

Dataveillance - 15 Years On

[Roger Clarke](#)

Principal, [Xamax Consultancy Pty Ltd](#), Canberra

Visiting Professor, [Baker & McKenzie Cyberspace Law & Policy Centre](#), [University of N.S.W.](#)

Visiting Fellow, [Department of Computer Science](#), [Australian National University](#)

Revision of 31 March 2003

Prepared for presentation at the Privacy Issues Forum run by the [New Zealand Privacy Commissioner](#),
Wellington, 28 March 2003

The accompanying PowerPoint slide-set is at <http://www.anu.edu.au/people/Roger.Clarke/DV/DVNZ03.ppt>

© [Xamax Consultancy Pty Ltd](#), 2003

This document is at <http://www.anu.edu.au/people/Roger.Clarke/DV/DVNZ03.html>

Abstract

I coined the term 'dataveillance' in the mid-1980s, as a convenient short form for 'data surveillance'. This presentation briefly reviews developments in the area since then.

It concludes that the development of dataveillance technologies has continued apace, and that appreciation of their nature and impact is still very low. The maturation process in policy debates is still in its infancy, and needs to be brought forward very quickly if legal structures are to enable humanity to survive the onslaught. Reliance on the vacuous idea of 'self-regulation', or on Privacy Enhancing Technologies (PETs), as excuses to avoid effective legislation, invites a cleft between official and unofficial societies. There is plenty of scope for the public to create and operate counter-technologies.

Contents

- [1. Dataveillance Then](#)
 - [2. Dataveillance Now](#)
 - [2.1 The Perception](#)
 - [2.2 The Reality](#)
 - [3. Identification Revisited](#)
 - [4. Public Policy Responses](#)
 - [5. The Broad Sweep of I.T. History](#)
 - [6. Conclusions](#)
 - [References](#)
-

1. Dataveillance Then

I introduced the concept of 'dataveillance' in [\(1988\)](#), defining it as "the systematic monitoring of people's actions or communications through the application of information technology".

The paper drew attention to the consolidation of personal data from multiple sources, the emergence of new technologies to exploit that data, and the central role of multi-purpose identification schemes. Techniques already in use included front-end verification, cross-system enforcement, profiling [\(1993b\)](#), and data matching [\(1994d, 1994b, 1995\)](#).

Monitoring people's behaviour has always been expensive, because physical surveillance, even when technology-enhanced, is labour-intensive. The paper argued that economics would ensure that, because dataveillance was highly automated, it would not merely augment conventional surveillance, but would to a considerable extent supplant it.

The paper drew attention to the serious implications of the techniques for both individuals and society as a whole. It considered intrinsic controls over unreasonable and excessive uses of the technologies (which were entirely inadequate), and assessed extrinsic controls (which were very limited).

2. Dataveillance Now

2.1 The Perception

Although the public's appreciation of surveillance technologies is somewhat greater than it was, there are several blindspots that continue to plague the limited discussions that do take place.

The first is the continuing mistake of using visual images of surveillance when it has gone underground, out of sight, and virtual. The original anti-utopian novel, Zamyatin's 'We', involved technology-aided observation of the populace. Its descendant, Orwell's '1984', conditioned us to the visual notions of two-way 'telescreens' ([1993a](#), [2000f](#)). Video-surveillance is an issue of concern, but has had nowhere near as significant an impact as dataveillance.

A second blind-spot is that few people distinguish between personal surveillance and mass surveillance. Personal dataveillance is the monitoring of an identified person, generally for a specific reason. Mass dataveillance, on the other hand, involves monitoring groups of people, usually large groups. The reason for the monitoring is to identify individuals who belong to some particular class of interest to the surveillance organization. In short, mass dataveillance is a suspicion-generator.

2.2 The Reality

Since my foundation analysis in the mid-1980s, a wide array of dataveillance technologies has been developed. Initially, these leveraged off the great many data trails that arise as a byproduct of people's transactions with organisations ([1996a](#)), but many new data trails have been created, specifically to advantage organisations. In addition, many technologies have been created and deployed, for which I coined the term 'the PITs' (Privacy-Invasive Technologies, in late 1998. See [2001b](#)).

These new developments have included:

- marketers' 'loyalty' schemes ([1998a](#));
- Internet tracing ([1998b](#), [1999a](#)), including cookies, spam, and spyware;
- highways that deny anonymous travel and demand identification ([2000e](#));
- digital rights management ([1999c](#), [2000d](#), [2001f](#));
- enum, a proposal to express telephone numbers as Internet addresses ([2002b](#));
- chip-based identification ([1994f](#), [1997b](#));
- digital signatures and public key infrastructure ([1997a](#), [2000b](#));
- person location and tracking ([2001e](#));
- biometrics ([1994f](#), [2002a](#));
- extraction, stock-piling and use of human genetic data.

