ISTOCK PHOTO

What is Überveillance? (And What Should Be Done About It?)

ROGER CLARKE

Corporate marketers have promoted technologies as means to monitor the behavior of all manner of things. Governments have suspended their disbelief and permitted agencies to buy technologies and install monitor systems. Some corporations have imposed similar schemes on their employees and their customers.

Digital Object Identifier 10.1109/MTS.2010.937030

There is enormous diversity among the behavior monitoring schemes that have been installed or proposed. Indeed, there are many objectives, and considerable specialization is occurring, with the result that surveillance is going through divergence and even splintering.

But there are also signs of convergence and coordination, and this creates both some degree of promise and a vastly increased threat to society.

Fundamentals of "Surveillance"

In my work over the last 20 years, I've referred to surveillance as "the systematic investigation or monitoring of the actions or communications of one or more persons." This definition requires some adjustment, in particular to take account of the monitoring of spaces, and of objects other than humans. The primary concern of this article is the surveillance of people and their behavior, whether directly or indirectly.

The original forms of physical surveillance were typified by visual observation, and symbolized by Bentham's panopticon.

Watching and listening have come to be aided by equipment of various kinds which offers enhancement of optical and aural signals, e.g., through telescopes and directional microphones. This has enabled physical surveillance at distance.

A development in recent years has been the emergent phenomenon of what might be called auto-physical surveillance. Auto-physical surveillance is enabled by means of devices that are attached to the person (whether loosely but reliably, as with a mobile phone, or tightly as with an anklet, or even within the person's body). Rather than the modern connotation of "automated," the prefix "auto-" is intended here to convey its original meaning of "self-".

Progressively, surveillance ceased to be constrained to the observation of ephemera. The recording of signals meant that data trails could be built up, and that retrospective analysis could be undertaken of those trails. As the number of such trails increased, information originating from different times and places could be interwoven, enabling additional inferences to be drawn.

The monitoring of data-flows, and the analysis of data-holdings, are economically efficient because they can be automated. Furthermore, they are inherently surreptitious, so the watched are far less aware of the watchers than is the case with physical surveillance, even at a distance. As a result, dataveillance (a convenient contraction of "data surveillance") has been used to augment, and increasingly to substitute for, physical surveillance [8]. The volume of monitoring undertaken has also grown, because it is inexpensive, which enables more of it to be done within the same budget. The natural limitations on the number of people who can be hired to wear trench-coats and watch doorways have been overcome.

As telecommunications improved, a further capability was added. The data became available very soon after being collected, which meant that the trail was warm and real-time tracking could be conducted. This increased the chances of being able to intercept a target. It also introduced the possibility of predictive tracking, by inferring a target's intended destination.

As telecommunications developed, first telegraphic, then telephonic and later facsimile transmissions became vehicles for electronic surveillance. In recent decades, this has been extended to all forms of Internet communications, particularly those that depend on wired connections, but also on wireless channels.

Until recently, electronic communications supported the equivalent of speech. Generally, the law permitted connections monitoring or traffic analysis (which detects who is talking with whom) although it subjected such activities to controls. Because of the enormous intrusiveness and the risks involved in granting powers to law enforcement agencies, greater obstacles were placed in the way of communications surveillance (which discloses who is saying what to whom).

Since the advent of the Web in the early-to-mid-1990s, however, electronic communications have also supported the equivalents of buying books and going to the library. Monitoring being conducted by employers and governments is now far more intrusive, because what might be described as experience surveillance provides access not merely to what a person is saying, but also to what they are thinking about and researching.

Within each of the categories discussed above, it is important to distinguish two sub-categories:

- personal surveillance. This is focused on an identified person, generally for a specific reason. It is undertaken because suspicion has arisen from some other source;
- mass surveillance. This is less precisely targeted, and is imposed on groups of people, often large groups. Generally, its purpose is to identify individuals who belong to some particular class of interest to the surveillance organization. In short, it is a suspicion-generator, designed to produce candidates against whose actions counter-measures or pre-counters can be implemented, or who can be submitted to personal surveillance.

