The Future Prospects of Embedded Microchips in Humans as Unique Identifiers: The Risks versus the Rewards

Authors: Katina Michael* and M.G. Michael**
* School of Information Systems and Technology, University of Wollongong
** Researcher, uberveillance.org

1 Introduction

Microchip implants for humans are not new. Placing heart pacemakers in humans for prosthesis is now considered a straightforward procedure. In more recent times we have begun to use brain pacemakers for therapeutic purposes to combat illnesses such as epilepsy, Parkinson's Disease, and severe depression. Microchips are even being placed inside prosthetic knees and hips during restorative procedures to help in the gathering of post-operative analytics that can aid rehabilitation further. While medical innovations that utilise microchips abound, over the last decade we have begun to see the potential use of microchip implants for non-medical devices in humans, namely for control, convenience and care applications. Most of these emerging applications that have been demonstrated in numerous case studies have utilised passive radio-frequency identification (RFID) tags or transponders embedded in the tricep, forearm, wrist or hand of the implantee. The RFID transponder stores a unique identifier that is triggered when the device comes into range of a reader unit.

2 The First Commercial RFID Implantable- the VeriChip

After Professor Kevin Warwick's Cyborg 1.0 experiment in Britain in 1998 (Warwick 2002), came the unrelated establishment of the VeriChip Corporation in the United States, soon after the September 11, 2001 terrorist strike. Scott Silverman, the CEO of the then VeriChip Corporation was often quoted describing the need for implants, especially for first responders, given the tragic way so many firemen lost their lives in the Twin Towers (Applied Digital Solutions 2003). He and Richard Seelig, the Vice President of Medical Applications at VeriChip, were implanted in early 2002. On the 11th of May 2002, the Jacobs family volunteered to be the first consumers to undergo the chipping procedure which was broadcast live on American television (BBC 11 May 2002). VeriChip then chose to implant some high profile people, including Mr Rafael Macedo de la Concha (Mexico's Attorney General) and a number of his staff citing security purposes. In 2004 and 2006, Baja Beach Club and Citywatcher.com respectively, were engaged in human implantable programs on their company premises. According to VeriChip about 2,000 persons had been implanted worldwide by the end of 2008.

2.1 Medical and Non-Medical Implantable Applications

When VeriChip first launched their product range, they had four cornerstone application contexts: (1) VeriPay, (2) VeriMed, (3) VeriGuard, and (4) Corrections. The VeriPay system allowed end-users the capability to perform cash and credit transactions with the embedded implant. VeriMed was a user-driven healthcare information portal whereby consumers (i.e. patients) could maintain their own personal health record (PHR) online. Hospital staff and emergency services personnel could then access that information to get patient history, as well as allergic reactions to drugs and more. The VeriGuard application was considered to be versatile secure access technology which let in authorized persons and blocked out unauthorized persons (VeriChip 9 October 2003). Finally, VeriChip's 'Corrections' product had to

do with chipping people who had committed a crime, were on parole or probation, or were awaiting trial.

3 Methodology

This paper uses a case study to showcase the issues arising from the application of RFID implants in humans. The study focuses on one of the earliest deployments of the VeriChip VeriGuard application within a business context at Citywatcher.com. The data for the case study is collected using a single interview with Mr Gary Retherford of Six Sigma Consulting who was the external consultant responsible for the deployment of the verichips at Citywatcher.com, and was himself voluntarily implanted (Associated Press 13 February 2006). The data from the interview was analysed using emergent themes and the narrative is characterised by thick descriptions from the interview. The conceptual framework for the study focused on the social implications of RFID implant technology pertaining to risk, security, privacy, control and human rights. The study was also concerned with drawing out the motivation behind the adoption for RFID implants versus consumer resistance against RFID implants.

3.1 Case Study: About Citywatcher.com

Located in Cincinnati, Ohio, Citywatcher.com was a small government contractor specialising in surveillance equipment and surveillance-related projects. On the 1st of February 2006, two of its employees had glass encapsulated microchips with miniature antennas embedded in their forearms (WND 10 February 2006). All employees of the small business were given an opportunity to get an implant for access control, and a total of four employees were implanted. The microchips acted just like RFID proxy cards, save for the fact they were beneath the skin. The embedded microchips were used by the employees to gain access to a restricted area containing vaults of sensitive data and images related to policing (e.g. Cincinnati Police Department) and private business. Citywatcher mainly stored on its premises CCTV video surveillance of public streets in Cincinnati. The CEO of the company, Mr Sean Darks, considered the implants to be more sophisticated than keycards and touted their usability and affordability when compared to biometric systems. Darks was quoted on several occasions as saying that the solution was very convenient. It should be made clear, that the company ceased operations in 2008 for reasons that were unrelated to the implanting of employees.

