Necipujtenas.cz

2007

A Note on Überveillance / A Note on Uberveillance

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

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

Publication Details

This article was originally published as Michael, MG and Michael K, A Note on Überveillance / A Note on Uberveillance, From Dataveillance to Überveillance and the Realpolitik of the Transparent Society, The Second Workshop on Social Implications of National Security, Wollongong, Australia, 29 October 2007, 9-26.

A Note on Überveillance / A Note on Uberveillance

Abstract

The following note from the editors presents a summary of the term überveillance, as it was originally presented by the primary author in May 2006. Überveillance is an above and beyond, an exaggerated, an omnipresent 24/7 electronic surveillance. It is a surveillance that is not only "always on" but "always with you" (it is ubiquitous) because the technology that facilitates it, in its ultimate implementation, is embedded within the human body. The problem with this kind of bodily invasive surveillance is that omnipresence in the 'material' world will not always equate with omniscience, hence the real concern for misinformation, misinterpretation, and information manipulation.

Keywords

surveillance, dataveillance, überveillance, uberveillance, radio-frequency identification (RFID), microchip implants, social implications

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as Michael, MG and Michael K, A Note on Überveillance / A Note on Uberveillance, From Dataveillance to Überveillance and the Realpolitik of the Transparent Society, The Second Workshop on Social Implications of National Security, Wollongong, Australia, 29 October 2007, 9-26.

2

A Note on 'Überveillance'

M.G. Michael[1] and Katina Michael[2]

[1]Honorary Fellow, [2]Senior Lecturer, School of Information Systems and Technology, University of Wollongong

Abstract

The following note from the editors presents a summary of the term *überveillance*, as it was originally presented by the primary author in May 2006. Überveillance is an *above* and *beyond*, an *exaggerated*, an omnipresent 24/7 electronic surveillance. It is a surveillance that is not only "always on" but "always with you" (it is *ubiquitous*) because the technology that facilitates it, in its ultimate implementation, is embedded within the human body. The problem with this kind of bodily invasive surveillance is that *omnipresence* in the 'material' world will not always equate with *omniscience*, hence the real concern for misinformation, misinterpretation, and information manipulation.

Keywords: surveillance, dataveillance, überveillance, radio-frequency identification (RFID), microchip implants, social implications

1 Überveillance- an emerging concept

Überveillance is an emerging concept, in the full sense of both its application and power it is not yet arrived (M.G. Michael 2007). For some time Roger Clarke's (1988, p. 498) *dataveillance* has been prevalent: the "systematic use of personal data systems in the investigation or monitoring of the actions of one or more persons". Almost twenty years on, technology has developed so much and the national security context has altered so greatly (Snow 2005), that there was a pressing need to formulate a new term to convey both this present reality, and the *Realpolitik* (policy primarily based on power) of our times. It should be said, however, that if it had not been for dataveillance, überveillance could not be. And for that matter, it must be emphasized that dataveillance will always be- it will provide the scorecard for the engine being used to fulfill überveillance.

Überveillance takes that which was "static" or "discrete" in the dataveillance world, and makes it "constant" and "embedded". Consider it not only "automatic" and to do with "identification" BUT also about "location"- that is, the ability to automatically locate AND identify- in essence the ability to perform *automatic location identification* (ALI). It has to do with the fundamental "who" (ID), "where" (location), "when" (time) questions in an attempt to derive "why" (motivation), "what" (result), and even "how" (method/plan/thought). Überveillance can be a predictive mechanism for one's expected behaviour, traits, characteristics, likes or dislikes; or it can be based on historical fact, or something in between. The inherent problem with überveillance is that facts do not always add up to *truth* (ie as in the case of an exclusive disjunction T+T=F), and predictions based on intelligence are not always correct.

Überveillance is more than closed circuit television (CCTV) feeds, or cross-agency databases linked to national identity cards, or biometrics and ePassports used for international travel. Überveillance is the sum total of all these types of surveillance and the deliberate integration of an individual's personal data for the continuous tracking and monitoring of identity and location in real time. In its ultimate form, überveillance has to do with more than automatic identification technologies that we carry with us. It has to do with "under the skin" technology that is embedded in the body like microchip implants; it is that which cuts into the flesh- a charagma ("mark"). Think of it as Big Brother, on the inside looking out. This charagma is virtually meaningless without the hybrid network architecture which supports its functionality: to make the person a walking online node, beyond luggable mobile phones, PDAs and smart cards. We are referring here, to the lowest common denominator, the smallest unit of tracking- presently a tiny chip in the body of a human being.

Implants cannot be left behind, cannot be lost, 'cannot' be tampered with, they are always on, can link to objects, make the person seemingly otherworldly. This act of *chipification* is best illustrated by the ever-increasing uses of implant devices for medical prosthesis and for diagnostics (Swedberg 2007). Humancentric implants are giving rise to the *Electrophorus* (Michael & Michael 2007, p. 313), the bearer of electric technology; an individual entity very different to the sci-fi notion of *Cyborg* as portrayed in such popular television series as the *Six Million Dollar Man* (1974-1978). In its current state the Electrophorus relies on a device being triggered wirelessly when it enters an electromagnetic field; these properties now mean that "systems" can interact with people within a spatial dimension, and for the greater part unobtrusively. And it is surely not simple coincidence that alongside überveillance we are witnessing the philosophical reawakening (throughout most of the fundamental streams running through our culture) of Nietzsche's *Übermensch*– the overcoming of the "all-too-human" (Honderich 1995b).