Physical surveillance was applied to a location or place. Enhancements enabled the watchers

and their equipment to be separated by some distance from the place being watched, but the locus of the surveillance remained the same. Three different categories of place are discernible; these might be described as private, controlled, and public.

The notion of private places relates to locations in which an individual, or two, or perhaps a few, could reasonably expect not to be subject to surveillance by other parties. This has seemed to have a central core of the marital bedroom, a more qualified zone comprising the rest of the home and even more so its visible exterior (gardens and patios), and some further outposts such as the insides of toilet cubicles.

Organizations that exercise substantial control over particular places have asserted the right to conduct surveillance where, when and how they wish. The contestability of claims in relation to controlled places increases from, for example, the rooms from which nuclear power stations and air traffic are controlled, via the footpaths outside government agencies and the faces presenting to ATMs, to railway stations and cinema precincts.

One interpretation of public place is "everywhere that is neither of the other two." Subscribers to the "original sin" philosophy assert that all forms of surveillance of public places are legitimate, on the grounds that privacy inherently doesn't exist in public places, or no longer exists in public places, or should not exist in public places. Yet people have always had reasonable expectations of privacy in public places. That applies all the more to people who are not well known. More generally, everyone has a reasonable expectation of privacy when they are behaving in a manner that is intended to be private, e.g., when in the company of family, rather than projecting themselves (or their "public persona") to some kind of "public." Because parliaments have been slow to protect such behaviors, the courts are being forced to develop a tort through case law.

> The old concepts of private, controlled, and public places have given way to private, controlled, and public spaces.

Electronic surveillance broke the nexus with a single location. Initially, it was feasible to re-define it to a multi-location phenomenon, as in the monitoring of both ends of a phone conversation. But first dataveillance and then new forms of electronic surveillance forced further re-thinking. It is now necessary to define the actions or communications that are subject to surveillance as occurring in "space" rather than "place", and to conceive of the space as being either physical or figurative (as in abstractions such as "cyberspace"). With that change, the old concepts of private, controlled, and public *places* have given way to private, controlled, and public *spaces*.

The purposes and potential benefits of surveillance are discussed in [16, sect. 2]. This article focuses primarily on its negative impacts.

Categorization of Surveillance

Drawing on the outline of the surveillance concept above, the following can be distinguished dimensions of surveillance applications.

1) Of What?
That which is subjected to surveillance may be a specified individual, specified groups of individuals, specified objects, specified groups of objects, or a specified space.

2) For Whom?
The beneficiaries of surveillance may be the individual who is the subject of the surveillance, an individual who has a direct interest in the subject of the surveillance, or another party with an interest in the behavior of the subject.

3) By Whom?
The surveillance may be conducted by the individual who is the subject of the surveillance, an individual who has a direct interest in the subject of the surveillance, another party with an interest in the behavior of the subject, or a third party who is in some sense acting on behalf of one of the above.

4) Why?
The primary purpose of the surveillance may be to assist with the health or safety of the subject of surveillance, to detect or collect evidence of behavior that conforms or does not conform with some norm, or to encourage conformant behavior and/or deter non-conformant behavior.

5) How?
The means whereby the surveillance is conducted may be physical surveillance (visual and aural), physical surveillance at distance, auto-surveillance, retrospective analysis, dataveillance, real-time tracking, predictive tracking, traffic analysis, communications surveillance, or experience surveillance; and each of them may be targeted personal surveillance or much broader mass surveillance.

6) Where?
The locus of the surveillance may be defined in physical space, or in some virtual space. A common form of virtual space is that enabled by electronic communication networks, but another is the web of ideas inherent in published text, uttered words, and recorded behavior.

7) When?
The timeframe in which surveillance is conducted may be defined across a single span of time, or recurrent spans (such as a particular

> Our world needs an antidote to "national security extremism," and it needs it fast.

span within each 24-hour cycle), or scattered across time (e.g., triggered by particular conditions detected in published text, uttered words, and recorded behavior), or continuous and unremitting.