3.2 Interview with Mr Gary Retherford of Six Sigma Consulting

Mr Gary Retherford of Six Sigma Security (Six Sigma 2010), who previously consulted for Citywatcher.com was interviewed on the 17th of June 2009 by telephone by Katina Michael and MG Michael. In 2006, Retherford was acting as an external consultant to Citywatcher.com for the implementation of their access control system.

4. Lessons from Citywatcher.com

4.1 Seeing what the World was made of

Retherford described a feeling of excitement, anticipation and even trepidation when he announced that the first employees had been chipped. He was thinking about the future impact the announcement might have because from his research “it was going to be the first time in any place of employment, [that] employees [had been] implanted with a microchip.” He noted: “…and this is a little strange to say this – but

I wanted to see… how the human race would react and what the world was made of to deal with this concept and so when… I clicked the little send button… I remember I had kind of a pause and a thought and a deep breath. Because I knew there was no coming back once I hit the send." Furthermore, from a personal motivation, Retherford stated:

> "… there was also a part of me that felt that there was nothing wrong with this [human microchipping]… as humans we begin to do things more and more as we get used to it. So there's the initial shock, but once you get over it, whatever "it" is, we tend to absorb it, we bring it into our minds, we're able to wrap arms around it and we continue to move forward. Now sometimes it takes a little bit longer for some than for others, depending on the situation or what it is."

4.2 Taking the Risks and the Pace of Change

We asked Retherford about the importance of deploying new RFID services and applications with the user at the centre of the design effort as a risk minimisation strategy. Retherford's responses ranged from 'there are no risks at all' putting on his Six Sigma Consulting hat, to there are 'tremendous risks' putting on his Baby Boomer's hat. No doubt this was a natural attempt to reconcile the pace of change between the era he grew up in with the era he was now living in. He stated: "[i]t's unfathomable… to ever think that I was watching a television with only three channels and I did not have a cell phone and I did not have a computer… so the differences are so vast…" But finally, Retherford stated: "No, I don't think there are risks because it's a mute point to say that there are."

It was not difficult to see where Retherford was coming from and how he conceptualized the world around him. For Retherford, technological change of any type was ever-present so fighting it did not make sense. Probing further K. Michael asked Retherford to clarify whether risk was an inherent part of all change and therefore it was not that big a deal. Retherford agreed that the risk argument was no longer even an argument anymore, but rather another "mute point". He was much more amenable to the idea of, well "okay, it's going to happen so now how do we do it. Let's address the issues that we have to based on the "fact" that it's going to happen anyway."

4.3 Resistance and the Vocal Minority

Retherford especially found irritating the negativity surrounding RFID implants by some members of the global community. He called it "irrational paranoia by the vocal minority." According to Retherford, some people were making RFID implants out to be bigger than they actually were and linked to some type of conspiracy theory related to Big Brother type technology. Putting aside the claims of the passionate opposers of RFID implantable technologies, Retherford again asserted, "I think by and large, society is ready for it… I'm one of these people, that if I know something is coming, I don't try to not embrace it, I go ahead and embrace it and look for the positive sides of it and on this [RFID implants] it was pretty obvious to me that there was a positive side."

To a degree, Retherford categorises opposition to chip implants as a type of hysteria which stems from personal beliefs which take on one of several forms including: (1) civil libertarian, (2) religious literalist, (3) paranoid, and or (4) mentally imbalanced. He emphasizes that instead of people talking about risk return, or the value

proposition of chip implants, i.e. what do I get out of it for getting implanted, people are directly engaging with statements to do with *Big Brother* or the *Mark of the Beast* (from the *Book of Revelation*). Retherford points to other technologies that he perceives to be of greater significance to Big Brother than mere implants. He uses the example of cell phones and the Internet and questions why the group concerned by Big Brother are not lobbying against the widespread diffusion of such technologies as biometrics. He says circumspectly: "So now you have to consider the arguments of the people that are against it [implants] and really come down to a rational reason why people would argue either for or against either way and I don't consider paranoia or just someone of a radical viewpoint to be a rational reason to either include or not include something." This is a sentiment that is echoed by another implantee, Mr Amal Graafstra (Graafstra, Michael et al. 2010). There were also some consultants at the time who did not want to start VeriChip deployments until they had addressed all the issues but according to Retherford, these people "were left behind."

4.4 The Socio-Ethical Implications

Repeated questioning of what the socio-ethical implications that microchip implants in humans will give rise to, does nothing to alter Retherford's stance. Retherford is not interested in opinions or feelings about the implants as he sees these as irrelevant. More importantly he is focussed on where the future trajectory of technology is headed and how he will best work around those parameters. The "what ifs" posed by K. Michael were somewhat redundant lines of questioning for Retherford who is much more interested in "not should we do this, but how do we implement it." Here Retherford does allude to the importance of finding a balance between law and control but emphasizes that the question of whether or not we should use the chip is long in the past.

