2010

Toward a state of Überveillance

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

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

Publication Details
Michael, M. G. & Michael, K. (2010). Toward a state of Uberveillance. IEEE Technology and Society Magazine, 29 (2), 9-16.

Toward a state of Überveillance

Abstract
Überveillance is an emerging concept, and neither its application nor its power have yet fully arrived [38]. For some time, Roger Clarke's [12, p. 498] 1988 dataveillance concept has been prevalent: the "systematic use of personal data systems in the investigation or monitoring of the actions of one or more persons."

Keywords
toward, state, uberveillance

Disciplines
Physical Sciences and Mathematics

Publication Details
Michael, M. G. & Michael, K. (2010). Toward a state of Uberveillance. IEEE Technology and Society Magazine, 29 (2), 9-16.

M.G. MICHAEL
AND KATINA MICHAEL

Toward a State of Überveillance

Überveillance is an emerging concept, and neither its application nor its power have yet fully arrived [38]. For some time, Roger Clarke's [12, p. 498] 1988 *dataveillance* concept 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 [52], that there is a pressing need to formulate a new term to convey both the present reality, and the *Realpolitik* (policy primarily based on power) of our times. However, if it had not been for dataveillance, überveillance could not be. It must be emphasized that dataveillance will always exist – it will provide the scorecard for the engine being used to fulfill überveillance.

Dataveillance to Überveillance

Überveillance takes that which was static or discrete in the dataveillance world, and makes it constant and embedded. Consider überveillance not only automatic and having to do with identification, but also about real-time location tracking and condition monitoring. That is, überveillance connotes the ability to automatically locate and identify – in essence the ability to perform automatic location identification (ALI). Überveillance has to do with the fundamental who (ID), where (location), and 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 a person's expected behavior, traits, likes, or dislikes; or it can be based on historical fact; or it can be something in between. The inherent problem with überveillance is that facts do not always add up to *truth* (i.e., as in the case of an exclusive disjunction $T + T = F$), and predictions based on überveillance are not always correct.

Überveillance is more than closed circuit television 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

Digital Object Identifier 10.1109/MTS.2010.937024

M.G. Michael is an Honorary Senior Fellow and Katina Michael is an Associate Professor at the School of Information Systems and Technology, Faculty of Informatics, University of Wollongong, Wollongong, Australia; mgm@uow.edu.au; katina@uow.edu.au.

 1932-4529/10/$26.00©2010IEEE

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, such as microchip implants; it is that which cuts into the flesh – a *charagma* (mark) [61]. Think of it as Big Brother on the inside looking out. This charagma is virtually meaningless without the hybrid network architecture that supports its functionality: making the person a walking online node – i.e., beyond luggable netbooks, smart phones, and contactless cards. We are referring here to the lowest common denominator, the smallest unit of tracking – presently a tiny chip inside the body of a human being, which could one day work similarly to the black box.

Implants cannot be left behind, cannot be lost, and supposedly cannot be tampered with; they are always on, can link to objects, and 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 [54]. Humancentric implants are giving rise to the *Electrophorus* [36, p. 313], the bearer of electric technology; an individual entity very different from 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, unobtrusively [62]. 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" [25].

Legal and Ethical Issues

In 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 [45]. The thirty-four page document outlines legal and ethical issues having to do with ICT implants, and is based on 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 [45, pp. 20–21]:

a) the existence of a recognised serious but uncertain risk, currently applying to the simplest types of ICT implants 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, partly to prevent them from being invoked as a means to legitimize other types of application;
c) the *data minimization 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.

ICT implants for non-medical purposes violate fundamental legal principles. ICT implants also have numerous ethical issues, including the requirement for: non-instrumentalization, privacy, non-discrimination, informed consent, equity, and the precautionary principle (see also [8], [27], [29]). 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 [45, 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 favor 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 certainly useful, we have growing concerns about 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 occurred commensurate to developments in this domain.

Herein rests the problem of human rights and striking a "balance" between freedom, security, and justice. First, we contend that it is a 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 that 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."