The public and political acceptability, the legality, and the effectiveness of a particular instance of surveillance differ greatly depending on the design choices that it evidences. An approach to developing an ethical framework for surveillance is in [1].

What is Überveillance?

The theme of this special section originates in the work of Michael and Katina Michael, with the first published use in lecture notes [6]. The notion is emergent rather than established, and it continues to evolve. A useful working definition that they offer is "an above and beyond omnipresent 24/7 surveillance where the explicit concerns for misinformation, misinterpretation, and information manipulation, are ever more multiplied and where potentially the technology is embedded into our body" [7, p. 361].

The word überveillance appears not to have existed until Michael & Michael coined it. Its stem and suffix, "-veillance", are clearly co-opted from "surveillance". Originally, this derived from the French "surveiller", whose contemporary senses include "to keep an eye on" (e.g., luggage), to supervise (e.g., people), to monitor (e.g, people, an object or a space), and to invigilate (to watch candidates in an examination).

Judging by the entry in the Oxford English Dictionary, the word was co-opted into English in 1799, originally in a report on the French Revolution. The relationship was readily recognized with Bentham"s panopticon proposal, which originated in 1787 but was current for 25 years. During the 200 years since then, the English word "surveillance" has come to be used primarily with sinister associations. It has been subject to a number of adaptations and extensions, including this author's own neologism "dataveillance," of 1988, which the Michaels explicitly identify as one of the inspirations for their work.

The prefix "über" is drawn directly from German. Its several senses are investigated in the following sections.

Omni-Surveillance

An apocalyptic vision would see "überveillance" as referring to surveillance that applies across all space and all time (omni-present), and support some organization that is all-seeing and even all-knowing (omniscient), at least relative to some person or object. The apocalyptic theme is a key thread in M.G. Michael's work [2]–[5].

An effective way to achieve omni-surveillance would be to embed the surveillance mechanism within the person or thing to be monitored, and endow it with the capacity to monitor itself continuously, and report to a monitoring authority, whether periodically, by exception, or continuously. Applying the dictum that "information is power," this leads easily to a feeling of inevitability of the surveillance organization becoming an all-powerful (omnipotent) being.

On the one hand, this is the stuff of science fiction, and the dystopian genre within sci-fi at that. On the other hand, most of the elements needed to realize the nightmare already exist, including:

- chips with substantial capacity to gather, store, process and output data;
- devices containing such chips that can be reliably associated with individuals (as already occurs consensually with mobile phones, and nonconsensually with anklets and wristlets on various categories of the institutionalized, particularly prisoners, parolees, and even remandees);
- chips that can be (and, in small quantities already have been) embedded in humans;
- convenient, readily replenishable power sources for such chips (such as that already available when the carrier moves through a magnetic field to induce current in an antenna); and
- wireless networks through which data can be transmitted.

Remarkable as it may seem, some categories of people are being enveigled, coerced and even mandated to submit to such a "panelectricon," particularly as a condition of employment, or in return for reduced constraints on the space within which the individual is permitted to move. Aspects of the "digital persona" in contexts such as these are investigated in [13].

If the word "überveillance" achieves broad currency, this may well be the primary interpretation that our children and grandchildren have of it. The idea of überveillance remains somewhat speculative at this stage, however, and is sufficiently forbidding that many people are likely to remain "in denial." The following two alternative interpretations may therefore be of greater immediate relevance right now.

Exaggerated Surveillance

One interpretation of "überveillance" questions the extent to which surveillance is undertaken. This can be along various dimensions. For example, surveillance may be excessive because it has too broad a scope, or is instigated for reasons that are minor in comparison with

its negative impacts. In either case, its justification is exaggerated.

Costs and Disbenefits

Surveillance has costs and "disbenefits," and its benefits need to be balanced against them. The costs and disbenefits may be incurred by the organization conducting the surveillance, or by others, particularly the individuals subjected to it.

The term "costs" is used here in the financial sense, and includes all forms of expenditure, in particular on the conduct of the surveillance, on the infrastructure to support it, and on the analysis of the resulting data stream(s). It encompasses at least some of the costs of actions taken as a result of surveillance, in particular those actions that transpire to have been unjustified because they arose from "false positives."