> "I think that discussion has already been done. I think that discussion is over with. Because the fact that it is within the sights of the technological world to achieve it, you no longer make the argument on should it or shouldn't be, now you go into the realm of: how do we discuss and maybe legislate on the trade-offs between how much control and how much not to control, because we're already there for all practical purposes. We're there now even if you don't look at it is an implantable chip. We're there…"

It is on this crucial point that Retherford seems to have contradicted himself. On the one hand he is saying that questions to do with socio-ethical implications are irrelevant, and on the other he is talking about having a discussion about the trade-offs between how much control is too much or too little and about the legislative trade-offs.

4.5 Privacy, Security and Control

Retherford is in agreement that there is no doubt that the implantable microchip is going to have an impact on society. Retherford acknowledges M.G. Michael's references to control and privacy issues but emphasizes that these issues are only relative to security. The compelling question that is needed to be asked is whether "my security supersede[s] my neighbours right to privacy?" asks Retherford. Alluding to homeland security and law enforcement personnel whom Retherford has had contact with in his day-to-day tasks, he reaffirms the philosophy of the sector as being: "It's my job to protect you regardless of what it costs you." In fact, it is quite clear the attitude which is propelling this philosophy forward says: "I will protect you no matter how much of your privacy and your liberties I destroy, it's my job to make

sure that no harm comes to you…" More recently see the work of Magnet (2011) who writes on the relationship between RFID, surveillance and bodily scrutiny.

K. Michael attempts to convey the rigidity that such an implant regime would have upon the individual, especially in the employer-employee context. New types of operational efficiencies in organisations, would mean there would be limited flexibility built into the way people worked. Some level of choice would be automatically withdrawn from the individual, even on which route to take on a given job using the company car. Retherford who does acknowledge the broader issues had to admit to this looming scenario. He reflected:

> "[w]ell I think what you're saying makes sense… I understand what your saying – in the mind, it does make you wonder, 'Okay, can I really work like this?', because you know if I want to veer off and stop off somewhere that's not typically where I would go next because I want to stop and get something to drink, a Coke or something. I mean, is this going to be in the back of my mind that I'm now outside of that control? And I do believe that that is certainly a risk which is coming at us as a society. That is, can we operate under those types of conditions?"

But again, Retherford returns to the security versus privacy question, and the driving force behind someone being implanted. Retherford recounts that there is a question he poses to others, that is always answered the same way: "Does my right to security supersede my neighbours right to privacy? … Because the question then comes is– "Do I want to be chipped? No. But I don't really know my neighbour that well, so maybe Congress should pass a law that chips my neighbour."

RFID implants may well be an alternative but they too will be open to the same abuses as present day technology systems (Reynolds 20 July 2004). And we need to consider what they will mean for humanity. If we are embedding computer systems into the human body for non-medical purposes, then we need to be ready for the internalisation of a lot of the same problems that personal and mobile computing have brought with them. Even Retherford has to concede: "I think that there will be attempts to maybe abuse it by those people who are already trying to attempt to do these things that are either external to the government or you know, say other organisations that we interact with. But I don't think it's going to be any different from what we see today."

4.6 Sizing up the Implantable Market

Retherford does not doubt that the market for RFID implantables, like so many other technologies, will be driven by commerce. He believes that adoption will happen in "small incremental ways" at first, "in efforts that are first imposed on smaller groups." Among these groups he cites Alzheimer's facilities or nursing homes, and prisons given their fundamental use of access control systems to let people come and go or to keep people in. Retherford referred to jails being excellent outlets for RFID implants and framed the argument by referring to citizenry who would be more than happy to see "less desirable" citizenry chipped to stamp down on criminal acts, or those that are repeat offenders. Despite this approach being fraught with ethical issues, it is likely that RFID implants will be rolled out to address needs in minority groups, such as those suffering from mental illness, or children who are under the guardianship of their parents, or the elderly who are being looked after in care. For Retherford, this is

exactly the manner in which the whole populace might grow accustomed to the idea of opting into implants. Of course, the other way, would be to herald in an implant during a state of emergency for management and coordination purposes (Klein 2007; Associated Press September 2005).