Consider the very real case where the "Papua Legislative Council was deliberating a regulation that would see microchips implanted in people living with HIV/AIDS so authorities could monitor their actions" [50]. Similar discussions on "registration" were held regarding asylum seekers and illegal immigrants in the European Union [18]. RFID implants or the "tagging" of populations in Asia (e.g., Singapore) were also considered "the next step" in the containment and eradication of the Severe Acute Respiratory Syndrome (SARS) in 2003 [43]. Apart from disease outbreaks, RFID has also been discussed as a response and recovery device for emergency services personnel dispatched to terrorist disasters [6], and for the identification of victims of natural disasters, such as in the case of the Boxing Day Tsunami [10]. 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 of the Schengen Information System II in the European Union where differing states have recorded alerts on individuals based on their understanding of a security risk [17].

In June of 2006, legislative analyst Anthony Gad, reported in brief 06-13 for the *Legislative Reference Bureau* [16], that the:

> 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.

A number of states in the United States have passed similar laws [63], despite the fact that at the national level, the U.S. Food and Drug Administration [15] has allowed radio frequency identification implants for medical use in humans. The Wisconsin Act [59] 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 followed Wisconsin's example. Wisconsin Governor Hoeven signed a two sentence bill into state law on April 4, 2007. The bill was criticized 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 [51]. And indeed, there are now a number of swallowable capsule technologies for a variety of purposes that have been patented in the U.S. and worldwide. As with a number of other states, California 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" [28], [60]. According to the Californian Office of Privacy Protection [9] 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 went into effect January 1, 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 occurred, despite the calls for caution. The first human-implantable passive RFID microchip (the VeriChip™) was approved for medical use in October of 2004 by the U.S. Food and Drug Administration. Nine hundred hospitals across the United States have registered the VeriChip's VeriMed system, and now the corporation's focus has moved to

"patient enrollment" including people with diabetes, Alzheimer's, and dementia [14]. The VeriMed™ Patient Identification System is used for "rapidly and accurately identifying people who arrive in an emergency room and are unable to communicate" [56].

In February of 2006 [55], 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." Implants may soon be applied to the corrective services sector [44]. 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 location [33]. Despite continued claims by researchers that RFID is only used for identification purposes, *Health Data Management* 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" [19]. A number of these issues have moved the American Medical Association to produce an ethics code for RFID chip implants [4], [41], [47].

Outside the U.S., we find several applications for human-centric RFID. VeriChip's Scott Silverman stated in 2004 that 7000 chip implants had been given to distributors [57]. Today the number of VeriChip implantees worldwide is estimated to be at about 2000. So where did all these chips go? As far back as 2004, a nightclub in Barcelona, Spain [11] and Rotterdam, The Netherlands, known as the Baja Beach Club 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" [39]. Microchips have also been implanted in a number of Mexican officials in the law enforcement sector [57]. "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 that RFID is not a secure technology (see Gartner Research report [42]).

Despite the obvious issues related to security, there are a few unsolicited studies that forecast that VeriChip (now under the new corporate name Positive ID) will sell between 1 million and 1.4 million chips by 2020 [64, p. 21]. While these forecasts may seem over inflated to some researchers, one need only consider the very real possibility that some Americans may opt-in to adopting a Class II device that is implantable, life-supporting, or life-sustaining for more affordable and better quality health care (see section C of the Health Care bill titled: National Medical Device Registry [65, pp. 1001–1012]. There is also the real possibility that future pandemic outbreaks even more threatening than the H1N1 influenza, may require all citizens to become implanted for early detection depending on their travel patterns [66].

In the United Kingdom, *The Guardian* [58], 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 from tracking a stolen car, albeit for 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 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 [53]. In 2007, Trutex, a company in Lancashire England, was seriously considering fitting the school uniforms they manufacture with RFID [31]. What might be next? Will concerned parents force microchip implants on minors?