Despite this explosion, however, legislators, policy advisors and social commentators have abjectly failed to notice that dataveillance is rampant, and that it is imposing major change on societies ([2001a](#)).

3. Identification Revisited

In 1994, I published a work on '[Human Identification in Information Systems](#)', whose purpose was to fill a yawning gap in the literature. During the last decade, it's become apparent just how much ignorance exists among information systems designers about the real world of identity. I examined the emergent concept of a 'nym', originally using the term 'digital persona' ([1994c](#), [1999b](#), [2000g](#), [2001b](#), [2001g](#)). A series of papers then analysed the concepts of anonymity and pseudonymity (in particular, [1996b](#), [1999b](#)). I've subsequently extended that line of argument into the area of authentication in the service of eBusiness ([2001g](#)), and into biometrics ([2002a](#)).

It is critical that the notions of identity and entity be distinguished, and that the role of nyms be appreciated. Otherwise, an understanding of dataveillance, and of the real nature of biometrics, is impossible to achieve. Two recent works re-visit the social implications of dataveillance technologies, by drawing out the effects of the naive biometrics applications that have been trialled (and much-hyped) in the wake of the terrorist strikes on New York and Washington in September 2001 ([2002a](#), [2003](#)).

4. Public Policy Responses

One of the most stunning features of the last 15 years has been the complete absence of policy responses to the explosion of dataveillance.

Michael Kirby referred to the 1970s as 'the decade of privacy'. Policy-makers are still stuck there. The OECD Guidelines have been a complete failure as a means of countering the explosion of dataveillance technologies. (To be fair, their purposes were, firstly and explicitly, to avoid inconsistencies among international laws; and secondly to provide governments with an excuse not to do anything more than the minimum. They have been quite successful when measured against their original purposes). The vast range of inadequacies of the 'Fair Information Practices' movement, as codified by the OECD Guidelines, is catalogued in ([2000a](#)).

1970s-style 'data protection' laws are still being passed. The imagination of bureaucrats has been exercised, in order to find ways of trimming the original interpretations of the data protections expressed in the OECD Guidelines back to very little indeed. That movement has its finest expression in the Howard Government's anti-privacy law of 2000, which purported to extend data protection law to the private sector in Australia, but actually, through a series of devices, legitimised a wide array of privacy-invasive practices ([2000b](#)).

Considerable imagination has also been shown by the opponents of legislation that would protect privacy and regulate surveillance technologies:

- the **victimhood** school of thought is alive and well, and encouraged by the corporation-serving information technology media ('they know all about us already, and governments and businesses

- control our lives anyway, so why bother fighting it');
- seizing on that opportunity, a '**give up on privacy**' school of thought has come into existence, with Sun's Scott McNeely as its spokesperson;
- David Brin would have us believe that we can achieve '**privacy through openness**'. [\(1999a\)](#) argued that this was wishful thinking;
- attempts are being made to reduce the human right of privacy to a **mere economic right**. This movement, which is even supported by at least one Privacy Commissioner, was severely criticised in [\(2000a\)](#);
- the **self-regulation** option is touted, even outside the U.S.A. It is merely a contemporary version of what Jim Rule described as the Alan Westin 'administrative convenience' approach. The idea of 'self-regulation' is a chimera: as I've put it to many audiences over the years, "wolves self-regulate for the good of themselves and the pack, not the deer";
- a **co-regulatory** school of thought began to emerge [\(1999a\)](#), and [the New Zealand Privacy Act 1993](#) was suggested as a model. But the idea was quickly debased into mere 'self-regulation';
- a '**technology will solve it**' school of thought is being championed, not least by Privacy Commissioners, who must find it a welcome relief from arguing to politicians and bureaucrats the necessity of genuine laws. Privacy enhancing technologies (PETs) are of several kinds, which I've distinguished as 'PIT countermeasures', 'savage PETs' and 'gentle PETs' [\(2001b\)](#) and [\(2001c\)](#). They are valuable adjuncts to an effective protective regime, but they cannot be a substitute;
- meanwhile **the black-letter regulatory school of thought** has languished. Genuinely and significantly new developments in privacy protection law have been almost non-existent since the end of the 1970s.