The term disbenefits is used to encompass non-financial impacts that are negative, whether for the society, economy or polity as a whole, or only for some individuals or groups. The enormous scope of disbenefits arising from surveillance is exemplified by the list in Table I.

Controls Over Excesses

A crucial question in any organic system is the extent to which natural controls exist. If natural controls are in place and not seriously impeded, then the system may be best left to find its own equilibrium. If, on the other hand, the controls are impeded in a significant way, then some intervention may be needed, in order to overcome the impediments, or to stimulate the control aspects. In some settings, however, the system may be doomed to spiral out of control. In that case, the architecture is in need of overhaul if the system is to survive.

To what extent is surveillance an organic system, and which of those archetypes best describes it?

In [9], "intrinsic controls" over the particular dataveillance technique of data matching were examined. They were found to include:

- the exercise of countervailing political power by the class of data subjects affected by the process, by their representatives, by the mass media, or by the general public. Given the imbalance of power between organisations and individuals, it is not realistic to expect this factor to be of any great significance except in particular circumstances;
- the displeasure of some organisation, such as a competitor or regulatory agency;
- self-restraint practised by the agency itself, influenced by professional norms, or by an appreciation of the delicacy of public confidence in its institutions and the resultant need to respect constitutional rights and moral concerns; and
- general blundering.

Clarke concluded in 1995 [9] that "the intrinsic factor which might be expected to exercise the most significant degree of control over computer matching is economics: surely government agencies will not apply the technique in circumstances in which it is not worthwhile. The primary means whereby the economic factor will influence decision-making about computer matching programs is cost/benefit analysis". The various forms of cost/benefit analysis are described in [14] and [15].

Table I
Real and Potential Dangers of Dataveillance
Source: [8]

Dangers of Personal Dataveillance
Wrong identification
Low quality data
Acontextual use of data
Low quality decisions
Lack of subject knowledge of data flows
Lack of subject consent to, data flows
Blacklisting
Denial of redemption
Dangers of Mass Dataveillance
• To the Individual
Arbitrariness
Acontextual data merger
Complexity and incomprehensibility of data
Witch hunts
Ex-ante discrimination and guilt prediction
Selective advertising
Inversion of the onus of proof
Covert operations
Unknown accusations and accusers
Denial of due process
• To Society
Prevailing climate of suspicion
Adversarial relationships
Focus of law enforcement on easily detectable and provable Offences
Inequitable application of the law
Decreased respect for the law and law enforcers
Reduction in the meaningfulness of individual actions
Reduction in self-reliance and self-determination
Stultification of originality
Increased tendency to opt out of the official level of society
Weakening of society's moral fiber and cohesion
Destabilization of the strategic balance of power
Repressive potential for a totalitarian government

> The proponents of surveillance successfully avoid scrutiny of their proposals.

A mere decade later, that sentiment seems quaint. Today, government agencies have barely adopted so much as a pretense of conducting cost/benefit analyses. They have become thoroughly politicized, and "business cases" dominate. A "business case" differs from a cost/benefit analysis in two important ways. It is one-dimensional, because it adopts the view of the sponsor, rather than reflecting the varying perspectives of multiple stakeholders. Second, it is designed as a justification of a policy position that has already been adopted, rather than as an analytical tool.

In the surveillance arena, there has not only been little evidence of cost/benefit analysis being applied, there has seldom even been a compelling business case. The proponents of surveillance successfully avoid scrutiny of their proposals, especially since the windfall of terrorist strikes in New York and Washington, DC, in 2001, and what marketers refer to as "mid-life kickers" in Bali in 2002, in Madrid in 2004, and in London in 2005. Since 2001, surveillance has been implemented as an imperative, as those worst forms of policy-formation – knee-jerk reaction, the bandwagon effect, and sacrosanct slogans.