Recently, decade-old experimental studies on microchip implants in rats have come to light tying the device to tumors [29]. The American Veterinary Medical Association [3] was so concerned that they released the following statement:

> 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. . . . 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. [**emphasis added]**

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

The Norplant System was a *levonorgestrel* contraceptive insert that over 1 million women in the United States, and over 3.6 million women worldwide had been implanted with through 1996 [2]. 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

2700 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" [2]. Thus, concerns for the potential for widespread health implications caused by humancentric implants have also been around for some time. 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 [13].

Role of Emerging Technologies

Wireless networks are now commonplace. What is not yet common are formal service level agreements to hand-off transactions between different types of networks. 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 [26]. For instance, a wristwatch device with GPS capabilities to be worn under the skin translucently is one idea that was proposed in 1998. Hengartner and Steenkiste [23] forewarn that "[l]ocation is a sensitive piece of information" and that "releasing it to random entities might pose security and privacy risks."

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 question is not whether state governments will invest in this technology: they are already making these investments [40]. There is a question whether the next generation will view this technology as super "cool" and convenient and opt-in without comprehending the consequences of their compliance.

The social implications of these *über*-intrusive technologies will obey few limits and no political borders. They will affect our day-to-day existence and our family and community relations. They will give rise to mental health problems, even more complex forms of paranoia and obsessive compulsive disorder. Many scholars now agree that with the support of modern neuroscience, "the intimate relation between bodily and psychic functions is basic to our personal identity" [45, p. 3]. Religious observances will be affected; for example, in the practice of confession and a particular understanding of absolution from "sin" – people might confess as much as they might want, but the records on the database, the slate, will not be wiped clean. The list of social implications is limited only by our imaginations. The peeping Tom that we carry on the inside will have manifest consequences for that which philosophers and theologians normally term self-consciousness.

Paradoxical Levels of Überveillance

In all of these factors rests 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 could further aggravate potential "puppeteers" of any comprehensive surveillance system. Marcus Wigan captures this critical facet of context when he speaks of "asymmetric information held by third parties." Second, chip implants will not necessarily make a person smarter or more aware (unless someone can *afford* chip implants that have that effect), but on the contrary and under the "right" circumstances may make us increasingly unaware 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 tamperproof, and they may cause harmful effects to the body. They are a foreign object and their primary function is to relate to the outside world not to the body itself (as in the case of pacemakers and cochlear implants). Fourth, chip implants at present do not give a person greater control over her space, but allow for others to control and to decrease the individual's autonomy and as a result decrease 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 this suggests a fresh interpretation to the biblical tower of Babel (Gen. 11:9).

In the scenario, where a universal ID is instituted, unless the implant is removed within its prescribed time, the body will adopt the foreign object and tie it to tissue. At this moment, there will be no exit strategy and no contingency plan; it will be a life sentence to upgrades, virus protection mechanisms, and

inescapable intrusion. Imagine a working situation where your computer – the one that stores all your personal data – has been hit by a worm, and becomes increasingly inoperable and subject to overflow errors and connectivity problems. Now imagine the same thing happening with an embedded implant. There would be little choice other than to upgrade or to opt out of the networked world altogether.

A decisive step towards überveillance will be a unique and "non-refundable" identification number (ID). The universal drive to provide us all with cradle-to-grave unique lifetime identifiers (ULIs), which will replace our names, is gaining increasing momentum, especially after September 11. Philosophers have have argued that names are the signification of identity and origin; our names possess both sense and reference [24, p. 602f]. Two of the twentieth century's greatest political consciences (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. It is far easier to extinguish an individual if you are rubbing out a number rather than a life history.

Aleksandr Solzhenitsyn recounts in *The Gulag Archipelago* (1918–56), (2007, p. 346f):

> [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 – referred to the abuses of the *emperor cult* which was practiced in Asia Minor away from the more sophisticated population of Rome [37, pp. 176–196]. He was Saint John the Evangelist, commonly recognized as the author of the *Book of Revelation* (c. A.D. 95):

> 16 Also it causes all, both small and great, both rich and poor, both free and slave, to be marked on the right hand or the forehead, 17 so that no one can buy or sell unless he has the mark, that is, the name of the beast or the number of its name. 18 This calls for wisdom: let him who has understanding reckon the number of the beast, for it is a human number, its number is six hundred and sixty-six (Rev 13:16–18) [RSV, 1973].