While this serial avoidance behaviour has been indulged in, the ravages of new technologies have gone completely unchecked by legislatures and watchdogs. Privacy Commissioners, and their conferences, concentrate on the administrivia of data protection. Meanwhile, 'the main game' continues unabated, largely undiscussed, and beyond the scope of privacy laws and of privacy law administrators. See [\(2000a\)](#).

5. The Broad Sweep of I.T. History

In two 1994 articles, I depicted the period 1980-2000 as 'the uneasy era of unjustified centralisation' [\(1994a\)](#), [\(1994e\)](#). We've now reached what I depicted then as 'the era of dispersed power'.

The argument proceeded as follows. From the invention of computing in about 1940, until about 1980, Grosch's Law held. This asserted that the processing power of computers grew exponentially with their cost. In other words, bigger was more efficient. This tendency towards centralised systems was supported by 'star' topologies for networks, with a powerful machine at the 'hub', and a flotilla of 'dumb terminals' at the peripheries. The relationship between the nodes was master-to-slave. The natural

organisational form to utilise such infrastructure was hierarchical. Software was closed and proprietary. The political form that was served by the information technology of the era was authoritarian and intolerant.

Grosch's Law was rescinded in about 1969, although the impact was felt in the marketplace only gradually (hence my selection of 1980 as the indicative year in which the old era ended).

Very Large Scale Integrated (VLSI) circuitry spawned new machine architectures, and a new economics. Many micro-computers deliver not just greater flexibility than fewer larger machines, but also more power more cheaply. Networks quickly evolved into the multiply-connected, decentralised form that they currently have. Master-slave relationships gave way to so-called client-server arrangements, where intelligent remote workstations request services from dispersed devices scattered around an office, a campus, and the world. Organisations that take advantage of this technology exhibit not centralised form, but networked form. Software and politics were both thrown into confusion, from which they are only now beginning to emerge.

What, then, is the future?

To paraphrase the fast food industry mantra, it's 'chips with everything'. Computing is embedded, and taken for granted. Connections are increasingly wireless, and ubiquitous. Client-server relationships are already being overtaken by peer-to-peer (now dubbed 'P2P') cooperations. The managed networks of the last two decades of the 20th century are being superseded by self-managing networks that are more akin to markets than to the old hierarchies.

Software, and increasingly also digital content, are open rather than closed. Microsoft and the Recording Industry Association of America will fight a rearguard action for some years yet; but the battle is already lost, and they badly need to start adapting. The natural political form in this era is democracy (and direct, optionally participative democracy rather than the tired old idea of representative democracy). It would be nice to think that tolerance might be a feature of the new order; but all the evidence to date (such as the misguided attempts to regulate pornography and on-line gambling) suggests that intolerance will continue, but that the intolerant will be increasingly frustrated.

The description in this section is a direct presentation of the argument in my 1994 papers - which of course drew heavily on the thinking of others, as indicated in [\(1993a\)](#). But, even with the benefit of a decade's hindsight, I suggest that both my analysis and my suggested timings were about right.

6. Conclusions

In the first part of this paper, I drew attention to the unchecked explosion of dataveillance technologies, and I bemoaned the abject failure of lawmakers to even notice it, let alone do anything about it. So it

might have been expected that I would end this paper on a downbeat note.

I don't.

Elements of the public have been much more active than legislators and Privacy Commissioners. For every Scott McNeely sneeringly dismissing the contemporary relevance of the very concept of privacy, and every David Brin arguing the abandonment of privacy-through-secrecy in favour of privacy-through-openness, there are scores of backroom activists at work. In addition to the Privacy Enhancing Technologies (PETs) movement ([2001b](#), [2001c](#)), the Internet is being used as a means of countering authoritarianism ([2001f](#)).

The near-future world would be a much nicer place if politicians, government executives and business leaders would take the trouble to understand technological change and its implications. They would be able to lead the world towards new forms of societies and economies. These would feature less centralised, networked organisations, and a reduction in outdated, authoritarian structures and processes. In this scenario, technologies would be conceived and developed to balance multiple interests.

Instead, simple-minded, authoritarian corporatism reigns supreme. So counter-technologies have to be developed, to undermine and subvert authoritarian ones. Instead of PETs focussing on the equilibrating notion of pseudonymity, the activists in the back rooms are working on anonymity, as a means of avoiding authority, and defeating it. We're stuck in the old politics of thesis and counter-thesis, the morass of adversarial systems.

The conclusion 15 years on is that the world learns far too slowly.

