PRIVACY AS A MEANS OF ENGENDERING TRUST IN CYBERSPACE COMMERCE

ROGER CLARKE*

I INTRODUCTION

Electronic relationships are only effective, and electronic transactions are only conducted, if the requisite degree of trust exists among the parties. The focus of this article is on the role of privacy in generating trust in cyberspace, and primarily on economic relationships in cyberspace rather than those of a familial or social nature.

For inter-personal communications on the Internet, trust *is* achievable. This article commences by briefly reviewing firstly the Internet and its use, and then the nature of trust online, concluding that privacy is a factor necessary to trust in cyberspace. A brisk analysis of privacy risks in cyberspace (and various methods of dealing with them) leads into an argument that, while various methods can be devised to protect privacy and encourage trust between individuals in their online dealings, the minimalist 'fair information practices' movement of the last thirty years is utterly inadequate as a basis for providing 'net-consumers' with the privacy they need. The current situation (which has resulted from that movement) therefore prevents individuals from trusting organisations and seriously constrains their preparedness to deal with them electronically. This article concludes that unless organisations establish their trustworthiness with consumers and citizens, the sluggishness in the growth of electronic commerce will continue for years to come.

II THE NATURE OF CYBERSPACE

The Internet is a telecommunications network that links other telecommunication networks; its purpose is to enable computers that are attached to any Internet-connected network to communicate with one another. Thus the Internet represents an infrastructure that provides a basis upon which valuable

* Principal, Xamax Consultancy Pty Ltd, Canberra; Visiting Fellow, Department of Computer Science, Australian National University.
This article is also available at <http://www.anu.edu.au/people/Roger.Clarke/DV/eTrust.html>.

services can be built. Important among these services are those that enable people to send one another messages (for example, via email), or to store information that other people can retrieve (for example, on the World Wide Web).[1]

These and other services together create an 'experience space', in which people have a 'shared hallucination'. While there is nothing physically 'there', if the parties suspend their disbelief, and perceive themselves as having a sufficiently common understanding based on the information they are exchanging, then it seems as if there is, in fact, 'something there'. A sci-fi novelist coined the term 'cyberspace' as a means of referring not to the underlying inter-networking arrangements of the Internet, nor to the services built upon that infrastructure, but to the virtual experience users share.

III THE CONCEPT OF TRUST

Trust can be defined in many ways. In my ongoing research and consultancy in this area, I use the following working definition: *trust is confident reliance by one party on the behaviour of other parties.*

Trust differs depending on the relationship between the parties. Economic relationships may be direct, as in principal-agent and contractual relationships. In many cases, however, a party may rely on another party despite having no formal relationship with them, or even much knowledge about them. (Examples from cyberspace include unthinking acceptance of the veracity of the contents of an email message or a website.)

Trust may be relatively unimportant where the risks that the parties are exposed to are limited and the elapsed time during which the exposure exists is quite short, or where the risks are well known but insurance is taken into account in the costs. Where such factors do not exist, trust tends to be crucial for transactions to take place and relationships to develop.[2]

IV TRUST IN CYBERSPACE

When business interests finally discovered the Internet in the mid-1990s, it was assumed that electronic commerce would explode. It hasn't. The primary reason is that cyberspace evidences many characteristics that render trust very important, and business has signally failed to address the trust gap.

A key reason for trust being a substantially different challenge in cyberspace – in comparison with the physical world – is that the parties have little knowledge

[1] See Roger Clarke *et al*, *A Primer on Internet Technology* (1998) <http://www.anu.edu.au/people/Roger.Clarke/II/IPrimer.html> at 21 May 2001.

[2] For a deeper discussion of trust in cyberspace, see Roger Clarke, 'Of Trustworthiness and Pets: What Lawyers Haven't Done for e-Business' (Paper presented at the 5th Biennial Pacific Rim Computer Law Conference, Sydney, 22-24 February 2001) (also at <http://www.anu.edu.au/people/Roger.Clarke/EC/PacRimCL01.html> at 21 May 2001).

about one another, and cannot depend on such confidence-engendering measures as physical proximity, handshakes, body language, a common legal jurisdiction, or even necessarily any definable jurisdiction.[3] A range of measures is needed to inculcate sufficient confidence in Internet users that economic transactions can proceed and relationships can be built online. These measures include the availability of information that can be authenticated, recommendations from trusted parties (as distinct from ersatz, engineered proxies for reputation, such as brand names and 'seals of approval'), message and data security, limitation of risk exposure, and other general safeguards against risk. This article focuses on a particularly important factor relevant to encouraging trust online: ensuring users' privacy.

