University of Wollongong
Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

2006

National Security: The Social Implications of the Politics of Transparency

M. G. Michael
University of Wollongong, mgm@uow.edu.au

K. Michael
University of Wollongong, katina@uow.edu.au

Publication Details

This article was originally published as: Michael, MG & Michael, K, National Security: The Social Implications of the Politics of Transparency, Prometheus, 2006, 24(4), 359-364. The journal is available here from Taylor & Francis journals.

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

National Security: The Social Implications of the Politics of Transparency

Abstract
This special issue of Prometheus is dedicated to the theme of the Social Implications of National Security Measures on Citizens and Business. National security measures can be defined as those technical and non-technical measures that have been initiated as a means to curb breaches in national security, irrespective of whether these might occur by nationals or aliens in or from outside the sovereign state. National security includes such government priorities as maintaining border control, safeguarding against pandemic outbreaks, preventing acts of terror, and even discovering and eliminating identification fraud. Governments worldwide are beginning to implement information and communication security techniques as a way of protecting and enhancing their national security. These techniques take the form of citizen identification card schemes using smart cards, behavioural tracking for crowd control using closed-circuit television (CCTV), electronic tagging for mass transit using radio-frequency identification (RFID), e-passports for travel using biometrics, and 24x7 tracking of suspected terrorists using global positioning systems (GPS). The electorate is informed that these homeland security techniques are in actual fact deployed to assist government in the protection of its citizenry and infrastructure. The introduction of these widespread measures, however, is occurring at a rapid pace without equivalent deliberation over the potential impacts in the longer term on both citizens and business.

Keywords
national security, information and communication technologies, risk, surveillance, privacy, security

Disciplines
Physical Sciences and Mathematics

Publication Details
This article was originally published as: Michael, MG & Michael, K, National Security: The Social Implications of the Politics of Transparency, Prometheus, 2006, 24(4), 359-364. The journal is available here from Taylor & Francis journals.

This journal article is available at Research Online: http://ro.uow.edu.au/infopapers/390

National Security: The Social Implications of the Politics of Transparency

M.G. Michael & Katina Michael

This special issue of *Prometheus* is dedicated to the theme of the Social Implications of National Security Measures on Citizens and Business. National security measures can be defined as those technical and non-technical measures that have been initiated as a means to curb breaches in national security, irrespective of whether these might occur by nationals or aliens in or from outside the sovereign state. National security includes such government priorities as maintaining border control, safeguarding against pandemic outbreaks, preventing acts of terror, and even discovering and eliminating identification fraud. Governments worldwide are beginning to implement information and communication security techniques as a way of protecting and enhancing their national security. These techniques take the form of citizen identification card schemes using smart cards, behavioural tracking for crowd control using closed-circuit television (CCTV), electronic tagging for mass transit using radio-frequency identification (RFID), e-passports for travel using biometrics, and 24x7 tracking of suspected terrorists using global positioning systems (GPS). The electorate is informed that these homeland security techniques are in actual fact deployed to assist government in the protection of its citizenry and infrastructure. The introduction of these widespread measures, however, is occurring at a rapid pace without equivalent deliberation over the potential impacts in the longer term on both citizens and business.

Governments today maintain a patchwork of information systems and technologies, each limited in their scope, and each system claiming seamless interoperability with the other. Literally hundreds of millions of taxpayer dollars have been used to implement band-aid solutions that are workable for the interim but have increasingly become an administrative nightmare. With each mass-market solution government claims to be saving costs or undergoing optimisation, and with each aftermath of implementations the real costs are identified and the alleged benefits diminished. Technology observers remain sceptical how some government *super*-schemes- despite their identifiable flaws from the outset- still make it right through to operation.

It has been argued in recent times and with an increasing frequency, that no information system is absolutely foolproof, so the introduction of truly global solutions is fraught with a range of intrinsic dangers. Moreover while software vendors pronounce bug-free systems and hardware vendors continue to lay claim to their equipment uptime to adhere to the 99.9999% principle of availability, it is the notion of "singularities" that becomes a disturbing factor. That is, what can go wrong in times of system outages, what services can still be processed without compromise when there is no power and backup battery generators have reached their limits. And what happens when someone does penetrate the system's security defences and goes unnoticed. Secondary issues are related to traditional problems such as who has access to reading and updating individual fields in personal records ensuring confidentiality, the source of origin of data and the integrity of the data, and the mechanisms present to protect citizens from system and human errors. At first glance these problems appear to be technical in nature, but in practice have more to do with the actual processes of decision-making.