References

Clarke R. (1987) 'Just Another Piece of Plastic for Your Wallet: **The Australia Card**' Prometheus 5,1 June 1987 Republished in Computers & Society 18,1 (January 1988), with an 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. (1991) '**The Tax File Number Scheme**: A Case Study of Political Assurances and Function Creep' Policy 7,4 (Summer 1991), at <http://www.anu.edu.au/people/Roger.Clarke/DV/PaperTFN.html>

Clarke R. (1992) '**The Resistible Rise of the Australian National Personal Data System**' Software L. J. 5,1 (January 1992), at <http://www.anu.edu.au/people/Roger.Clarke/DV/SLJ.html>

Clarke R. (1993a) 'A 'Future Trace' on Dataveillance: **The Anti-Utopian and Cyberpunk Literary Genres**' 9 March 1993, at <http://www.anu.edu.au/people/Roger.Clarke/DV/NotesAntiUtopia.html>

Clarke R. (1993b) '**Profiling**: A Hidden Challenge to the Regulation of Data Surveillance', Journal of Law and Information Science 4,2 (December 1993) ', at <http://www.anu.edu.au/people/Roger.Clarke/DV/PaperProfiling.html>

Clarke R.A. (1994a) '**The Eras of Dataveillance**' (March 1994), at <http://www.anu.edu.au/people/Roger.Clarke/DV/NotesDVEras.html>

Clarke R.A. (1994b) 'Matches Played Under Rafferty's Rules: **The Parallel Data Matching Program Is Not Only Privacy-Invasive But Economically Unjustifiable As Well**' Policy 10,1 (Autumn 1994), at <http://www.anu.edu.au/people/Roger.Clarke/DV/PaperMatchPDMP.htm> 1

Clarke R. (1994c) 'The **Digital Persona** and its Application to Data Surveillance' The Information Society 10,2 (June 1994), at <http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html>

Clarke R. (1994d) 'Dataveillance by Governments: The Technique of **Computer Matching**' Information Technology & People 7,2 (June 1994), at <http://www.anu.edu.au/people/Roger.Clarke/DV/MatchIntro.html>

Clarke R. (1994e) '**Information Technology: Weapon of Authoritarianism or Tool of Democracy?**' Proc. World Congress, Int'l Fed. of Info. Processing, Hamburg, September 1994, at <http://www.anu.edu.au/people/Roger.Clarke/DV/PaperAuthism.html>

Clarke R. (1994f) '**Human Identification** in Information Systems: Management Challenges and Public Policy Issues' Info. Technology & People 7,4 (December 1994), at <http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html>

Clarke R. (1995) '**A Normative Regulatory Framework for Computer Matching**' Journal of Computer and Information Law XIII,4 (Summer 1995) 585-633, at <http://www.anu.edu.au/people/Roger.Clarke/DV/MatchFrame.html>

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

Clarke R. (1996b) '**Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue**', 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) 'Privacy Implications of **Digital Signatures**' IBC Conference on Digital Signatures, Sydney (secondary author to G.W. Greenleaf, March 1997), at <http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html>

Clarke R, (1997b) '**Chip-Based ID: Promise and Peril**', for the [International Conference on Privacy, Montreal](http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html) (September 1997), at <http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html>

Clarke R, (1998a) '**Direct Marketing** and Privacy' 23 February 1998, at <http://www.anu.edu.au/people/Roger.Clarke/DV/DirectMkting.html>

Clarke R, (1998b) 'Information Privacy On the Internet: **Cyberspace Invades Personal Space**' Telecommunication Journal of Australia 48, 2 (May/June 1998), at <http://www.anu.edu.au/people/Roger.Clarke/DV/IPrivacy.html>

Clarke R, (1999a) 'Internet Privacy Concerns Confirm the **Case for Intervention**' Commun. ACM 42, 2 (February 1999) 60-67, Special Issue on Internet Privacy, at <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM99.html>

Clarke R, (1999b) '**Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice**' Proc. Conf. User Identification & Privacy Protection, Stockholm, 14-15 June 1999, at <http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html>

Clarke R. (1999c) '**Freedom of Information? The Internet as Harbinger of the New Dark Ages** ', Proc. Conf. 'Freedom of Information and the Right to Know', Melbourne, 19-20 August 1999. Republished in [First Monday](http://www.anu.edu.au/people/Roger.Clarke/II/DarkAges.html) 4, 11 (November 1999), at <http://www.anu.edu.au/people/Roger.Clarke/II/DarkAges.html>

Clarke R. (2000a) 'Beyond the OECD Guidelines: **Privacy Protection for the 21st Century**' January 2000, at <http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html>

Clarke R. (2000b) 'Privacy Requirements of **Public Key Infrastructure**' Proc. IIR Conf., Canberra, March 2000, and [PowerPoint slides](http://www.anu.edu.au/people/Roger.Clarke/DV/PKI2000.html), at <http://www.anu.edu.au/people/Roger.Clarke/DV/PKI2000.html>

Clarke R. (2000c) 'Submission to the Commonwealth Attorney-General, re: '**A privacy scheme for the private sector: Release of Key Provisions**' of 14 December 1999', January 2000, at <http://www.anu.edu.au/people/Roger.Clarke/DV/PAPSSub0001.html>

Clarke R. (2000d) '**Technological Protections for Digital Copyright Objects**' Proc. 8th Euro. Conf.