V PRIVACY RISK ANALYSIS

There are many sources of risk in cyberspace, including the other individuals with whom one deals, the providers that services are acquired from, government agencies and corporations that one transacts with, and government regulatory agencies. The nature of the risks faced include monitoring of a person's communications, leakage of information to parties that may seek to exploit it, psychological pressure arising from aggressive communications, the construction of a digital persona that represents an individual, and use of that persona by others to predict and manipulate that individual's behaviour.[4]

However, a variety of risk management approaches are available to users. A principal proactive strategy is avoidance, which can involve declining to use particularly threatening Internet services (such as Microsoft products generally), avoiding central storage of personal data, not divulging sensitive personal data such as contact points and credit card details, and storing sensitive data and performing sensitive procedures on equipment that is not connected to the Internet. Other proactive strategies include deterrence (for example, providing notice to marketing organisations that are suspected of gathering personal data that consent is explicitly denied), and prevention (for example, by implementing

[3] See Roger Clarke, 'Key Issues in Electronic Commerce and Electronic Publishing' (Paper presented at the Information Online and On Disc 99 Conference, Sydney, 19-21 January 1999) (also at <http://www.anu.edu.au/people/Roger.Clarke/EC/Issues98.html#Iss2> at 21 May 2001).

[4] See Roger Clarke, 'The Digital Persona and its Application to Data Surveillance' (1994) 10(2) *The Information Society* 77 (also at <http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html> at 21 May 2001). Deeper analyses are available of the theory of dataveillance (Roger Clarke, 'Information Technology and Dataveillance' in C Dunlop and R Kling (eds), *Controversies in Computing* (1991) 496); human identification (Roger Clarke, 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' (1994) 7(4) *Information Technology and People* 6); direct marketing and privacy (Roger Clarke, 'Direct Marketing and Privacy' (Paper presented at the AIC Conference on the Direct Distribution of Financial Services, Sydney, 24 February 1998) (also at <http://www.anu.edu.au/people/Roger.Clarke/DV/DirectMkting.html> at 21 May 2001)); and privacy on the Internet (Roger Clarke, 'Information Privacy On the Internet: Cyberspace Invades Personal Space' (1998) 48(2) *Telecommunications Journal of Australia* 61).

counter-measures such as 'cookie' managers and personal 'firewalls').[5] Additional approaches are reactive in nature: detection strategies include virus detection software and monitoring of the traffic leaving one's own machine; recovery strategies include virus removal routines; and insurance strategies include backup of personal data complemented by clear plans as to how to recover from an invasion by harmful software. In some circumstances it may be rational to rely on the non-reactive strategy of risk tolerance: 'I don't have the time to consider it, or the money to address it, and if the worst happens, I'll worry about it then'.

Given the privacy risks confronting people in cyberspace, however, caution is generally advisable. Thus a tendency arises among experienced players to adopt a proactive avoidance strategy that includes denying other parties knowledge of one's identity, denying other parties information about oneself generally, and perhaps even falsifying information about oneself.[6] The following sections consider the efficacy of some approaches by individuals and by organisations (including governments and corporations) to privacy protection in fostering trust in cyberspace.

VI ANONYMITY AND PSEUDONYMITY

A fundamental approach adopted by individuals to managing privacy risk in cyberspace is to prevent other parties gaining knowledge of one's identity. Since most online transactions involve a succession of messages, it is essential that the anonymous participant be able to be reached by other parties, and be able to associate new messages with old ones. This requires a consistent identity, referred to as a 'persistent nym'.[7]

It is also likely that information about the entity behind the nym will be disclosed to other participants, at the very least through the nym's behaviour. Indeed, many social relationships in electronic fora involve what is sometimes referred to as 'performance-based reputation'. Nothing is known about the person other than their 'track-record' or history in that particular context, yet other members of the forum may be quite trusting of the person behind the nym, unless and until they destroy their own credibility through behaviour or expression inconsistent with the persona they have developed.