Surely, we might say, "the truth will out," user organizations will discover that "the emperor has no clothes," and the mythologies of surveillance will become common knowledg. Instead, an extraordinary phenomenon has emerged, that has not been evident in other contexts – alliances of vendors and user organizations. For example, the U.S. national security community has contrived the publication of tests and reports that have been grossly twisted and biased, in order to provide biometrics vendors with breathing space and credibility that their products do not warrant. The most extreme instance is in the laughably inadequate technology falsely projected as "facial recognition." Face Recognition Vendor Test (FRVT) projects have been breathtaking in their misrepresentation of reality. They were jointly sponsored in the U.S. by a group that included the Federal Bureau of Investigation (FBI), the National Institute of Standards, and Technology (NIST), and the Department of Homeland Security.

In Australia, a similar corruption has been mirrored in the Biometrics "Institute." The organization does not live up to its title. Its function is to provide a forum for the alignment of organizations whose interests, in an organic system, would be at considerable variance from one another. Government agencies and suppliers have conspired, and continue to conspire, to project biometrics technologies as things that they are not: effective, reliable, and safe for human consumption.

Corporations, unlike governments and government agencies, are subject to the constraints of return on investment (ROI). This somewhat tempers their enthusiasm for monitoring. For these reasons, the financial sector has long resisted the imposition of strong authentication on its customers. It also appears that the full power of consumer profiling and "customer relationship management" technology may not yet have been unleashed on Australian consumers.

But ROI has proven inadequate to ensure rational designs. The private sector too makes decisions that are far from balanced, because knee-jerk and bandwagon outweigh rationality. In addition, there has been increasing pressure from Governments, using such "motherhood and apple pie" sentiments as "money-laundering," "counter-terrorism," "homeland," and "critical infrastructure protection." The 2006-2007 rounds of "Anti-Money-Laundering and Counter-Terrorism Financing" (AML-CTF) legislation represent one of the most extreme forms of exaggeration to date, with business enterprises now obligatorily enlisted as spies against their customers.

Master-Surveillance

Another possible interpretation of "überveillance" derives from the use of "über" to imply "meta," "supra," or "master"-surveillance.

This could involve the consolidation of multiple surveillance threads in order to develop what would be envisaged by its proponents to be superior information. This might be performed *ad hoc*, as occurs in "intelligence assessment" agencies active in foreign affairs and national security.

The challenges are enormous, however. In particular, the dataflows are typically highly variable and unreliable. The bases on which they are conceived and implemented vary greatly between the streams. There may be considerable differences between the aims of each individual operator and the would-be "master." The challenges of diversity in data sources, data meaning and data quality were investigated in the context of data matching programs in [10].

In order to overcome the difficulties inherent in consolidating very different streams of information, there could be endeavors to achieve coordination among the various surveillance sources. An example of such an approach is the creation of an organization whose express purpose is to draw surveillance organizations closer together. A prime example was the creation of the U.S. Department of Homeland Security (which in the process changed the sense of

"DHS" from Human Services to something differently protective and much more sinister).

An approach that might seem superior to both consolidation and coordination is centralization. This involves the conception of an architecture intended from the outset to develop a set of feeds into a single "master," with all of the subsidiary surveillance processes serving the centrally-determined objectives. Stafford Beer naively thought that a centrally-planned cyber-economy could be consistent with an open society and a democratic polity. The experience of Beer's Cybersyn project (1970–1973) could have delivered the *coup de grace* to such Promethean idealism if Chile had not been seen to be acting against the interests of the American way of profit. Its elected President was eliminated, and with him Beer's experiment.

During the 1970s and 1980s, such "central planning" approaches were derided. To some extent this was due to their totalitarian nature, demanding as they do a controlled and inherently static society. But the primary reason was that they had been demonstrated not only behind the Iron Curtain, in Cuba, and under East Asian Communist regimes, but also in France, to lead to economic systems that were ineffective, inefficient, and in most cases stagnant.