Since automation, particularly computerisation, governments have increasingly looked towards *cradle-to-grave* surveillance; and now thanks to new and improved ICT capabilities and innovative government-to-business (G2B) relationships, they have 24x7 surveillance as well. Terrorism (from whatever ideological perspective we might approach the subject), has acted as a dominant catalyst for the widespread adoption of information and communication technology (ICT) since September 11th 2001. With each new adoption of ICT, vendors of networks, hardware and software (whose principal goal is to seek profit maximisation) count the potential revenues from the opportunity to implement nation-wide solutions. In addition, a deregulated marketplace now allows for private enterprises to partially provision (or even fully in some instances) government services, giving rise to the possibility of vested interests by a number of stakeholders. Government offshore and outsourcing agreements by their very nature pose a risk to national security, despite the legalities of service level agreements (SLA) and other contractual obligations. Business, too, is now expected to cooperate with government agencies to provide detailed lists of transactions by suspected persons such as mobile telephone calls or SMS (including complete conversations), bank and credit-card statements, e-mail/ voicemail, and other personal information such as sites browsed on the Internet. Warrants can now be issued by federal judges to federal and state law enforcement agencies authorising the interception of communications by means of any "telecommunication device" used by persons of interests, and other innocent third parties linked to persons of interest.

Concepts of *privacy*, at least in the tradition of western liberalism, touch on freedom, trust, the right to be left alone, obedience, and free will. And today few things are truly private in the more literal sense of "confidentiality" and "secrecy". Whatever George Orwell might have imagined in his satirical and futuristic *1984*, are we, ourselves, about to embark on a prison-like existence behind virtual bars? It has less to do with having anything to hide and more to do with the feeling that *Big Brother* is watching, controlling our private lives. We have laws for stalking, and we have laws for wire-tapping and digital recordings but what have happened to our laws on privacy. Privacy laws seem to be currently in conflict with lawful interception, and have certainly not kept pace with new ICTs. These emerging technologies will also inevitably give rise to new expressions of mental illness- for example the 'legitimate' preoccupation/ obsessiveness of being watched by someone else, *all the time*. And this will not be through a window but a camera- a supposed intelligent system that can compute certain images and conclude something meaningful about you and what you represent: like the so-called fact that you are linked to suspected criminals because you attend a football match and happen to look like someone else, because somehow your biometric has been permanently 'changed' in the official back-end system and you are denied access or entry because you simply do not add up, and about being at the wrong place at the wrong time and find yourself being questioned for something you never did. The potential scenarios are limited only by our imagination; and the ghosts in the machine. These will not be mere typographical errors to be leisurely brushed away.

Numbers, pure and simple, are all-pervading. Everywhere we turn we have numbers, and nowadays not only numbers but passwords. It is a reality many of us have learnt to live with and have with time taken for granted. We have gone through waves of innovation that have related names to numbers, numbers to smart cards- even our

biometric pattern is denominational. Currently we are at the brink of infringing a sensitive area of privacy. We are now expected to give something away freely, that is rightfully ours- our own *personal* biometric. To some degree this is equivalent to being asked to transfer our "power of attorney" to someone or something we do not have control over. In this case, it is not a question of whether a citizen trusts their government to act appropriately or not, but it has to do with the basics of human rights. This is a technological anomaly, given that many of us still cringe in attaching a copy of our hand-written signature in a digital message, and now we are being asked to hand over something of far greater value in the form of unique biometric minutiae. It will not be too long before we are requested and then required to provide more than one biometric pattern for the ease of using multimodal biometric solutions internationally. This means that we are progressively losing the right to be known by our own name, but also the impression that we no longer own a part of our own body (even if outwardly this appears to be *computational*).

Realistically, what could come next? The cognizant go-ahead to grant a third party authority, such as a government or service provider, virtually unreserved control over our personhood by permitting RFID transponders to penetrate the skin? This would not simply equate to "dataveillance" but to "überveillance"- an above and beyond omnipresent 24x7 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. Who would own such a comprehensive information system? Who would have the right to make amendments to the databases? Trenchant arguments that such extreme scenarios only turn up in the active imaginations of civil libertarians, conspiracy theorists, and religious fundamentalists are steadily losing ground. Device implants for medical purposes have been readily available since the 1970s, today the difference is that they are as small as a grain of rice and manifestly more powerful and can be used as much for ID purposes as any other application.

The philosophical debate for most technologists is whether a system of moral principles should have any considerable place in the new government mandated ICT implementations. Simply stated one of the primary questions in an ethical discussion of this type would be, *is technology neutral*? We seem to eschew deliberations over what is right or wrong or good or bad and are hesitant to critically engage with questions of morality. We would rather thrash out issues of whether *society shapes technology* or *technology shapes society*, and while this is an important area of study, we might be missing the mark. Are questions of future sustainability too difficult for us to discuss if they involve bringing some type of ideology into the equation? Should we not also be asking ourselves what sort of future we hope to generate and to live in? Many engaged in the terrorism debate are so engrossed in the topic that they suffer from a type of tunnel vision without too much consideration for the externalities that might occur from particular 'solutions'. The growing interconnectedness of systems means that any ICT solution proposed by powerful nation states will be rapidly adopted by other nations. Truly global solutions while seemingly convenient on the surface, lend themselves to wide-ranging dangers. Certainly, policies and procedures are important, so are laws and regulations, and standards, and guidelines but these all seem to be more exactly "reactionary" to the status quo. Studies have recently shown that at the height of terrorist events or other national security issues, public sentiment is swayed by media coverage, the public perception itself, and government statements.