The technological infrastructures—the software, the middleware, and the hardware for ULIs—are readily available to support a diverse range of human-centric applications, and increasingly those embedded technologies which will eventually support überveillance. Multi-national corporations, particularly those involved in telecommunications, banking, and health are investing millions (expecting literally billions in return) in identifiable technologies that have a tracking capability. At the same time the media, which in some cases may yield more sway with people than government institutions themselves, squanders its influence and is not intelligently challenging the automatic identification (auto-ID) trajectory. As if in chorus, blockbuster 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 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 vanguard 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 [7] 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.

Despite the 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 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 crush bones, break spirits, and rip out hearts without pausing.

The authors of this article are not anti-government; 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 are inevitable. But we do believe that we are close to the point of no return. Others believe that point is much closer [1]. 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 for a number of reasons will not legislate on this issue of their own accord, with some few exceptions. It would involve multifaceted industry and absorb too much of their time, and there is the fear they might be labelled anti-technology or worse still, failing to do all that they can to fight against "terror." This is one of the components of the modern-day Realpolitik, which in its push for a 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 avoiding some of the doomsday scenario outlined here.

Finally, the authors would like to underscore three main points. First, nowhere is it suggested in this paper that medical prosthetic or therapeutic devices are not welcome technological innovations. Second, the positions, projections, and beliefs expressed in this summary do not necessarily reflect the positions, projections, and beliefs of the individual contributors to this special section. And third 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

[1] ACLU, "Surveillance Society Clock 23:54," *American Civil Liberties Union*, 2007; http://www.aclu.org/privacy/spying/surveillancesocietyclock.html, accessed Oct. 5, 2007.

[2] AMA, "Norplant system contraceptive inserts," *Report 9 of the Council on Scientific Affairs (I-97)*, American Medical Association, 1997; http://www.ama-assn.org/ama/pub/category/print/13593.html, accessed Oct. 5, 2007.

[3] AVMA, "Breaking news: Statement on microchipping," *American Veterinary Medical Association*, Sept. 13, 2007; http://www.avma.org/aa/microchip/breaking_news_070913_pf.asp, accessed Oct. 5, 2007.

[4] B. Bacheldor, "AMA issues Ethics Code for RFID chip implants," *RFID J.*, July 17, 2007; http://www.rfidjournal.com/article/articleprint/3487/-1/1/, accessed Oct. 4, 2007.

[5] E. Ball and K. Bond, "Bess Marion v. Eddie Cafka and ECC Enterprises, Inc.," no. 2005-CV-0237, *IT Moot Court*, 2005; http://www.itmootcourt.com/2005%20Briefs/Petitioner/Team18.pdf, accessed Oct. 2, 2007.

[6] BBC. "Implant chip to identify the dead," *BBC News*, July 28, 2005; http://news.bbc.co.uk/1/hi/technology/4721175.stm, accessed Jan. 10, 2006.

[7] C. Bernstein, *The Guardian*, June 3, 1992.

[8] P. Burton and K. Stockhausen, *The Australian Medical Association's Submission to the Legal and Constitutional's Inquiry into the Privacy Act 1988,* Feb. 22, 2005; http://www.ama.com.au/web.nsf/doc/WEEN-69X6DV/$file/Privacy_Submission_to_Senate_Committee.doc, accessed Oct. 5, 2007.

[9] Californian Office of Privacy Protection "California privacy legislation," Office of Privacy Protection, State of California, July 23, 2007; http://www.privacy.ca.gov/califlegis.htm, accessed Oct. 10, 2007.

[10] Channel, "Thai wave disaster largest forensic challenge in years: Expert," *Channel News Asia*, Jan. 3, 2005; http://www.channelnewsasia.com/stories/afp_asiapacific/view/125459/1/.html, accessed Feb. 10, 2005.

