2009

Uberveillance: microchipping people and the assault on privacy

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. (2009). Uberveillance: microchipping people and the assault on privacy. Quadrant, 53 (3), 85-89.

Uberveillance: microchipping people and the assault on privacy

Abstract

Uberveillance is above and beyond, an exaggerated, and omnipresent 24/7 electronic surveillance. It is a surveillance that is not only always on but always with you. It is ever-present because the technology that facilitates it, in its ultimate implementation, is embedded within the human body. The inherent problem with this kind of bodily pervasive surveillance is that omnipresence will not always equate with omniscience. Infallibility and ambient context will be for the greater part absent. For as Marcus Wigan has pithily put it, "context is all." Hence the real concern for misinformation, misinterpretation, and information manipulation of citizens' data.

Keywords

uberveillance

Disciplines

Computer Sciences | Physical Sciences and Mathematics

Publication Details

Michael, M. G. & Michael, K. (2009). Uberveillance: microchipping people and the assault on privacy. Quadrant, 53 (3), 85-89.

UBERVEILLANCE:
Microchipping People and the Assault on Privacy

M.G. Michael and Katina Michael

Augustine of Hippo (354-430 CE) one of the most highly revered doctors of the ecclesia catholica might not have been so greatly esteemed had he flourished centuries later in a world of uberveillance. One of the unique aspects of Augustine's life which endeared him to the community of the faithful, both past and present, was his rising up from the "fornications" and the "delight in thievery" to become a paradigm for both the eastern and western churches of the penitent who becomes a saint. But would the celebrated bishop and author of the *City of God* have risen to such prominence and reverence had his early and formative life been chronicled on *Facebook* or *MySpace* and "serialized" on *YouTube*? Would Augustine's long and grueling years of penitence and good works have been recognized? That we have his stylized and erudite *Confessions* on paper is another matter altogether; as to its effect and impact the written record cannot be compared to capturing someone "in the act" on closed circuit television (CCTV). The audio-visual evidence is there "forever" to be rerun at whim by those who have access. And what of the multitude of other canonized 'sinners' who in their own time and private space might not only mature by engaging with their humanity, indeed with their flaws and weaknesses, but also aspire to sainthood through repentance. If these "lives of the saints" were rerun before us, would we view such consecrated men and women in the same way? Where *context* is lacking or missing, then *all* interpretation of content, however compelling to the contrary, must be viewed with a high degree of suspicion.

Even in the political and civil rights arena, for example, had the private lives of colossal and 'untouchable' figures such as John F. Kennedy and Martin Luther King been subjected to *24/7* uberveillance, how might that not only have affected the biography of these two men, but changed the very course of history itself? Moreover, how would the knowledge of such *bio*-intrusive surveillance altered both Kennedy's and King's decision-making processes and life habits? We know for instance, particularly from the seminal study of M.F. Keen, that the surveillance of prominent sociologists in the United States played a major role in shaping the American sociological tradition. Certainly, J. Edgar Hoover's *FBI* might have kept a detailed account of the supposed meanderings and subversions of its "suspects", but these records whether *true* or *false* were not universally accessible- they were limited given the state of information and communication technology at the time. And what of the private lives of popes and patriarchs, kings and queens, great philanthropists, and other exalted figures, how might they have stood up to the nowadays literal 'fly on the wall' shadowing?

More recently engineers at Berkeley have been involved in the creation of "insect cyborgs" which amongst other applications can be rigged up with 'bugging' devices for miniature surveillance and sensors for reconnaissance. But we need not even go that far. Today the global positioning system (GPS), consisting of a constellation of 31 orbiting satellites, can pinpoint a person's location anywhere on the globe down to 15 metres on average. Small data loggers (called tracksticks), the size of a clothespin, have the capability of continuously recording their own location histories for extended periods of time. These miniature location devices can be placed discretely into the inner lining of a handbag, attached magnetically to an inconspicuous position on a vehicle, or even unobtrusively placed on an outer garment.