That we might establish that chip implants are not mere science-fiction we need to identify a number of sources which add confirmation to the current reality. It is important to do so because the widespread misconception by information and communication technology (ICT) and engineering researchers at international conferences attended by both authors, is that chip implants are not commercially available for a variety of applications, and that the technology is not relevant to national security *per se*. Some researchers even believe that RFID implants have naught to do with "tracking" and can only be used for "identification". The following accounts and background sources should place things into perspective, at least at an overview level (see also, K. Michael 2007).

In March of 2005 the European Group on Ethics (EGE) in Science and New Technologies, established by the European Commission (EC), submitted an Opinion on ICT implants in the human body (Rodotà & Capurro 2005). The thirty-four page document outlines a number of legal and ethical issues to do with ICT implants and is premised around the European Union Treaty (Article 6) which has to do with the "fundamental rights" of the individual. Fundamental rights have to do with human dignity, the right to the integrity of the person, and the protection of personal data. From the legal perspective the following was ascertained (Rodotà & Capurro 2005, pp. 18-19):

> a) the existence of a recognised serious but uncertain risk, currently applying to the simplest types of ICT implant in the human body, requires application of the precautionary principle. In particular, one should distinguish between active and passive implants, reversible and irreversible implants, and between offline and online implants;
> b) the purpose *specification principle* mandates at least a distinction between medical and non-medical applications. However, medical applications should also be evaluated stringently and selectively, partly to prevent them from being invoked as a means to legitimise other types of application;
> c) the *data minimisation principle* rules out the lawfulness of ICT implants that are only aimed at identifying patients, if they can be replaced by less invasive and equally secure tools;
> d) the *proportionality principle* rules out the lawfulness of implants such as those that are used, for instance, exclusively to facilitate entrance to public premises;
> e) the *principle of integrity and inviolability of the body* rules out that the data subject's consent is sufficient to allow all kinds of implant to be deployed; and
> f) the *dignity principle* prohibits transformation of the body into an object that can be manipulated and controlled remotely – into a mere source of information.

The conclusion is that ICT implants for non-medical purposes violate fundamental legal principles. From the ethical perspective, ICT implants have numerous issues, including the requirement for: non-instrumentalisation, privacy, non-discrimination, informed consent, equity, and the precautionary principle (see also IEEE 2007; Lewan 2007a; Burton and Stockhausen 2005). It should be stated, however, that the EGE while not recommending ICT implants for non-medical applications because they are fundamentally fraught with legal and ethical issues, did state the following (Rodotà & Capurro 2005, p. 32):

> ICT implants for surveillance in particular threaten human dignity. They could be used by state authorities, individuals and groups to increase their power over others. The implants could be used to locate people (and also to retrieve other kinds of information about them). This might be justified for security reasons (early release for prisoners) or for safety reasons (location of vulnerable children).
>
> However, the EGE insists that such surveillance applications of ICT implants may only be permitted if the legislator considers that there is an urgent and justified necessity in a democratic society (Article 8 of the Human Rights Convention) and there are no less intrusive methods. Nevertheless the EGE does not favour such uses and considers that surveillance applications, under all circumstances, must be specified in legislation. Surveillance procedures in individual cases should be approved and monitored by an independent court.
>
> The same general principles should apply to the use of ICT implants for military purposes.

Although this Opinion was entirely comprehensive for its time, we hold growing concerns for the development of the information society, the lack of public debate and awareness regarding this emerging technology, and the pressing need for regulation that has not eventuated commensurate to developments in this domain.

Herein rests the problem of human rights and the “balance” between freedom, security and justice. First, it is a built-in fallacy to speak of a balance. In the microchip implant scenario, there will never be a balance, so long as someone else has the potential to control the implant device or the stored data about us which is linked to the device. Second, we are living in a period where chip implants for the purposes of *segregation* are being discussed seriously by health officials and politicians. We are speaking here of the identification of groups of people in the name of “health management” or “national security.” We will almost certainly witness new, and more fixed forms, of ‘electronic’ apartheid. Whatever the guise of parliamentary speak we are not far from such potentially explosive perils as a global community.

Consider the very real case where the "Papua Legislative Council is deliberating a regulation that would see microchips implanted in people living with HIV/AIDS so authorities could monitor their actions" (Somba 2007). Similar discussions on "registration" were held regarding asylum seekers and illegal immigrants in the European Union (Hawthorne 2001). RFID implants or the "tagging" of populations in Asia (eg Singapore) were also considered "the next step" in the containment and eradication of the Severe Acute Respiratory Syndrome (SARS) in 2003 before it subsided (RFID 2003). Apart from disease outbreaks, RFID has also been discussed as a response and recovery device for emergency services personnel dispatched to terrorist disasters (BBC 2005), and for the identification of victims of natural disasters, such as in the case of the Boxing Day Tsunami (Channel 2005). The question remains whether there is a truly legitimate use function of chip implants for the purposes of emergency management as opposed to other applications. 'Definition' plays a critical role in this instance. A similar debate has ensued in the use and application of the Schengen Information System (SIS) II in the European Union where differing states have recorded alerts on individuals based on their definition and understanding of "security risk" (Guild and Bigo 2002).