Up to a point, systems exhibit efficiencies of scale, and efficiencies of scope. Beyond that point, they become unwieldy, excessively complex, and inherently unmanageable. Systems of the complexity of societies are well beyond the flex-point. They accordingly exhibit substantial inefficiencies of scale and of scope. General systems theory recognizes that, for large-scale systems to have the flexibility and adaptability that they need for survival, they need to comprise loosely coupled elements, and to be subject to control through the interplay of those elements rather than through any form of centrally-determined control.

What Do We Do About Überveillance?

The picture painted in the preceding sections may seem bleak. Surveillance is rampant. Human values have been trampled. Osama bin Laden and Al Qaeda, or rather the effigies that have been made of them, have triumphed. The limited and sporadic attacks in their names have struck at the moral weaknesses and contradictions inherent in the "Western," "democratic" world. That world has turned inward on itself. It is spiraling towards self-destruction through the denial of the very freedoms on which it was supposed to be built. Our world needs an antidote to "national security extremism," and it needs it fast.

The following discussion distills a few key messages about what we need to do in order to ensure survival of society, the economy, and the polity, in the face of rampant "control freaks." A small set of Principles is enunciated that is intended to contribute to the restoration of society by bringing the surveillance mania back under control. The intention is to generate countervailing power against the extremism of the national security agencies. In this context, a variant of the label "countervaillance" to "counterveillance" is appropriate. Table II lists the Principles.

The position adopted by the author in formulating these Principles is not extremist. There is common ground across society that terrorists are killing people from time to time, that there are (small numbers of) disaffected individuals who will be attracted to violent "solutions," that religious fundamentalism is a threat to open societies, that countermeasures are needed, and that both general alertness and capable public security institutions are needed.

Where this set of Principles might be seen by some to be radical is in the following:

- These Principles recognize that terrorism is not new and nor is it unusual.
- Although the "power to weight ratio" of a single strike has increased (because fewer terrorists can deliver a bigger payload), these Principles deny that this has particularly significant implications for public policy.
- The Principles refuse to accept reactionary extremism at face value, and to provide national security and law enforcement interests with *carte blanche* to do what they say needs to be done in order to counter the threats.
- The Principles deny that "secrecy" is a necessary precondition of "security."
- They reject the legitimacy of treating what are really "public safety" issues as though they were "national security" matters.

Table II
Counterveillance Principles

1) Independent Evaluation of Technology
2) A Moratorium on Technology Deployments
3) Open Information Flows
4) Justification for Proposed Measures
5) Consultation and Participation
6) Evaluation
7) Design Principles
   - Balance
   - Independent Controls
   - Nymity and Multiple Identity
8) Rollback

> The "Western" "democratic" world is spiraling towards self-destruction through the denial of the very freedoms on which it was supposed to be built.

- They are deeply sceptical about counter-terrorism depending on everyone having to be limited to a single State-managed identity, because this helps not at all against "virgin terrorists."

Independent Evaluation of Technology

Surveillance of the intensive kinds that are drastically altering our society are heavily dependent on technologies. The assertions of technologists and marketers must be viewed with scepticism, and subjected to testing. That testing must not be warped, and must not be conducted by participants in the field of play (such as the FBI, NSA, NIST, and, in Australia, the Defence Science & Technology Organisation – DSTO). Normal science and technology must be resumed. Rather than "Government policy" driving and twisting outcomes, rational consideration of technologies and their applications is essential.

A Moratorium on Technology Deployments

Some years ago, I called for a moratorium on biometric implementations in Australia [12]. I argued that "[a] ban must be imposed on the application of biometrics technologies until and unless a comprehensive and legally enforced regulatory regime has been established." This may have appeared quixotic. My rationale was not only that applications of biometrics had gross, negative impacts, but also that a moratorium might be the only means of saving an industry that has promised much for years and delivered very little.

There are enormous impediments to the adoption of "advanced technologies." In the majority of cases, their dysfunctions are considerable, and the extent to which they achieve their primary objectives is in serious doubt.

Open Information Flows

The antidote to inappropriate deployments of inadequate technologies is openness. The public needs facts about the context in which surveillance schemes are to be deployed. They need a statement of the scheme's objectives. They need to know sufficient details about the design features so that they can apply reasonable tests to the scheme's feasibility, and assess its effectiveness under varying circumstances. The public needs the opportunity to apply systemic reasoning in order to evaluate whether the design features can give rise to the claimed benefits.