Steve Mann created *glogger.mobi* to guard against the tampering of both overt and covert surveillance output. There are now over 35,000 people who have become *gloggers* and who record cyborglogs (abbreviated 'glog). Armed with a simple camera phone or web cam a glogger takes a first person recording of an event in which they are a participant and then uploads it to a web server where they can broadcast content to the rest of the community or to any of their social networking sites, blogs or personal pages. The glog is the gloggers' unique record of events, the world through their own exclusive lense, which can be used to provide counter-evidence to multi-media content that has been deliberately fabricated. This inverse surveillance, however, a component of what Mann has called sousveillance, is not without its own inherent risks.

Nevertheless, the incongruity behind all of these surveillance technologies (including wholesale surveillance and dataveillance) is that individuals of power and influence will as a rule not be subjected to the extreme and exaggerated types of projected surveillance techniques designed and planned for the common people. Except, of course, for those occasions of blackmail and industrial espionage, for example, when the powerful and influential will make use of whatever apparatus is at their disposal to spy upon and to turn against their own. Needless to say, of course, this is not a blanket assertion that all influential and powerful persons must necessarily be 'corrupt'. It is fundamentally a matter of control which revolves around *authority*, *access*, and *opportunity*. We return then, to the perennial question of who will guard the guards themselves: *Quis cutodiet ipsos custodes?*

Even those uniquely enlightened persons such as Siddhartha Gautama and Jesus of Nazareth needed private space to not only inwardly engage and to reflect on their respective missions, but also to do discrete battle with their respective "temptations." Uberveillance makes *private space* inch-by-inch obsolete. Private space is that location which we all need- "saint" and "sinner" alike- to make our mistakes in secret, to mature into wisdom, and to discover what we are and are not capable of. In losing large chunks of our privacy we are also forfeiting a critical component of our personal identity which for a substantial group of philosophers is "the identity of consciousness". There is then, the potential for personality disorders to develop, particularly anxiety or phobic neurosis.

Lest there be any misinterpretation of what is being said here, we are of course *not* speaking of concealing or protecting our private space in order to scheme or to commit indictable offences or crimes. Computerized monitoring in some instances may surely be warranted. But before we move on, what exactly is meant by this relatively new term *uberveillance* which the RNSA (Research Network for a Secure Australia, 2007) considered important enough to sponsor a national workshop to discuss its possible social and political implications in both the private and public sectors. It is also very significant that the keynote address delivered on that day was by Roger Clarke, himself, who had over twenty years earlier introduced us to the murky world of dataveillance.

Uberveillance is an above and beyond, an exaggerated, and omnipresent 24/7 electronic surveillance. It is a surveillance that is not only always on but always with you. It is ever-present because the technology that facilitates it, in its ultimate implementation, is embedded within the human body. The inherent problem with this kind of bodily pervasive surveillance is that omnipresence will *not* always equate with omniscience. Infallibility and ambient context will be for the greater part absent. For as Marcus Wigan has pithily put it, “context is all.” Hence the real concern for *misinformation*, *misinterpretation*, and *information manipulation* of citizens’ data.

Uberveillance is more than closed circuit television (CCTV) feeds, or cross-agency databases linked to national identity cards, or eTollways and automatic number plate recognition (ANPR), or biometrics and ePassports used for international travel. Uberveillance 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, uberveillance has to do with more than biometrics, radio-frequency identification (RFID), wearable or luggable devices. And it is certainly more than the ‘mere’ *casual capture* surveillance technology of either the *Nokia N95* or the *Apple iPhone*. Or the geo-tagging of dwellings and people using *Google StreetView* and *Google Latitude* towards the *Internet of Things*. Uberveillance, the *causa finalis* of surveillance, is Big Brother on the *inside* looking out. We are referring here, to the lowest common denominator, the smallest unit of tracking, a tiny microchip implant(s) inside the body of a human being, capturing and transmitting almost everything.