In June of 2006, legislative analyst, Anthony Gad, reported in brief 06-13 for the *Legislative Reference Bureau*, that:

> 2005 Wisconsin Act 482, passed by the legislature and signed by Governor Jim Doyle on May 30, 2006, prohibits the required implanting of microchips in humans. It is the first law of its kind in the nation reflecting a proactive attempt to prevent potential abuses of this emergent technology.

Today a number of states in the United States have passed similar laws, despite the fact that the U.S. Food and Drug Administration (FDA, 2004) at the national level have allowed radio frequency identification implants for medical use in humans. The Wisconsin Act (2006) states:

> The people of the state of Wisconsin, represented in senate and assembly, do enact as follows: SECTION 1. 146.25 of the statutes is created to read: 146.25 Required implanting of

> microchip prohibited. (1) No person may require an individual to undergo the implanting of a microchip. (2) Any person who violates sub. (1) may be required to forfeit not more than $10,000. Each day of continued violation constitutes a separate offense.

North Dakota was the next state to follow Wisconsin's example. Governor John Hoeven signed a two sentence bill into state legislature on 4 April 2007. The bill was criticised by some who said that while it protected citizens from being "injected" with an implant, it did not prevent someone from making them swallow it (Songini 2007). More recently, Californian Governor Arnold Schwarzenegger, signed bill SB 362 proposed by state Senator Joe Simitian barring "employers and others from forcing people to have a radio frequency identification (RFID) device implanted under their skin" (Woolfolk 2007; Jones 2007). According to the Californian Office of Privacy Protection (2007) this bill

> …would prohibit a person from requiring any other individual to undergo the subcutaneous implanting of an identification device. It would allow an aggrieved party to bring an action against a violator for injunctive relief or for the assessment of civil penalties to be determined by the court.

The bill which will be effective 1 January 2008, did not receive support from the technology industry on the contention that it was "unnecessary".

Interestingly, however, it is in the United States, that most chip implant applications have come to pass despite the calls for caution. This is not surprising given the first human-implantable passive RFID microchip (the VeriChip^{TM}) was approved for medical use in October of 2004 by the U.S. Food and Drug Administration. Today the VeriChip Corporation has 900 hospitals across the United States that have registered the VeriMed system, and now the corporation's focus has moved to "patient enrollment" including people with diabetes, Alzheimer's and dementia (Diabetes News 2007). The VeriMed^{TM} Patient Identification System is used for "rapidly and accurately identifying people who arrive in an emergency room and are unable to communicate" (VeriChip 2007).

In July of 2006 (The Age, 2007), CityWatcher.com reported two of its employees had "glass encapsulated microchips with miniature antennas embedded in their forearms… merely a way of restricting access to vaults that held sensitive data and images for police departments, a layer of security beyond key cards and clearance codes." It is not difficult to see how implants may soon find themselves being applied to the corrective services sector (RFID 2006). In 2002, 27 of 50 American states were using some form of satellite surveillance to monitor parolees. Similar schemes have been used in Sweden since 1994. In the majority of cases, parolees wear wireless wrist or ankle bracelets and carry small boxes containing the vital tracking and positioning technology. The positioning transmitter emits a constant signal that is monitored at a central intelligence point (Michael & Masters 2006a). Despite continued claims by researchers that RFID is only used for identification purposes, *Health Data Management* (2005a) disclosed that VeriChip (the primary commercial RFID implant patient ID provider) had enhanced its patient wander application by adding the ability to follow the "real-time location of patients, the ability to define containment areas for different classes of patients, and one-touch alerting. The system now also features the ability to track equipment in addition to patients." A number of these issues have moved the American Medical Association to produce an ethics code for RFID chip implants. Due to copyright restrictions, we cannot quote this code here but it can be sourced online (Sade 2007; Reichman 2006; Bacheldor 2007).

In chip implant cases outside the U.S. we also find a number of diverse applications for humancentric RFID. VeriChip's Scott Silverman had stated in 2004 that 7,000 chip implants had been given to distributors of which it was estimated 1,000 chips had been implanted in humans by year end worldwide (Weissert 2004). Today the number of VeriChip implantees is estimated to be at about 2,000. So where did all these chips go? Well, they may not be mainstream applications, but they are in operation. As far back as 2004, a nightclub in Barcelona, Spain, the *VIP Baja Beach Club* in Catalan City (Chase 2007) was offering "its VIP clients the opportunity to have a syringe-injected microchip implanted in their upper arms that not only [gave] them special access to VIP lounges, but also [acted] as a debit account from which they [could] pay for drinks" (Morton 2004). Microchips have also been implanted in 160 Mexican officials in the law enforcement sector (Weissert 2004). "Mexico's top federal prosecutors and investigators began receiving chip implants in their arms… in order to get access to restricted areas inside the attorney general's headquarters." In this instance, the implant acted as an access control security device despite the documented evidence purporting to the fact that RFID is not a secure technology at all (see *Gartner Research* report by Reynolds 2004).

In the United Kingdom, *The Guardian* (Wilson 2002), reported that 11-year old Danielle Duval had an active chip (i.e. containing a rechargeable battery) implanted in her. Her mother believes that it is no different to tracking a stolen car, simply that it is being used for another more important application. Mrs Duvall is considering implanting her younger daughter age 7 as well but will wait until the child is a bit older, "so that she fully understands what's happening". In Tokyo, Japan, the Kyowa Corporation in 2004 manufactured a schoolbag with a GPS device fitted into it, to meet parental concerns about crime, and in 2005 Yokohama City children were involved in a four month RFID bracelet trial using the I-Safety system (Swedberg 2005). In 2007, we now have a company in Lancashire in England, Trutex, which is seriously considering fitting the school uniforms they manufacture with RFID (Meikle 2007). What might be next? Concerned parents enforce microchip implants on minors?