Justification for Proposed Measures

No measure should be implemented unless its negative impacts are demonstrated to be outweighed by its benefits. It seems extraordinary that a case has to be mounted in support of such a straightforward contention. Yet national security and law enforcement agencies (NS&LEAs) have been permitted to make untested assertions about both threats to public safety and the benefits of surveillance measures in addressing those threats. Blind trust in NS&LEAs has to end. Those organizations must be required to present their arguments, and defend them in public.

Consultation and Participation

A further critical aspect of an open society is the ability of the public to participate in the debate. This enables testing of the information and arguments. It also brings the many perspectives of a complex society to bear on the information and the declared objectives.

Evaluation

Another form of normal service that needs to be resumed is the application of established techniques to the available information, in order to provide a basis for comparison among financial costs and benefits, on the one hand, qualitative factors on the second, and risks (and especially remote ones) on the third.

The technique of Privacy Impact Assessment (PIA) [17] has made headway during the last few years, and has attracted support now from such inherently conservative institutions in Australia as the Senate, the Privacy Commissioner, and in September 2007 the Australian Law Reform Commission (ALRC). An even broader notion of social impact assessment is crucial to the survival of an open society.

Design Principles

There are positive instances of surveillance, both for individuals and society. Surveillance is not itself evil. The problem has been the presumptiveness of its proponents, the lack of rational evaluation, and the exaggerations and excesses that have been permitted.

Proponents of surveillance have Design Principles that guide the creation of their systems. An alternative or complementary set of Design Principles is required, guiding the conception of schemes that do not threaten free society from within. Key examples includes the following:

- Balance. This must be achieved among the many competing values and interests, rather than a small cluster of "security" imperatives dominating, and being protected by a veil of secrecy.
- Independent Controls. These are essential in order to ensure that "national security"

interests are not the means whereby "national security" assertions are validated.

- Nymity and Multiple Identity. These must be recognised as natural human needs, and as keys to the freedoms in free society, despite the inevitability that they, like all freedoms, will be abused as well as used.

Nymity encompasses both anonymity and pseudonymity, and is addressed in depth in [11]. Genuine anonymity precludes the link being discovered between an identity and the entity or entities using it. It carries with it the risk of non-accountability. With pseudonymity, the link can be made, but its effectiveness depends on legal, organisational and technical protections, to ensure that the link is not made unless pre-conditions are fulfilled.

Rollback

Restoring sanity to the processes whereby schemes are evaluated and designed is crucial, but far from sufficient. The depredations of the last 5 years are so great that rollback of the great majority of anti-freedom provisions enacted is necessary.

This is not to suggest that every provision of every act must be overturned. National security and law enforcement agencies were, as they claimed, confronted by a variety of barriers that were accidental and inappropriate and needed to be overcome. On the other hand, inadequately brisk processes for the issue of warrants are not properly solved by creating extra-judicial warrants, but rather by a faster, online judiciary. And although telephonic interception warrants based on old, fixed-line numbering are inappropriate in the modern era of mobile phones, the balanced solution is person-based interception warrants, not the removal of controls.

National Security Fundamentalists

The English word "surveillance" derives from the French "surveiller", or "watch over", which in turn derives from the French sur- and the Latin *vigilare*. So "überveillance" takes a somewhat ambiguous Romance stem and imposes on it an abrupt and authoritarian Germanic prefix.

There are multiple flavors of "überveillance", none of them comforting to someone who lives in the real world of moderate daily dangers from cancer, heart conditions, and road traffic, and of minuscule dangers from terrorism.

Unfortunately, as this paper has shown, all of the interpretations of "überveillance" are descriptive of another reality, and one that has become rapidly more pervasive in the few years since the turn of the present century. We are confronted by the twin extremisms of religious fundamentalists in Muslim garb, on the one hand, and men in short haircuts chanting the mantra "national security," on the other.