[11] C. Chase, "VIP Verichip," *Baja Beach House- Zona VIP;* http://www.baja-beachclub.com/bajaes/asp/zonavip2.aspx, accessed Oct. 12, 2007.

[12] R.A. Clarke, "Information technology and dataveillance," *Commun. ACM*, vol. 31, no. 5, pp. 498–512, 1988.

[13] S. Covacio, "Technological problems associated with the subcutaneous microchips for human identification (SMHId)," *InSITE-"Where Parallels Intersect*, pp. 843–853, June 2003.

[14] Diabetes News "13 diabetics implanted with VeriMed RFID microchip at Boston diabetes EXPO," *Medical News Today*, Mar. 20, 2007; http://www.medicalnewstoday.com/articles/65560.php, accessed Oct. 9, 2007.

[15] "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,* vol. 69, no. 237, Dec. 10, 2004; http://www.fda.gov/ohrms/dockets/98fr/04-27077.htm, Oct. 5, 2007.

[16] A. Gad, "Legislative Brief 06-13: Human Microchip Implantation," *Legislative Briefs from the Legislative Reference Bureau*, June 2006; http://www.legis.state.wi.us/lrb/pubs/Lb/06Lb13.pdf.

[17] E. Guild and D. Bigo, "The Schengen Border System and Enlargement," in *Police and Justice Co-operation and the New European Borders*, M. Anderson and J. Apap, Eds., *European Monographs*, pp. 121–138, 2002.

[18] M. Hawthorne, "Refugees meeting hears proposal to register every human in the world," *Sydney Morning Herald*, Dec. 13, 2001; http://www.smh.com.au/breaking/2001/12/14/FFX058CU6VC.html, accessed July 1, 2003.

[19] HDM, "VeriChip enhances patient wander app," *Health Data Management*, May 2005; http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=12361, accessed Oct. 5, 2007.

[20] HDM, "VeriChip buys monitoring tech vendor," *Health Data Management*, July 2005; http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=12458, accessed Oct. 5, 2007.

[21] HDM, "Chips keep tabs on babies, moms," *Health Data Management*, Oct. 2005; http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=15439. accessed Oct. 5, 2007.

[22] HDM, "Baylor uses RFID to track newborns," *Health Data Management*, July 2007; http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=15439, accessed Oct. 5, 2007.

[23] U. Hengartner and P. Steenkiste, "Access control to people location information," *ACM Trans. Information Syst. Security*, vol. 8, no. 4, pp. 424–456, 2005.