More recently decade-old experimental studies on microchip implants in rats have come to light tying the device to tumours (Lewan, 2007b). The American Veterinary Medical Association (AVMA 2007) was so concerned with the report that on 13 September 2007 they released the following statement, quoted here in full:

> The American Veterinary Medical Association (AVMA) is very concerned about recent reports and studies that have linked microchip identification implants, commonly used in dogs and cats, to cancer in dogs and laboratory animals. AVMA staff and member veterinarians are actively looking into any potential for this technology to induce tumor formation in dogs, cats, or people but must await more definitive data and test results before taking further action. Based on the fact that a large number of pets have already been implanted with this microchip technology and there has been a relatively small number of confirmed cases of chip-induced tumors, the AVMA

> advises pet owners against a rush to judgment on the technology. In fact, there is a concern among veterinary medical researchers that some of the research into chip-induced tumors may be flawed, because the animals used were genetically predisposed to cancer. In addition, **removal of the chip is a more invasive procedure and not without potential complications**. It's clear that there is a need for more scientific research into this technology. [bold eds.]

We can see here, already, evidence pointing to the notion of 'no return'- an admittance that removal of the chip is not easy, and not without complications.

Let us for a moment revisit the decade old case of the Norplant System, the *levonorgestrel* contraceptive inserts that over 1 million women in the United States, and over 3.6 million women worldwide had been implanted with through 1996 (AMA 1997). The implants were inserted just under the skin of the upper arm in a surgical procedure under local anesthesia and could be removed in a similar fashion. As of 1997, there were 2,700 Norplant suits pending in the state and federal courts across the United States alone. Most of the claims had to do with "pain or damage associated with insertion or removal of the implants… [p]laintiffs have contended that they were not adequately warned, however, concerning the degree or severity of these events" (AMA 1997). While the Norplant system did not use RFID there are many lessons to be gained. Concerns for the potential for widespread health implications caused by humancentric implants have also been around for some time, it should not surprise us. In 2003, Covacio provided evidence why implants may impact humans adversely, categorizing these into thermal (i.e. whole/partial rise in body heating), stimulation (i.e. excitation of nerves and muscles) and other effects most of which are currently unknown.

The future is here now, and it is *wireless*. What is not completely here yet are the formal service level agreements to hand-off transactions between different types of networks owned by a multitude of network providers (few of whom are truly global)- free or commercial. These architectures and protocols are being developed, and it is only a matter of time before existing technologies have the capability to track individuals between indoor and outdoor locations seamlessly, or a new technology is created to do what present-day networks cannot (Identec 2007). For instance, a wristwatch device with GPS capabilities to be worn under the skin translucently is one idea that was proposed as far back as 1998. Hengartner and Steenkiste (2005) forewarn that "[l]ocation is a sensitive piece of information" and that "releasing it to random entities might pose security and privacy risks."

In short, there is *nowhere* to hide in this digital society, and *nothing* remains private (in due course, perhaps, not even our thoughts). *Nanotechnology*, the engineering of functional systems at the molecular level, is also set to change the way we perceive surveillance- microscopic bugs (some 50,000 times smaller than the width of the human hair) will be more parasitic than even the most advanced silicon-based *auto-ID* technologies. In the future we may be wearing hundreds of microscopic implants, each relating to an exomuscle or an exoskeleton, and which have the power to interact with literally millions of objects in the 'outside world'. The dangers are not whether state governments will invest in this technology, they are and they will (Ratner & Ratner 2004), but whether the next generation will idealistically view this technology as super 'cool' and 'convenient' and opt-in without comprehending the full extent of their compliance.

The social implications of these *über*-intrusive technologies will have no restricted limits or political borders. They will affect everything from our day-to-day existence, to our family and community relations. They will give rise to mental health problems, even more complex forms of paranoia and obsessive compulsive disorder. The refusal of some thinkers to admit to a body and mind correlation, i.e. psychophysical interaction, is progressively losing ground with many now agreeing, especially with the support of modern neuroscience, that "the intimate relation between bodily and psychic functions is basic to our personal identity" (Rodotà and Capurro 2005, p. 3). Even those engaged in religious observances will be affected, especially in the context of their practice of confession and their specific understanding of absolution of 'sin'- we might 'confess' as much as we might want, but the records on the database, 'the slate', will not be wiped 'clean'. The list of social implications is endless; it is an exercise for our imaginations. Whatever our respective *–ism* or not, condition of our mental health or not, this ‘peeping Tom’ which we will carry on the inside, will have manifest consequences for that which philosophers and theologians normally term *self-consciousness*.

