. (1994) 'The Digital Persona and Its Application to Data Surveillance' The Information Society 10,2 (June 1994). Abstract

at http://www.anu.edu.au/people/Roger.Clarke/DV/AbstractDigPersona.html

Clarke R.A. (1995a) 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' Info. Technology & People 7,4 (March 1995). At http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html

Clarke R. (1995b) 'When Do They Need to Know 'Whodunnit?' The Justification for Transaction Identification; The Scope for Transaction Anonymity and Pseudonymity', March 1995, at http://www.anu.edu.au/people/Roger.Clarke/DV/PaperCFP95.html

Clarke R. (1995c) 'Netethiquette Cases', May 1995. At http://www.anu.edu.au/people/Roger.Clarke/II/Netethiquettecases.html

Clarke R. (1995d) 'Electronic Payment Mechanisms', at http://www.anu.edu.au/people/Roger.Clarke/EC/EPMEPM.html

Clarke R. (1995e) 'Information Technology & Cyberspace: Their Impact on Rights and Liberties', Address to the Victorian Council for Civil Liberties, Melbourne, 13 September 1995. At http://www.anu.edu.au/people/Roger.Clarke/II/VicCCL.html

Clarke R. (1996a) 'Cyberculture: Towards the Analysis That Internet Participants Need', April 1996, at http://www.anu.edu.au/people/Roger.Clarke/II/CyberCulture.html

Clarke R.A. (1996b) 'Cryptography in Plain Text' Privacy Law & Policy Reporter 3, 4 (May 1996). At http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html

Clarke R.A. (1996c) 'Crypto-Confusion: Mutual Non-Comprehension Threatens Exploitation of the GII' Privacy Law & Policy Reporter 3, 4 (May 1996). At http://www.anu.edu.au/people/Roger.Clarke/II/CryptoConf.html

Clarke R. (1996d) 'Privacy and Dataveillance, and Organisational Strategy', presented at EDPAC, May 1996, and at http://www.anu.edu.au/people/Roger.Clarke/DV/PStrat.html

Clarke R. (1996e) 'Trails in the Sand', at http://www.anu.edu.au/people/Roger.Clarke/DV/Trails.html

Clarke R. (1996f) 'Issues in Technology-Based Consumer Transactions' Invited Address to the Annual Conference of the Society of Consumer Affairs Professionals (SOCAP), Melbourne, 26 September 1996, at http://www.anu.edu.au/people/Roger.Clarke/SOS/SOCAP96.html

Clarke R. (1996g) 'Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue', Presentation to the Conference on 'Smart Cards: The Issues', Sydney, 18 October 1996. At http://www.anu.edu.au/people/Roger.Clarke/DV/AnonPsPol.html

Clarke R. (1997a) 'What Do People Really Think? MasterCard's Survey of the Australian Public's Attitudes to Privacy', Privacy Law & Policy Report 3,9 (January 1997), at http://www.anu.edu.au/people/Roger.Clarke/DV/MCardSurvey.html

Clarke R. (1997b) 'Encouraging Cyberculture', April 1997, at http://www.anu.edu.au/people/Roger.Clarke/II/CAUSE97.html

Greenleaf G. & Clarke R. (1997) 'Privacy Implications of Digital Signatures', March 1997, at http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html

This paper is available at http://www.anu.edu.au/people/Roger.Clarke/II/IIRSecy97.html