[24] T. Honderich, Ed., "Names," in *Oxford Companion to Philosophy.* Oxford, U.K.: Oxford Univ. Press, 1995, p. 602f.
[25] T. Honderich, Ed., "Nietzsche, Friedrich," in *Oxford Companion to Philosophy.* Oxford, U.K.: Oxford Univ. Press, 1995, pp. 619-623.
[26] Identech, "RFID tags equipped with GPS," *Navigadget,* 2007; http://www.navigadget.com/index.php/2007/06/27/rfid-tags-equipped-with-gps/, accessed Oct. 10, 2007.
[27] IEEE, "Me & my RFIDs," *IEEE Spectrum*, vol. 4, no. 3, pp. 14–25, Mar. 2007.
[28] K.C. Jones, "California passes bill to ban forced RFID tagging," *InformationWeek*, Sept. 4, 2007; http://www.informationweek.com/shared/printableArticle.jhtml?articleID=201803861, accessed Oct. 10, 2007.
[29] T. Lewan, "Microchips implanted in humans: High-tech helpers, or Big Brother's surveillance tools?" *The Associated Press*, 2007; http://abcnews.go.com/print?id=3401306, accessed Oct. 5, 2007.
[30] T. Lewan, "Chip implants linked to animal tumors," Associated Press/ *WashingtonPost.com*, Sept. 9, 2007; http://www.washingtonpost.com/wp-dyn/content/article/2007/09/09/AR2007090900467.html, accessed Oct. 4, 2007.
[31] J. Meikle, "Pupils face tracking bugs in school blazers," *The Guardian*, Aug. 21, 2007; http://www.guardian.co.uk/uk_news/story/0, 2152979,00.
[32] K. Michael, *Selected Works of Dr. Katina Michael*. Wollongong, Australia: Univ. of Wollongong, 2007; http://ro.uow.edu.au/kmichael/, accessed Oct. 5, 2007.
[33] K. Michael and A. Masters, "Realised applications of positioning technologies in defense intelligence," in D. Essam and H. Abbass, Eds., *Applications of Information Systems to Homeland Security and Defense.* IDG Press, 2006, ch. 7, pp. 164–192.
[34] K. Michael and A. Masters, "The advancement of positioning technologies in defence intelligence" in *Applications of Information Systems to Homeland Security and Defense*, D. Essam and H. Abbass, Eds. IDG Press, 2006, ch. 8, pp. 193–214.
[35] K. Michael and M.G. Michael, "Towards *chipification*: The multifunctional body art of the net generation," in *Cultural Attitudes Towards Technology and Communication*, (Tartu, Estonia), 2006, pp. 622–641.
[36] K. Michael and M.G. Michael, "Homo electricus and the continued speciation of humans," in *The Encyclopedia of Information Ethics and Security*, Marian Quigley, Ed. IGI Global, 2007, pp. 312–318.
[37] M.G. Michael, "Ch IX: Imperial cult" in *The Number of the Beast, 666 (Revelation 13:16-18): Background, Sources, and Interpretation,* Honors Masters Thesis, Macquarie Univ., 1998, pp. 176–196. unpublished.
[38] M.G. Michael, "Überveillance: 24/7 × 365– People tracking and monitoring," in *Proc. 29th International Conference of Data Protection and Privacy Commissioners: Privacy Horizons, Terra Incognita* (Montreal, Canada), Sept. 25-28, 2007; http://www.privacyconference2007.gc.ca/Terra_Incognita_program_E.html.
[39] S. Morton, "Barcelona clubbers get chipped," *BBC News,* 2004; http://news.bbc.co.uk/2/hi/technology/3697940.stm, accessed Oct. 11, 2007.
[40] D. Ratner and M.A. Ratner, *Nanotechnology and Homeland Security: New Weapons for New Wars.* New Jersey, U.S.A.: Prentice Hall, 2004.
[41] J.H. Reichman, "RFID labeling in humans," American Medical Association House of Delegates: Resolution: 6 (A-06), *Reference Committee on Amendments to Constitution and Bylaws,* 2006; http://www.ama-assn.org/ama1/pub/upload/mm/471/006a06.doc.
[42] M. Reynolds, "Despite the hype, microchip implants won't deliver security," *Gartner Research*, July 20, 2004; http://www.gartner.com/DisplayDocument?doc_cd=121944; accessed Oct. 12, 2007.
[43] RFID, "Singapore fights SARS with RFID," *RFID J.*, June 4, 2003; http://www.rfidjournal.com/article/articleprint/446/-1/1/, accessed Aug. 10, 2005.
[44] RFID, "I am not a number - Tracking Australian prisoners with wearable RFID tech," *RFID Gazette*, Aug. 22, 2006; http://www.rfidgazette.org/2006/08/i_am_not_a_numb.html; accessed Oct. 11, 2007.