This act of *chipification*, the embedding of a ‘technique’ inside the human body, is best illustrated by the ever-increasing, and in this instance positive uses of implant devices, for both medical prosthesis and for diagnostics. Humancentric implants are giving rise to the *Electrophorus*, the bearer of electric technology. And it is surely not just coincidence, that alongside uberveillance 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”. This is especially obvious in our rampant efforts to rebuild our bodies, to be *better*, *stronger*, *faster*- “[w]e have the technology.” This is reminiscent of course, of the popular American television series *The Six Million Dollar Man* (1974-78).

The unbridled rush and push to create the *transparent society*, as David Brin very well described it, has social implications which are largely ignored, or at best marginalized. The social implications of information security measures which are connected to 24/7 surveillance or indeed to other network applications have serious and often irreversible psychological consequences of which only a few can be cited here: increased cases of mental illness (new forms of obsessive compulsive disorder and paranoia); a rise in related suicides; decreased levels of trust (at all spheres of relationships); and the impossibility of a “fresh start.” Case in point, the traditionally received idea of the unconditional absolution of sin in the secrecy of the confessional already does not exist in the world of some religious communities; believers are encouraged to log on and to "confess" online. These types of social networks are especially dangerous for individuals already battling mental illness, and who might afterwards deeply regret to having uploaded imaginary or real discretions for everyone to read on the web log.

The author of a noteworthy article published in *Newsweek* (10 September, 2007) commenting on the high profile suicides of two internationally recognized digital technologists, Theresa Duncan and Jeremy Blake, put it well when he surmised "for some, technology and mental illness have long been thought to exist in a kind of dark symbiosis." The startling suicides first of Duncan and soon after that of her partner Blake, for whom "the very technologies that had infused their work and elevated their lives became tools to reinforce destructive delusions" is a significant, albeit sad reminder that even those heavily involved in new technologies are not immune from delusional and paranoid torment, whether based on fact or not. And that's precisely the point, that with covert shadowing you can never be completely sure that your paranoia is groundless. Long term research at a clinical level remains to be conducted on the subject of never-ending surveillance and mental illness. There is some evidence to suggest that a similar paranoia played at least some part in another shocking suicide, that of the Chinese American novelist and journalist Iris Chang, well-known author of *The Rape of Nanking*.

The positions expressed in this paper should not be viewed as alarmist, but rather as an advisory forecast of where the automatic identification (auto-ID) trajectory is increasingly taking us given present evidence, both at the applied and theoretical levels. The application of technology is rarely unbiased. Once a technique is set in motion and diffused into our society it becomes progressively irreversible, particularly given the key component of interoperability and the vast amounts of capital invested in 21st century machinery. However, our comprehension of this hi-tech diffusion is not on commensurate levels. Cross-disciplinary discourse, public debate, and legislation lag far behind the establishment of the infrastructure and the application of the technology. In simple terms, this lag is the "too much change in too short a period of time" which Alvin Toffler famously referred to as *future shock*.

It is, unfortunately, reminiscent of that time in Alamogordo, New Mexico in 1945, when some of those engaged in the Manhattan Project, including one of the group's top physicists the Nobel laureate Enrico Fermi, were taking side bets on the eve of the test on whether they would "ignite the atmosphere" once the atomic bomb was tested! A major difference being that the "fall-out" from uberveillance is distributed, and it will initially at least, be invisible to all except the approved operators of the data vacuum. The setting and foreboding of notable dystopian novels which warn of the "dangerous and alienating future societies," i.e. Yevgeny Zamyatin's We (1921), Aldous Huxley's Brave New World (1932), Ayn Rand's Anthem (1938), George Orwell's 1984 (1949), Ray Bradbury's Fahrenheit 451, (1953), whose central premise that "dissent is bad" and the deified State "knows all" is being gradually realized. This is especially worrying, for as Noam Chomsky and others point out, we are concurrently witnessing a "growing democratic deficit".

Great strides are also being taken in the field of biomedical engineering, the application of engineering principles and techniques to the medical field. New technologies will heal and give hope to many who are suffering from life-debilitating and life-threatening diseases. The broken will walk again. The blind will see. The deaf will hear. The dumb will sing. Even bionic tongues are on the drawing board. Hearts and kidneys and other organs will be built anew. The fundamental point is that society at large is able to distinguish between positive uses and applications of technological advancements before we diffuse and integrate such innovations into other areas of our day-to-day existence.