In all of this rest the multiple paradoxical levels of überveillance. In the first instance, it will be one of the great blunders of the new political order to think that chip implants (or indeed nanodevices) will provide the last inch of detail required to know where a person is, what they are doing, and what they are thinking. Authentic ambient *context* will always be lacking, and this will further aggravate the potential ‘puppeteers’ of any comprehensive surveillance system. Marcus Wigan captures this critical facet of “context” very well in his paper where he speaks of “asymmetric information” held by third parties. Second, chip implants will not necessarily make you smarter or more aware (unless you can *afford* it, of course), but on the contrary and under the ‘right’ circumstances make us increasingly dumb and mute. Third, chip implants are not the panacea they are made out to be- they can fail, they can be stolen, they are not tamper-proof, and they may cause harmful effects to the body- they are after all a foreign object and their primary function is to relate to the outside world not the body itself (as in the case of pacemakers and cochlear implants). Fourth, chip implants in our present framework in any case, do not give you greater control over your space, but allow for others to control you and to decrease your autonomy and as a result your interpersonal trust at both societal and state levels. *Trust* is inexorably linked to both *metaphysical* and *moral* freedom. Therefore the naive position routinely heard in the public domain that if you have “nothing to hide, why worry?” misses the point entirely. Fifth, chip implants will create a presently unimaginable digital divide- we are not referring to computer access here, or Internet access, but access to another mode of existence. The “haves” (implantees) and the “have-nots” (non-implantees) will not be on speaking terms; perhaps a fresh interpretive approach to the biblical account of the tower of Babel (Gen. 11:9).

At this point of adoption, unless the implant is removed within a short time, the body will adopt the foreign object and tie it to tissue. At this moment, there will be no exit strategy, no contingency plan, it will be a life enslaved to upgrades, virus protection mechanisms, and inescapable intrusion. Imagine a working situation where your computer- the one which has all your personal data stored on it- has been hit by a worm, and becomes increasingly inoperable and subject to overflow errors and connectivity problems, being the only machine you could use; now imagine the same thing happening with an embedded implant. There would be *little* choice other than to upgrade or, the unthinkable, to opt out of the networked world altogether.

The first discernible movement towards this escalating and forward-looking scenario, with the potential to entangle us all "both small and great", will be our unique and 'non-refundable' identification number (ID). The universal drive to provide us all with cradle-to-grave ULIs (unique lifetime identifiers) which will replace our names is gaining increasing momentum, especially post *September 11*. Philosophers have generally held that our names are the most identifiable expressions of our personhood. Names, they have argued, are the signification of identity and origin; our names possess both sense and reference (Honderich 1995a, 602f). Two of the twentieth century's greatest political consciousness (one who survived the Stalinist purges and the other the holocaust) Aleksandr Solzhenitsyn and Primo Levi, have warned us of the connection between murderous regimes and the numbering of individuals. There is no quicker way to dehumanize an individual than by 'removing' someone's name and replacing it with a number. It is far easier to extinguish an individual on every level if you are 'rubbing' out a number rather than a life history.

Aleksandr Solzhenitsyn recounts in one place from his famous anti-Stalinist testament, *The Gulag Archipelago* (1918-56), (2007, p. 346f):

> Then again, they [Corrective Labor Camps] quite blatantly borrowed from the Nazis a practice which had proved valuable to them – the substitution of a number for the prisoner's name, his "I", his human individuality, so that the difference between one man and another was a digit more or less in an otherwise identical row of figures… [i]f you remember all this, it may not surprise you to hear that making him wear numbers was the

> most hurtful and effective way of damaging a prisoner's self-respect.

Primo Levi writes similarly in his own well-known account of the human condition in *The Drowned and the Saved* (1989, p. 94f):

> Altogether different is what must be said about the tattoo [the number], an altogether autochthonous Auschwitzian invention… [t]he operation was not very painful and lasted no more than a minute, but it was traumatic. Its symbolic meaning was clear to everyone: this is an indelible mark, you will never leave here; this is the mark with which slaves are branded and cattle sent to the slaughter, and this is what you have become. You no longer have a name; this is your new name.

And many centuries before both Solzhenitsyn and Levi were to become acknowledged as two of the greatest political consciences of our times, an exile on the isle of Patmos- during the reign of the Emperor Domitian- expressed a disturbingly comparable position when referring to the abuses of the *emperor cult* which was especially practiced in Asia Minor away from the more sophisticated population of Rome (M.G. Michael 1998, pp. 176-196). He was Saint John the Evangelist, commonly recognized as the author of the *Revelation* (c. A.D. 95):

> He causes all, both small and great, rich and poor, free and slave, to receive a mark on their hand or on their foreheads, and that no one may buy or sell except one who has the mark or the name of the beast, or the number of his name. Here is wisdom. Let him who has understanding calculate the number of the beast, for it is the number of a man: His number is 666 (Rev 13:16-18).

The technological infrastructures: the software, the middleware, and the hardware for ULIs, are readily available to support a diverse range of humancentric applications, and increasingly those embedded technologies which will eventually support überveillance. Multi-national corporations, particularly those involved in telecommunications and banking, are investing millions (expecting literally billions in return) in such 'identifiable' technologies that have a tracking capability. At the same time the media which in most instances can yield more sway with people than government institutions themselves, squanders this influence and is not intelligently challenging this auto-ID (automatic identification) trajectory. As if in chorus, block-buster productions from Hollywood are playing up all forms of *biometrics* as not only hip and smart, but also as *unavoidable* mini-*device* fashion accessories for the upwardly mobile, and attractive. Advertising, of course, plays a dominant role in this cultural *tech-rap.* Advertisers are well aware that the market is literally limitless and demographically accessible at all levels (and more tantalizingly from cradle-to-grave consumers). Our culture, which in previous generations was for the better part the van guard against most things detrimental to our collective well-being, is dangerously close to bankrupt (it already is *idol worshipping*) and has progressively become fecund territory for whatever idiocy might take our fancy. Carl Bernstein (1992) of Bernstein and Woodward fame has captured the atmosphere of recent times very well:

> We are in the process of creating what deserves to be called the idiot culture. Not an idiot sub-culture, which every society has bubbling beneath the surface and which can provide harmless fun; but the culture itself. For the first time the weird and the stupid and the coarse are becoming our cultural norm, even our cultural ideal.