[45] S. Rodotà and R. Capurro, "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 Oct. 4, 2007.
[46] RNZI, July 25, 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 Oct. 12, 2007.
[47] R.M. Sade, "Radio frequency ID devices in humans, Report of the Council on Ethical and Judicial Affairs: CEJA Report 5-A-07," in *Reference Committee on Amendments to Constitution and Bylaws,* R.E. Quinn, Ed., 2007; http://www.ama-assn.org/ama1/pub/upload/mm/369/ceja_5a07.pdf, accessed Oct. 5, 2007.
[48] B.K. Schuerenberg, "Implantable RFID chip takes root in CIO: Beta tester praises new mobile device, though some experts see obstacles to widespread adoption," *Health Data Management*, Feb. 2005; http://www.healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=12232, accessed Oct. 5, 2007.
[49] B.K. Schuerenberg, "Patients let RFID get under their skin," *Health Data Management*, Nov. 2005; http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=12601, accessed Oct. 5, 2007.
[50] N.D. Somba, "Papua considers 'chipping' people with HIV/AIDS," *The Jakarta Post*, July 24, 2007; http://www.thejakartapost.com/yesterdaydetail.asp?fileid=20070724.G04, accessed Oct. 12, 2007.
[51] M.L. Songini, "N.D. bans forced RFID chipping, Governor wants a balance between technology, privacy," *ComputerWorld*, Apr. 12, 2007; http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=15&articleId=9016385&intsrc=hm_topic, accessed Oct. 10, 2007.
[52] D.M. Snow, *National Security For A New Era: Globalization And Geopolitics.* Addison-Wesley. 2005.
[53] C. Swedberg, "RFID watches over school kids in Japan," *RFID J.*, Dec. 16, 2005; http://www.rfidjournal.com/article/articleview/2050/1/1/, accessed Oct. 11, 2007.
[54] C. Swedberg, "Alzheimer's care center to carry out VeriChip pilot," *RFID J.*, May 25, 2007; http://www.rfidjournal.com/article/articleview/3340/1/1/, accessed Oct. 8, 2007.
[55] "Chips: High tech aids or tracking tools?" *Fairfax Digital: The Age*, July 22, 2007; http://www.theage.com.au/news/Technology/Microchip-Implants-Raise-Privacy-Concern/2007/07/22/1184560127138.html, accessed Oct. 4, 2007.
[56] Verichip, "VeriChip Corporation adds more than 200 hospitals at the American College of Emergency Physicians (ACEP) Conference," *VeriChip News Release,* Oct. 11, 2007; http://www.verichipcorp.com/news/1192106879.
[57] W. Weissert, "Microchips implanted in Mexican officials," *Associated Press*, July 14, 2004; http://www.msnbc.msn.com/id/5439055/, accessed Oct. 11, 2007.
[58] J. Wilson, "Girl to get tracker implant to ease parents' fears," *The Guardian*, 2002, http://www.guardian.co.uk/Print/0,3858,4493297,00.html, accessed Oct. 15, 2002.
[59] "Wisconsin Act 482," May 30, 2006; http://www.legis.state.wi.us/2005/data/acts/05Act482.pdf.
[60] J. Woolfolk, "Back off, Boss: Forcible RFID implants outlawed in California," *Mercury News*, Oct. 12, 2007; http://www.mercurynews.com/portlet/article/html/fragments/print_article.jsp?articleId=7162880.
[61] S. Butler, Ed., *Macquarie Dictionary*, 5th ed. Sydney University, 2009, p. 1094.
[62] K. Michael and M.G. Michael, *Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants.* Hershey, PA: IGI Global, 2009, p. 401.
[63] A. Griggieri, K. Michael, and M.G. Michael, "The legal ramifications of microchipping people in the United States of America- A state legislative comparison," in *Proc. 2009 IEEE Int. Symp. Technology and Society*, 2009, pp 1–8.
[64] A. Marburger, J. Coon, K. Fleck, Treva Kremer, VeriChip™: Implantable RFID for The Health Industry," June 7, 2005; http://www.thecivilrightonline.com/docs/Verichip_Implantable%20RFID.pdf.
[65] 111TH CONGRESS, 1ST SESSION H. R. ll A BILL: To provide affordable, quality health care for all Americans and reduce the growth in health care spending, and for other purposes; http://waysandmeans.house.gov/media/pdf/111/AAHCA09001xml.pdf, accessed Apr. 1, 2010.
[66] Positive ID. 2010. Health-ID; http://www.positiveidcorp.com/health-id.html, accessed May 1, 2010.