Nanotechnology, which is the motivation behind many of these marvelous medical wonders, will interconnect with the surveillance field and quite literally make the notion of "privacy"- that is *revealing ourselves selectively*- an artifact. We must do whatever is in our lawful power to check, mitigate, and to legislate against the unwarranted and abusive use of *uber*-intrusive surveillance applications. We are talking about applications with such incredible capabilities which will potentially have the power to de-humanize us and reach into the secret layers of our humanity. These are not unruly exaggerations when we consider wireless sensors and motes, body area networks (BANs) and brain-computer interfaces (BCIs) are already established technologies and that the era of mind control, particularly through pioneering advancements in brain-scanning technology, is getting steadily closer.

The argument most often heard in the public domain is "if you have nothing to hide, then why worry?" There are, however, at least three inherent problems with this popular mantra. First, *freedom* implies not only being 'free of chains' in the practical sense, to be permitted to go about one's daily business freely and without undue constraint, but nowadays also without your every move being tracked, monitored, and recorded. Second, there is a metaphysical freedom connected to *trust*, which also implies to be able to dream, to think and to believe without any outside coercion. And finally, whether we care to admit it or not, we *all* have something to hide. Disruption of any of these freedoms or rights would affect our decision-making processes and contribute to an unhealthy personality development where what we "want" to do (or to engage in) becomes what we think we "must" do (and to theatrically engage in).

To artificially build a personality or to hold onto a set system of synthetically engineered beliefs is to deconstruct the human entity to the point where both initiative and creativity (two vital components of a healthy individual) are increasingly diminished, and ultimately eradicated. Humancentric implants for surveillance will alter the "inner man" as much as the externals of technological innovation will transform the "outer man". There are those, for instance, who would argue that the body is obsolete and should be fused with machines; and others who would support mind and identity downloading. In the context of such futuristic scenarios Andrew Ross has aptly spoken of the "technocolonization of the body." Others on the cutting-edge of the digital world are using technology in ways 'supposedly' never intended by the manufacturers themselves.

If there are elements to this essay which might point to the potential mushrooming of new totalitarian regimes and paradoxically so, after all we are living and reveling in a post-modern and liberal society where the individual cult on a mass scale is idolized and thriving, then we should stand back for a moment and reconsider the emerging picture. Two of the more prominent features of the murderous regimes of both Stalin and Hitler, were the obsession with state secrecy and the detailed collection of all sorts of evidence (whether 'incriminating' or not) documented in scrupulous registers. Related to this second action was the well-known and beastly numbering of minorities, prisoners, and political dissidents. In our time, privacy experts such as David Lyon are warning, that this type of "social sorting" is becoming evidenced once more. Where are we heading today? Already in the USA there are a number of states (e.g. North Dakota and Wisconsin) which have passed antichipping bills banning the forced implantation of RFID tags or transponders into people. Here in Australia it is time *now*, at both the State and Federal levels, for political parties to make clear to the electorate their position on the question of human microchipping.

A great deal of this discussion should revolve around the related ethics of emerging technologies, and as we have noted this discourse is especially critical when we consider the "unintentional" and hidden consequences of innovation. However, one of the methodological weaknesses in this global debate is the direct focus by some of the interlocutors on metaethics alone. What we must understand, if we are to make any practical progress in our negotiations, is that this subject must first be approached from the perspective of normative and applied ethics. The lines of distinction between all three of these approaches will at times remain unclear and even merge, but there are some "litmus tests" (human rights for example) for determining the morality and the ultimate price of our decisions.

Unique lifetime identifiers (ULI's) are more touted than ever before by both the private and public sectors as they have become increasingly synonymous with tax file and social security numbers. The supposed benefits of this permanent cradle-to-grave identification are energetically broadcast at various national and international forums, and especially in the contexts of white collar crime and national security. There is no quicker way to de-humanize an individual than by deleting their 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. Two of the twentieth century's greatest political consciences, one who survived the Stalinist purge and the other the Holocaust, Aleksandr Solzhenitsyn and Primo Levi, have warned of the connection between murderous regimes and the numbering of individuals.