Oddly enough, given this technological fixation with which most of the world is engaged, there is a perceptible mood of a collective disquiet that something is not as it should be. In the face of that, this self-deception of ‘wellness’ is not only taking a stronger hold on us, but it is also being rationalized and deconstructed on many authoritative platforms and levels. We must break free of this dangerous daydream to make out the cracks that have already started to appear on the gold tinted rim of this seeming 21st century utopia. The *machine*, the new technicized “gulag archipelago” is ever pitiless and without conscience. It can tear sinew; crush bones; break spirits; and rip out hearts without ever needing to take a break.

Lest there be any misunderstanding the authors of this note are not anti-government, after all, the alternative is anarchy-; nor are they conspiracy theorists (though we now know better than to rule out *all* conspiracy theories). Nor do they believe that these dark scenarios need necessarily eventuate as precisely as they are describing them. But they do believe that we are close to reaching the critical point of no return. Others believe that point is much closer (ACLU, 2007). It remains for individuals to speak up and argue for, and to demand regulation, as has happened in several states in the United States where Acts have been established to avoid *microchipping* without an individual's consent, i.e. compulsory electronic tagging of citizens. Our politicians (there are some exceptions) for a number of reasons will not legislate on this issue of their own accord, it would involve multifaceted industry and absorb too much of their time, and the fear they might be labelled anti-technology or worse still, failing to do all that they can in the fight against "terror". This is one of the components of the modern-day Realpolitik which in its push for the *transparent society* is bulldozing ahead without any true sensibility for the richness, fullness, and sensitivity of the undergrowth. As an actively engaged community, as a body of concerned researchers with an ecumenical conscience and voice, we can make a difference by postponing or even downgrading the doomsday scenario of even the most pessimistic futurist.

Finally, the editors would like to underscore two main points. First, the positions, projections, and beliefs expressed in this summary do not necessarily reflect the positions, projections, and beliefs of the individual contributors to this volume. And second, as with our previous workshop, it is clear that the authors of the papers do embrace all that which is vital and dynamic with technology, but reject its rampant application and diffusion without studied consideration as to the potential effects and consequences.

References

ACLU (2007). "Surveillance Society Clock 23:54", *American Civil Liberties Union*, <http://www.aclu.org/privacy/spying/surveillancesocietyclock.html> (Accessed 5 October 2007).

AMA (1997). "Norplant System Contraceptive Inserts", *Report 9 of the Council on Scientific Affairs (I-97)*, *American Medical Association*, <http://www.ama-assn.org/ama/pub/category/print/13593.html>

Accessed 5 October 2007.

AVMA (13 September 2007). “Breaking News: Statement on Microchipping”, *American Vetinerary Medical Association*, <http://www.avma.org/aa/microchip/breaking_news_070913_pf.asp> Accessed 5 October 2007.

Bacheldor, B. (17 July 2007). “AMA Issues Ethics Code for RFID Chip Implants”, *RFID Journal*, <http://www.rfidjournal.com/article/articleprint/3487/-1/1/> Accessed 4 October 2007.

Ball, E. and Bond, K. (2005). “Bess Marion v. Eddie Cafka and ECC Enterprises, Inc., No. 2005-CV-0237”, *IT Moot Court*, <http://www.itmootcourt.com/2005%20Briefs/Petitioner/Team18.pdf> Accessed 2 October 2007.

BBC. (28 July 2005). “Implant Chip to Identify the Dead”, *BBC News*, <http://news.bbc.co.uk/1/hi/technology/4721175.stm> Accessed 10 January 2006.

Bernstein, C. (1992). *The Guardian*, June 3.

Burton, P. and Stockhausen, K. (22 February 2005). *The Australian Medical Association’s Submission to the Legal and Constitutional’s Inquiry into the Privacy Act 1988* <http://www.ama.com.au/web.nsf/doc/WEEN-69X6DV/$file/Privacy_Submission_to_Senate_Committee.doc> Accessed 5 October 2007.

Californian Office of Privacy Protection. (23 July 2007). “California Privacy Legislation”, *Office of Privacy Protection, State of California*, <http://www.privacy.ca.gov/califlegis.htm> Accessed 10 October 2007.

Channel (3 January 2005). “Thai Wave Disaster Largest Forensic Challenge In Years: Expert”, *Channel News Asia*, <http://www.channelnewsasia.com/stories/afp_asiapacific/view/125459/1/.html> Accessed 10 February 2005.

Chase, C. (n.d.). VIP Verichip, *Baja Beach House- Zona VIP*, <http://www.baja-beachclub.com/bajaes/asp/zonavip2.aspx> Accessed 12 October 2007.

Clarke, R.A. (1988). “Information Technology and Dataveillance”, *Communications of the ACM*, 31(5), pp. 498-512.

Covacio, S. (2003). “Technological Problems Associated with the

Subcutaneous Microchips for Human Identification (SMHId), *InSITE-"Where Parallels Intersect*, June, pp. 843-853.