In many cases, however, denial of identity protects one party while preventing the other party from developing trust through shared information. An approach

[5] For an introduction to information security matters see Roger Clarke, 'Introduction to Information Security' (2001) <http://www.anu.edu.au/people/Roger.Clarke/EC/IntroSecy.html> at 21 May 2001.

[6] A notable editorial in *The Sydney Morning Herald* after the passage of the *Privacy Amendment (Private Sector) Act 2000* (Cth) concluded that because the legislation 'allows businesses to continue to build electronic lists ... many cynics will continue along the path of least resistance: filling in those annoying forms anyway – with an alias and a fictional address': Editorial, *The Sydney Morning Herald* (Sydney), 8 December 2000, 18.

[7] See Roger Clarke, 'Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice' (Paper presented at the User Identification and Privacy Protection Conference, Stockholm, 14-15 June 1999) (also at <http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html> at 21 May 2001).

that is riskier for the first party, but more conducive to the development of trust, is to use a nym that is traceable but not readily so. Other parties can have some confidence that serious misbehaviour by a person (for example, criminal acts like harassment and fraudulent misbehaviour, and civil wrongs like failure to perform contractual obligations and insolvency) can be addressed by breaking through the protections surrounding the nym and identifying the individual.

The challenge is to find suitable means whereby legal, organisational and technical protections can be breached when conditions demand it, but not breached casually, even by a powerful organisation (such as a government or a large corporation), simply when the organisation believes its interests have been harmed.

VII PRIVACY-INVASIVE PRACTICES AND CONTROLS OVER THEM

The mainstream approach to engendering trust by ensuring privacy has been through the protection of personal data. For three decades, the presumption has been made that the right to privacy, or at least that sub-set of the right to privacy reasonably described as 'information privacy' or 'data privacy', can be suitably addressed by requiring that practices in relation to the handling of personal information be 'fair'.

The 'fair information practices' movement originated in American business and government circles in the late 1960s, but flowered in Europe during the 1970s. Substantial bodies of so-called 'data protection' laws have developed as a result and are still being refined. The model has been adopted and adapted in many non-European countries, resisted by the United States Federal Government, and bastardised by the Australian Government.

The notion of 'fair information practices' has proven to be utterly inadequate, with inadequate scope, manifold exemptions and exceptions, and missing control mechanisms.[8] It has become so ingrained, however, that the focus of public policy is very difficult to shift away from the protection of mere data, back to the protection of people's privacy.

In the meantime, organisations continue to enthusiastically develop and implement inherently privacy-invasive technologies, for example, by seeking to impose intrusive online identification, identity-authentication mechanisms,[9] and

[8] See Roger Clarke, 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century' (2000) <http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html> at 21 May 2001.

[9] See Clarke, 'Human Identification in Information Systems', above n 4; Roger Clarke, 'Chip-Based ID: Promise and Peril' (Paper presented at the International Conference on Privacy, Montreal, 23-26 September 1997) (also at <http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html> at 21 May 2001).

person location and tracking technologies,[10] including controversial 'digital signature' schemes.[11]

VIII RECOURSE AND ENFORCEMENT

For privacy protections to be of any consequence, miscreants must be subject to sanctions. The sanctions need to be commensurate with the gravity of the action taken and the harm caused, and applied in such a manner as to cause a change in behaviour. There is an expectation that 'watchdog' agencies will assume this enforcement function and will audit for compliance, address deficiencies and misbehaviour, and prosecute breaches.

However, many privacy-abusive activities are subject only to organisational self-restraint and industry association codes. So-called 'self-regulation' is regarded by the public as completely lacking in credibility. Measures like meta-brands (for example, the 'seals of approval' provided by TRUSTe and WebTrust) and privacy statements are repeatedly breached, and seen to be breached, without any action being taken; the undertakings made are therefore nominal, unenforced, and in most cases unenforceable. Self-regulation is seen by the public for what it is: supervision of the sheep by the wolves, for the benefit of the wolves, and a means for business to establish a pretence of regulation in order to hold off actual regulation.