As a result sweeping changes are introduced in a short period of time, particularly "changes" with large pieces of legislative content. There never seems to be enough time for additional public consultation, for broad debate and discussion; time to consider the consequences of the implementation of these far reaching decisions and for the scrutiny of their overall effect on the community in the long-term.

We seem to have become captive to a whirlpool cycle of surplus change, a capital accumulation of power house capabilities without the follow-on forethought. New government and business challenges are created as emerging technologies and are prematurely released to the market, still newer technologies are invented to overcome the challenges, laws are instituted to set the bounds of how technology should and should not be used and people are ultimately expected to learn to live with the implications and complications. Information and communication security measures adopted in haste in response to terrorism and other national security breaches have only acted to increase this cycle of change. There is also an underlying paradox in all of this which political sceptics would have already noted. Though in recent years governments are ostensibly committed to reducing state power, they have in reality increased it massively.

This issue of *Prometheus* introduces the reader to a wide array of perspectives on the topic of National Security from interdisciplinary fields of study, including philosophy, sociology, history, law, information and communication technology, and business. The volume acknowledges the difficulties of interdisciplinary research, especially the differences in approach and methodology, but also clearly evidences to the coherence in findings between schools of thought seemingly poles apart. The issue contains seven papers, proceedings from a workshop that was held in Australia on the 29th of May 2006, sponsored by the Research Network for a Secure Australia (RNSA). This issue will bring readers up-to-date on the current and potential status of information security measures, their implications on citizens and business, and their impact on legislation and privacy at a local and global level. Those stakeholders involved in implementation should be aiming to ethically integrate new technologies into society or run the risk potential for enhanced national security to come at the cost of freedom. There are many questions linked to this trade-off. Some of these include: How much technology is too much and whether technology is really the answer to all our problems? Can we legitimately claim that system safeguards ensure error-free databanks in monolithic-style systems? How does society ensure that authorities use the data in global systems appropriately and that stakeholders do not misuse their powers of read/write access? How voluntary is enrolment in these new schemes and how interlinked are citizen benefits to participation? And finally, what trajectory will the implementation of national citizen systems follow. Where to next? And what level of invasiveness into our personal lives are we willing to accept in the name of *security*.

Michael and Michael's paper is a historical review of prominent identification techniques throughout the ages and how they have been used, or misused, by people in authority. Jackson and Ligertwood's paper is a comparative legal study on the proposed UK citizen ID card and proposed Australia Card. Wigan and Clarke look at the broader context of information and security techniques in transportation and present the interconnectedness of seemingly disparate schemes. Tootell's paper

focuses on the study of location-based services in national security, and calls for the use of new methodological approaches to national security problems using the socio-critical theory approach which considers the lifeworld view. Bronitt and Stellios' paper analyses the Telecommunications Interception and Access (TIA) Act of Australia and reveals the increasing powers of government authorities with a view toward the need for changes to legislation. Rix follows with a studied criticism of the new anti-terrorism laws in Australia with respect to the community legal sector. Resnyansky completes the contributions by identifying the weaknesses of using solely quantitative modelling techniques for combating terrorism and focuses on the notion of critical reflexivity as a way to uncover the root causes of breaches in national security.

While the volume for the greater part is dedicated to an Australian context, global events and examples are used throughout to illustrate the major issues. In fact the lessons gained from the Australian context, can be applied comparatively to other nation states, particularly given the similarities and speed with which the UK and USA have paralleled their roll-outs of laws and proposed amendments to laws and adoption of information and communication security measures. The consequences of these initiatives will take some time to be felt but already we can predict with some confidence what some of the shortfalls will be. Postmodernist theory might have us believe that the profession of history is in crisis and that its methods are outmoded, but as Richard Evans and others have effectively argued, the discipline can teach us many lessons and provide us with "genuine insights". And in the context of technology itself, thinkers in the sociological tradition of Lewis Mumford and Jacques Ellul continue to challenge us to stop for a moment and to critically evaluate the unchecked consequences upon our civilization of an "artificial environment".

Whatever happens, whatever road is taken or 'not taken', the irreversible consequences of our "technicized" society will be felt by future generations. This is perhaps a traditional problem that has less to do with technology and more to do with people. Are we continually building new defences with a "catch me if you can" way of thinking, and "here, try penetrating my latest solutions", or are we genuine about peaceful resolutions which look at the root causes of national security concerns? The question is how much room are we truly leaving ourselves for future modification and change, if we go ahead and implement what we are proposing today? For the record, no one is debunking technology; there are no neo-Luddites here. The basic point is, to remain the masters over that which we create, and to not allow for the *machine* to dictate the terms and boundaries of our existence.