Diabetes News. (20 March 2007). "13 Diabetics Implanted With VeriMed RFID Microchip At Boston Diabetes EXPO", *Medical News Today*, <http://www.medicalnewstoday.com/articles/65560.php> Accessed 9 October 2007.

FDA (10 December 2004). "Medical Devices; General Hospital and Personal Use Devices; Classification of Implantable Radiofrequency Transponder System for Patient Identification and Health Information", *U.S. Food and Drug Administration- Department of Health and Human Services,* 69(237), <http://www.fda.gov/ohrms/dockets/98fr/04-27077.htm> 5 October 2007.

Gad, A. (June 2006). "Legislative Brief 06-13: Human Microchip Implantation", *Legislative Briefs from the Legislative Reference Bureau*, <http://www.legis.state.wi.us/lrb/pubs/Lb/06Lb13.pdf> 5 October 2007.

Guild, E. and Bigo, D. (2002). "The Schengen Border System and Enlargement" in Malcolm Anderson and Joanna Apap (eds), *Police and Justice Co-operation and the New European Borders*, European Monographs, pp. 121-138.

Hawthorne, M. (13 December 2001). "Refugees Meeting Hears Proposal To Register Every Human In The World", *Sydney Morning Herald*, <http://www.smh.com.au/breaking/2001/12/14/FFX058CU6VC.html> Accessed 1 July 2003.

HDM. (May 2005a). "VeriChip Enhances Patient Wander App", *Health Data Management*, <http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=12361> Accessed 5 October 2007.

HDM (July 2005b). "VeriChip Buys Monitoring Tech Vendor", *Health Data Management*, <http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=12458> Accessed 5 October 2007.

HDM. (October 2005c). "Chips Keep Tabs on Babies, Moms", *Health Data Management*, <http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?

articleId=15439> Accessed 5 October 2007.

HDM. (July 2007). “Baylor Uses RFID to Track Newborns”, *Health Data Management*, <http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=15439> Accessed 5 October 2007.

Hengartner, U. and Steenkiste, P. (2005). “Access Control to People Location Information”, *ACM Transactions on Information and System Security*, 8(4), pp. 424-456.

Honderich, T. (ed.) (1995a). “Names” in *Oxford Companion to Philosophy*, Oxford University Press, Oxford, p. 602f.

Honderich, T. (ed.) (1995b). “Nietzsche, Friedrich” in *Oxford Companion to Philosophy*, Oxford University Press, Oxford, p. 619-623.

Identech (2007). “RFID Tags Equipped with GPS”, *Navigadget,* <http://www.navigadget.com/index.php/2007/06/27/rfid-tags-equipped-with-gps/> Accessed 10 October 2007.

IEEE (March 2007), “Me & My RFIDs”, *IEEE Spectrum*, 4(3) 2007, pp. 14-25.

Jones, K.C. (4 September 2007). “California Passes Bill To Ban Forced RFID Tagging”, *InformationWeek*, <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=201803861> Accessed 10 October 2007.

Lewan, T. (2007a) “Microchips Implanted in Humans: High-Tech Helpers, or Big Brother’s Surveillance Tools?” *The Associated Press*, <http://abcnews.go.com/print?id=3401306> Accessed 5 October 2007.

Lewan, T. (9 September 2007b). “Chip Implants Linked to Animal Tumors”, Associated Press/ WashingtonPost.com, <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/09/AR2007090900467.html> Accessed 4 October 2007.

Meikle, J. (21 August 2007). “Pupils Face Tracking Bugs in School Blazers”, *The Guardian*, <http://www.guardian.co.uk/uk_news/story/0,,2152979,00.html> Accessed 24 August 2007.

Michael, K. (2007). “Selected Works of Dr. Katina Michael”, *University of Wollongong*, <http://ro.uow.edu.au/kmichael/> Accessed 5 October 2007.

Michael, K. & Masters, A. (2006a). “Realised Applications of Positioning Technologies in Defense Intelligence” in D. Essam & H. Abbass (eds), *Applications of Information Systems to Homeland Security and Defense*, IDG Press, ch. 7, pp. 164-192.

Michael, K. & Masters, A. (2006b). “The Advancement of Positioning Technologies in Defence Intelligence” in D. Essam & H. Abbass (eds), *Applications of Information Systems to Homeland Security and Defense*, IDG Press, ch. 8, pp. 193-214.

Michael, K. & Michael, M.G. (2006). “Towards *chipification*: the multifunctional body art of the net generation”, *Cultural Attitudes Towards Technology and Communication*, (28th-1st July: Tartu, Estonia), pp. 622-641.

Michael, K. & Michael, M.G. (2007). “Homo Electricus and the Continued Speciation of Humans”, in Marian Quigley (ed.), *The Encyclopedia of Information Ethics and Security*, IGI Global, pp. 312-318.

Michael, M.G. (1998). “Ch IX: Imperial Cult” in *The Number of the Beast, 666 (Revelation 13:16-18): Background, Sources, and Interpretation* Unpublished Honors Masters by Research Thesis at Macquarie University, pp. 176-196.

Michael, M.G. (2007). “Überveillance: 24/7 x 365- People Tracking and Monitoring”, *The 29th International Conference of Data Protection and Privacy Commissioners: Privacy Horizons, Terra Incognita*, 25-28 September, Montreal, Canada, <http://www.privacyconference2007.gc.ca/Terra_Incognita_program_E.html> Accessed 30 September 2007.