We need to ensure that the national security fundamentalists, who have ruled our lives for the first decade of the new century, are treated with the same seriousness as the terrorist threat, and are encouraged to return to the professionalism of the 1980s and 1990s, and to the respect for the free society that democratic societies believe they live in. Our society wants neither "unter-veillance" (i.e., "under-veillance") nor "überveillance." It wants balance.

Author Information

The author is Principal of Xamax Consultancy Pty Ltd., and is a Visiting Professor at the University of New South Wales and at Australian National University.

References

[1] K. Michael, A. McNamee, and M.G. Michael, "The emerging ethics of humancentric GPS tracking and monitoring," in *Proc. Int. Conf. Mobile Business* (Copenhagen, Denmark), July 25–27, 2006, pp. 34–44.

[2] M.G. Michael, "The Number of the Beast, 666 (Revelation 13:16-18). An historical and theological investigation of Saint John's conundrum," M.A. Honors Thesis, Macquarie University, NSW, Australia, 1998, unpublished.

[3] M.G. Michael, "For it is the number of a man," *Bull. Biblical Studies*, vol. 19, pp. 79–89, Jan.–June 2000.

[4] M.G. Michael, "666 or 616 (Rev 13:18): Arguments for the authentic reading of the Seer"s conundrum," *Bull. Biblical Studies*, vol. 19, pp. 77–83, July–Dec. 2000.

[5] M.G. Michael, "The canonical adventure of the apocalypse of John in the early church (A.D. 96–A.D. 377)," Ph.D. thesis, Australian Catholic University, 2003, unpublished.

[6] M.G. Michael, "Consequences of innovation," lecture notes no. 13 for IACT405/905 – Information Technology and Innovation, School of Information Technology and Computer Science, University of Wollongong, Australia, 2006, unpublished.

[7] M.G. Michael and K. Michael, "National security: The social implications of the politics of transparency," *Prometheus*, vol. 24, no. 4 pp. 359–363, Dec. 2006.

[8] R. Clarke, "Information technology and dataveillance," *Commun. ACM*, vol. 31, no. 5, pp. 498–512, May 1988; also in *Controversies in Computing*, C. Dunlop and R. Kling, Eds. Academic, 1991.

[9] R. Clarke, "Computer matching by government agencies: The failure of cost/benefit analysis as a control mechanism" *Information Infrastructure & Policy*, vol. 4, no. 1, pp. 29–65, Mar. 1995.

[10] R. Clarke, "A normative regulatory framework for computer matching," *J. Computer & Information Law*, vol. XIII, no. 4, pp. 585–633, Summer 1995.

[11] R. Clarke, "Identified, anonymous and pseudonymous transactions: The spectrum of choice," in *Proc. User Identification & Privacy Protection Conf.* (Stockholm, Sweden), June 14–15, 1999.

[12] R. Clarke, "Why biometrics must be banned," presented at the Cyberspace Law & Policy Centre Conf. "State Surveillance after September 11," (Sydney, Australia), Sept. 8, 2003.

[13] R. Clarke, "Human-artefact hybridisation and the digital persona," background information for an Invited Presentation to Ars Electronica 2005 Symp. Hybrid – Living (Paradox, Linz, Austria), Sept. 2–3, 2005.

[14] R. Clarke, "Business cases for privacy-enhancing technologies" in *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*, R. Subramanian, Ed. IDEA Group, 2007.

[15] R. Clarke and K. Stevens, "Evaluation or justification? The application of cost/benefit analysis to computer matching schemes," in *Proc. Euro. Conf. Info. Syst.* (Cork, Ireland), June 19–21, 1997.

[16] M. Wigan and R. Clarke, "Social impacts of transport surveillance," in *Proc. RNSA Workshop on Social Implications of Information Security Measures upon Citizens and Business* (Wollongong, Australia), May 2006.

[17] R. Clarke, "Privacy impact assessment: Its origins and development," *Computer Law & Security Rev.*, vol. 25, no. 2, pp. 123–135, Apr. 2009; http://www.rogerclarke.com/DV/PIAHist-08.html