In 1902 Georges Méliès short sci-fi film *A Trip to the Moon* (Le Voyage dans la Lune) spawned the fantastic tradition of putting celluloid form onto the predictive word. More recently representative of this tradition is Ian Fleming's *James Bond* in *Casino Royale* (2006) who becomes a 'marked' man, chipped in his left arm, just above the wrist by his government minders. "So you can keep an eye on me?" the famous spy sarcastically rejoins. The chip is not only for identification purposes but has multiple functions and applications, including the ability to act as a global positioning system (GPS) receiver for chronicling his every move. Later in the film when Bond is captured by his arch-nemesis, the banker *Le Chiffre*, he will have the microchip, which looks more like a miniature spark plug, cut out of his arm with a blade. These kinds of scenarios are no longer the exclusive domain of the sci-fi novelist, the conspiracy theorist, the religious apocalypticist, or the intellectual property of the tech-visionary.

We have the ability and potential to upgrade these information gathering mechanisms to unprecedented and sci-fi proportions: "[w]e have the technology." It seems ever more likely, that sooner rather than later, we will in fact set on a program to microchip implant every individual on this planet with a tracking and monitoring device. The justification for this act will rest on carefully articulated arguments, and they will range across the social and national security spectrums. For example, it was in July 2007 that Indonesia's government announced plans to chip implant over five thousand HIV/AIDS patients in Papua. It was only in December 2008, after human rights organizations lobbied for eighteen months against the move, that the plans were subsequently dropped.

Hybrid architectures, in particular those which involve RFID, sensors, wireless fidelity (Wi-Fi) and GPS are presently being developed, they will make this once undreamed of penetrating surveillance possible. We are living in times in which commercial innovations will possibly match the internal complexity of the neuron with the help of the appositely called *labs-on-chips*. Writers dealing with these subjects have been speaking less in terms of *future shock* and more along the lines of *hyper-future shock*. The key question, in so far as identification and information gathering technology is concerned, how are we as a concerned and informed community going to curb and regulate the broad dispersal and depth-charged reaches of surveillance. And to do this of course, *without* denying the many positive and desirable applications of the infrastructures which underlie these technologies, particularly in the domain of healing and repairing the sick and the injured.

Readers of this paper might well be asking what has technology to do with some of the metaphysical issues that we are raising here. Perhaps it would be sensible to periodically remind ourselves as has a discriminating online essayist that two of our greatest thinkers, Plato (*c*.428-347 BCE) and Aristotle (*c*.384-322 BCE), both warned of the inherent dangers of glorifying *techne* (*lit.* art, skill). It should be subject to "reason and law", and furthermore, they argued that *techne* represents "imperfect human imitation of nature". The pertinent question in this instance might be why modern societies gradually moved away from asking or seeking out these connections of metaphysics? This general apathy, with some few honorable exceptions, towards a philosophical critique of technology can probably be traced to a defensive response of western economic tradition to Karl Marx's "critique of Victorian progress".

In relation to surveillance and ubiquitous location determination technologies, we are at a critical junction; some might well argue that we have long made our decision of which road to travel down. Maybe these commentators are right. Perhaps there is no longer a place for trusty wisdom in our world. Just the same, full-scale uberveillance is not yet arrived. We must moderate the negative fall-out of science and control technology, that is, as Jacques Ellul would say "transcend" it: lest its *control* on us becomes non-negotiable and we ourselves become the frogs in the slow warming water.

Dr MG Michael is an honorary senior fellow in the School of Information Systems and Technology at the University of Wollongong. He is a member of the American Academy of Religion and the Research Network for a Secure Australia.

Dr Katina Michael is a senior lecturer in the School of Information Systems and Technology at the University of Wollongong. She is a senior member of the Institute of Electrical and Electronics Engineers (IEEE), and a board member of the Australian

Privacy Foundation.

The authors would like to acknowledge the insightful comments of Dr Stephen McInerney who had read earlier versions of the paper.