Morton, S. (2004). “Barcelona Clubbers Get Chipped”, *BBC News*, <http://news.bbc.co.uk/2/hi/technology/3697940.stm> Accessed 11 October 2007.

Ratner, D & Ratner M.A. (2004). *Nanotechnology and Homeland Security: New Weapons for New Wars*, Prentice Hall, New Jersey.

Reichman, J. H. (2006). “RFID Labeling in Humans”, American Medical Association House of Delegates: Resolution: 6 (A-06), *Reference Committee on Amendments to Constitution and Bylaws* <http://www.ama-assn.org/ama1/pub/upload/mm/471/006a06.doc> Accessed 5 October 2007.

Reynolds, M. (20 July 2004). “Despite the Hype, Microchip Implants

Won’t Deliver Security”, *Gartner Research*, <http://www.gartner.com/DisplayDocument?doc_cd=121944> Accessed 12 October 2007.

RFID. (4 June 2003). “Singapore Fights SARS with RFID”, *RFID Journal*, <http://www.rfidjournal.com/article/articleprint/446/-1/1/> Accessed 10 August 2005.

RFID. (22 August 2006). “I Am Not A Number - Tracking Australian Prisoners With Wearable RFID Tech”, *RFID Gazette*, <http://www.rfidgazette.org/2006/08/i_am_not_a_numb.html> Accessed 11 October 2007.

Rodotà, S. and Capurro, R. (16 March 2005). “Ethical Aspects of ICT Implants in the Human Body”, *Opinion of the European Group on Ethics in Science and New Technologies to the European Commission N° 20 Adopted on 16/03/2005*, <http://ec.europa.eu/european_group_ethics/docs/avis20_en.pdf> Accessed 4 October 2007.

RNZI (25 July 2007). “Papua Legislative Council Deliberating Microchip Regulation for People With HIV/AIDS”, *Radio New Zealand International*, <http://www.rnzi.com/pages/news.php?op=read&id=33896> Accessed 12 October 2007.

Sade, R.M. (2007). “Radio Frequency ID Devices in Humans, Report of the Council on Ethical and Judicial Affairs：CEJA Report 5-A-07” in R.E. Quinn *Reference Committee on Amendments to Constitution and Bylaws* <http://www.ama-assn.org/ama1/pub/upload/mm/369/ceja_5a07.pdf> Accessed 5 October 2007.

Schuerenberg, B.K. (February 2005a). “Implantable RFID Chip Takes Root in CIO: Beta tester praises new mobile device, though some experts see obstacles to widespread adoption”, *Health Data Management*, <http://www.healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=12232> Accessed 5 October 2007.

Schuerenberg, B.K. (November 2005b). “Patients Let RFID Get Under Their Skin”, *Health Data Management*, <http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?

articleId=12601> Accessed 5 October 2007.

Somba, N.D. (24 July 2007). “Papua Considers ‘Chipping’ People with HIV/AIDS”, *The Jakarta Post*, <http://www.thejakartapost.com/yesterdaydetail.asp?fileid=20070724.G04> Accessed 12 October 2007.

Songini, M.L. (12 April 2007). “N.D. Bans Forced RFID Chipping, Governor Wants a Balance between Technology, Privacy”, *ComputerWorld*, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=15&articleId=9016385&intsrc=hm_topic> Accessed 10 October 2007.

Snow, D.M. (2005). *National Security For A New Era: Globalization And Geopolitics*, Addison-Wesley.

Swedberg, C. (16 December 2005). “RFID Watches Over School Kids in Japan”, *RFID Journal*, <http://www.rfidjournal.com/article/articleview/2050/1/1/> Accessed 11 October 2007.

Swedberg, C. (25 May 2007). “Alzheimer’s Care Center to Carry Out VeriChip Pilot”, *RFID Journal*, <http://www.rfidjournal.com/article/articleview/3340/1/1/> Accessed 8 October 2007.

The Age (22 July 2007). “Chips: High Tech Aids or Tracking Tools?” *Fairfax Digital: The Age*, <http://www.theage.com.au/news/Technology/Microchip-Implants-Raise-Privacy-Concern/2007/07/22/1184560127138.html> Accessed 4 October 2007.

Verichip. (11 October 2007). “VeriChip Corporation Adds More Than 200 Hospitals at the American College of Emergency Physicians (ACEP) Conference”, *VeriChip News Release* <http://www.verichipcorp.com/news/1192106879> Accessed 11 October 2007.

Weissert, W. (14 July 2004). “Microchips implanted in Mexican officials”, *Associated Press*, <http://www.msnbc.msn.com/id/5439055/> Accessed 11 October 2007.

Wilson, J. (2002). “Girl to Get Tracker Implant to Ease Parents’ Fears”, *The Guardian*,

<http://www.guardian.co.uk/Print/0,3858,4493297,00.html> Accessed 15 October 2002.

Wisconsin Act (30 May 2006). "Wisconsin Act 482", <http://www.legis.state.wi.us/2005/data/acts/05Act482.pdf> Accessed 4 October 2007.

Woolfolk, J. (12 October 2007). "Back Off, Boss: Forcible RFID Implants Outlawed in California", *Mercury News*, <http://www.mercurynews.com/portlet/article/html/fragments/print_article.jsp?articleId=7162880&siteId=568> Accessed 13 October 2007.