European countries at least have a regulatory framework in place, even though its scope is quite inadequate for the 'information age' that was already very much in evidence late last century. Australia, however, is very different. Federal Privacy Commissioners seem to regard their role as restricted to a mere administrator of legislation. They talk pleasantly with the organisations that the public expects them to regulate, and they issue guidelines in relation to Internet usage that actively encourage organisations to invade their employees' privacy in ways that would be illegal if applied to person-to-person conversations and the telephone.

Far from enhancing trust between individuals, and between individuals and organisations, recent Australian legislation (in the form of the *Privacy Amendment (Private Sector) Act 2000* (Cth)) has subverted the principles of privacy protection outlined in the 1980 Organisation for Economic Co-operation and Development *Guidelines Governing the Protection of Privacy and Transborder Flows of Data* in order to legitimise a wide variety of privacy-intrusive practices by private sector corporations. This law is an actively 'anti-privacy' statute. The current Privacy Commissioner's laudable attempts to

[10] See Roger Clarke, 'Person-Location and Person-Tracking: Technologies, Risks and Policy Implications' (Paper presented at the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, September 1999) (also at <http://www.anu.edu.au/people/Roger.Clarke/DV/PLT.html> at 21 May 2001).

[11] See Roger Clarke, 'The Fundamental Inadequacies of Conventional Public Key Infrastructure' (Paper presented at the European Conference in Information Systems 2001, Slovenia, 27-29 June 2001) (also at <http://www.anu.edu.au/people/Roger.Clarke/II/ECIS2001.html> at 8 June 2001).

interpret the statute broadly enough to overcome some of its weaknesses are unlikely to succeed. It is a serious set back to hopes for privacy generally and for trust in Internet commerce in particular, and it demonstrates the inadequacy of the 'fair information practices' movement.[12] At a time when substantial new initiatives are needed, Australia is 30 years behind and going backwards.

Contrary to popular mythology, the United States ('US') is the country with the highest level of privacy regulation in the world. However, the relevant legislation comprises large numbers of highly specific statutes, created as 'knee-jerk' reactions to particular issues and public concerns. Comprehensive legislation is still being resisted, and, when it comes, will be subject to massive subversion by the corporate interests that fund American politicians. Yet the desperate need for measures that encourage trust in economic uses of cyberspace will eventually force the hand of the US Congress and the President.[13]

IX BEYOND MERE 'DATA PROTECTION'

Legislatures throughout the world have failed their citizens by providing weak protections for data instead of strong protections for people. In any case, the scope of privacy is far greater than just information privacy. Other dimensions that are of great significance in cyberspace dealings are the privacy of personal behaviour and the privacy of personal communications.

Organisations, and some individuals, are using the potential that Internet technologies provide to abuse these aspects of privacy by submitting users to privacy-invasive measures such as surveillance techniques. Technical devices such as 'click-trails', 'cookies' and single-pixel images (referred to in the popular literature as 'web-bugs') are used to complement simpler ideas like cajoling net-consumers to provide large quantities of personal data in return for very little recompense, and the pooling of behaviour-related data among companies.

X CONCLUSIONS

Social relationships in cyberspace are modestly constrained by trust concerns. Economic relationships between individuals and organisations in cyberspace, on the other hand, are at crisis point. The behaviour of marketers during the closing years of the last century and the beginning of the new one has been so irresponsible that there is very limited trust by people in the actions of companies on the Internet. It will take a long time for trust to be re-built, and

[12] See Roger Clarke, 'Submission to the Commonwealth Attorney-General Re: "A privacy scheme for the private sector: Release of Key Provisions" of 14 December 1999' (2000) <http://www.anu.edu.au/people/Roger.Clarke/DV/PAPSSub0001.html> at 8 June 2001.

[13] See Roger Clarke, 'Internet Privacy Concerns Confirm the Case for Intervention' (1999) 42(2) *Communications of the Association for Computing Machinery* 60 (also at <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM99.html> at 8 June 2001).

many factors will be relevant. But unless that framework features strong and comprehensive privacy laws, and systematic enforcement of those laws, corporations and government agencies will not succeed in stimulating trust in cyberspace commerce.