Infor. Sys. (ECIS'2000), July 2000, Vienna Uni. of Economics & Business Administration, pp. 745-752, with co-author S. Nees, at <http://www.anu.edu.au/people/Roger.Clarke/II/TPDCO.html>

Clarke R. (2000e) 'How to Ensure That Privacy Concerns Don't Undermine **e-Transport** Investments' AIC e-Transport Conference, Melbourne, 27-28 July 2000, at <http://www.anu.edu.au/people/Roger.Clarke/EC/eTP.html>

Clarke R. (2000f) '**Technologies of Mass Observation**' Notes for the 'Mass Observation Movement' Forum , run by Experimenta Media Arts and Open Channel, Melbourne, 26 October 2000, at <http://www.anu.edu.au/people/Roger.Clarke/DV/MassObsT.html>

Clarke R. (2000g) 'Famous **Nyms**' 29 November 2000, at <http://www.anu.edu.au/people/Roger.Clarke/DV/FamousNyms.html>

Clarke R. (2001a) '**While You Were Sleeping ... Surveillance Technologies Arrived**', [Australian Quarterly](#) 73, 1 (January-February 2001) 10-14, at <http://www.anu.edu.au/people/Roger.Clarke/DV/AQ2001.html>

Clarke R. (2001b) 'Introducing **PITs and PETs**: Technologies Affecting Privacy ' Privacy Law & Policy Reporter 7, 9 (March 2001) 181-183, 188, at <http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETs.html>

Clarke R. (2001c) 'Roger Clarke's **PITs and PETs Resources Site**' 6 April 2001, at <http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETsRes.html>

Clarke R. (2001d) '**P3P Re-visited**' [Privacy Law & Policy Reporter](#) 7, 10 (April 2001), at <http://www.anu.edu.au/people/Roger.Clarke/DV/P3PRev.html>

Clarke R. (2001e) '**Person-Location and Person-Tracking**: Technologies, Risks and Policy Implications' Information Technology & People 14, 2 (Summer 2001) 206-231 , at <http://www.anu.edu.au/people/Roger.Clarke/DV/PLT.html>

Clarke R. (2001f) 'Paradise Gained, Paradise Re-lost: **How the Internet is being Changed** from a Means of Liberation to a Tool of Authoritarianism' Mots Pluriels 18 (August 2001), Special Issue on 'The Net: New Apprentices and Old Masters', at <http://www.anu.edu.au/people/Roger.Clarke/II/PGPR01.html>

Clarke R. (2001g) '**Authentication**: A Sufficiently Rich Model to Enable e-Business' 26 December 2001, at <http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html>

Clarke R. (2002a) '**Biometrics' Inadequacies and Threats**, and the Need for Regulation' 15 April 2002, at <http://www.anu.edu.au/people/Roger.Clarke/DV/BiomThreats.html>

Clarke R. (2002b) '**ENUM** - A Case Study in Social Irresponsibility ' Proc. ISOC-AU Forum on New Protocols and Standards-Setting in Australia, 3 December 2002. Revised Version of 9 March 2003, for Privacy Law & Policy Reporter (March 2003) , at <http://www.anu.edu.au/people/Roger.Clarke/DV/enumISOC02.html>

Clarke R. (2003) '**SmartGate: A Face Recognition** Trial at Sydney Airport' 28 February 2003, at <http://www.anu.edu.au/people/Roger.Clarke/DV/SmartGate.html>

Navigation

Go to [Roger's Home Page](#).

Go to [the contents-page for this segment](#).

[Send an email to Roger](#)

Created: 18 March 2003

Last Amended: 31 March 2003



These community service pages are a joint offering of the Australian National University (which provides the infrastructure), and Roger Clarke (who provides the content).



[The Australian National University](#)

Visiting Fellow, Faculty of
Engineering and Information Technology,
Information Sciences Building Room 211

[Xamax Consultancy Pty Ltd](#), ACN: 002 360 456

78 Sidaway St
Chapman ACT 2611 AUSTRALIA
Tel: +61 2 6288 1472, 6288 6916