4.7 Being Implanted and Maintenance Issues

A great part of the story of the adoption of RFID implants has to do with the fact that technology is being implanted beneath the skin where bearers do not have any control to remove it at will (Masters and Michael 2007). The aspect of bodily privacy is especially important here. But for Retherford, the "psychology of having it [RFID] implanted is not going to be the hurdle." Retherford points to the younger generation as opposed to those in their 60s and thinks that those in their 20s will just view RFID implants as yet another technique akin to their iPod and cell phone. He parodies: "Ah, my chip doesn't work so therefore I need to go get some maintenance done". Retherford explains with reference to Gen Ys:

> "[t]hey're going to look at this and they're going to wonder why we ever had this discussion because they're going to say, "Well, I have the chip and somebody did knock my frequency out or they did render it a problem so now I need to go [to]… a chipping centre if you would, I need to go in and get my chip reprogrammed… or something like that.""

5. Discussion

5.1 Opting Out of the Single Sign-On Chip

A big part of the argument for proponents of chip implants for humans has to do with the fact that it is argued that microchips will be optional. Retherford for one does not see chip implants as ever being forced. People will be given an option. This is the common mantra among business developers of implantables (Michael and Michael 2010). Yet, the authors of this paper believe that when services are tied to a citizen's implantable unique ID, without an "alternative" device, opting-out means a loss of services, perhaps even monetary loss (Michael and Michael 2012). There are consequences to opting-out even from "optional" systems. Retherford is confident, that when people will be faced with the alternative possibilities, that they would rather have the implant than not have it. Today, risks related to a multitude of technologies and applications are evident, but words like "consent" and "choice" and "opting-out" have almost become synonymous with politically correct statements. At least for now, we can speak about options and not mere compliance. But for how long?

5.2 Scope Creep and Common Concerns

As technology moves faster than the enactment of policy and legislation, it is innovation that is now driving new levels of technology acceptance. The bombardment of the diffusion of new innovations, day after day, at an exponential growth rate, has meant that consumers' expectations and their ability to adapt to changes in the marketplace have made them more resilient and to some extent more akin to the trialability of new ideas (Kurzweil 2005). But with the onslaught of new inventions, also comes the increasing importance of how these technologies can be used, beyond their original scope of design. It is on this aspect, that reports on implants and nanotechnology coming from very different sources agree. That is, sober sources of secondary data from those vested with the direction of a state's policy, legislation, law enforcement, bio-ethical and health opinions, are surprisingly similar

to those who are generally labelled as “conspiracy theorists” or “religious fundamentalists” or “human rights activists” or “anti-globalisation revolutionaries” (Michael and Michael 2010).

5.3 Human Rights

Despite the inspiration for the argument that different groups are putting forward regarding why people should or should not be implanted for commercial applications, it is important to bring diverse groups of people together to debate and discuss what the possibilities might herald, what they might mean today and well into the future. Discussions about human rights, liability and loss, and the potential for an invasion of privacy and breakdown of trust between organizations and citizens or insurmountable control of governments over citizens will have major repercussions well into the future. Are there potential detrimental effects for individuals who bear high tech devices? Privacy experts would well warn about the perils of maintaining a false sense of “freedom”, “security”, and “justice” based around convenience solutions which look like they are making life easier but are instead encroaching on our human rights.

6 Conclusion

We have numerous case studies to go on which demonstrate the successful deployment of Verichip-style devices and commensurate applications but for the time being implantables for non-medical applications have drizzled for all but the hobbyist implantees, systems engineering researchers and artists. This does not mean that the potential for RFID implantees has gone- we may still be waiting for that next generation who may demand an *iplant* just like the current generation has demanded an iPod, iPhone and iPad. How the next generation go about achieving risk return might be using a completely new paradigm. If the risk taking behaviour is successful the dividends are purported to be great, but equally if the risks taken are not calculated the effects might well be detrimental and have long-term repercussions for humanity, for which there will be no turning back. One thing is clear that despite the arrival of the implantable microchip, we have not yet seen it unleashed in all its fullness. As a community of stakeholders, we have a great deal of thinking to do between now and then but perhaps not a commensurate time to act. Verichip Corporation may no longer be but there are now numerous other companies, including Positive ID and VeriTeQ who are deploying applications for RFID implants in the ‘care’ space. The potential for function creep is there for care-style applications to be underpinned by services that are principally oriented around consumer control.

REFERENCES

Applied Digital Solutions. (2003). "Implantable Personal Verification Systems." Retrieved 15 April 2004, from http://www.adsx.com/prodservpart/verichip.html.

Associated Press. (13 February 2006). "Company implants ID chips into employees' arms." Retrieved 19 October 2010, from http://www.foxnews.com/story/0,2933,184722,00.html.

Associated Press. (September 2005). "RFID chips help track Katrina dead " Retrieved 25 October 2010, from http://www.msnbc.msn.com/id/9514138/.

BBC. (11 May 2002). "US family gets health implants." Retrieved 26 October 2010, from http://news.bbc.co.uk/2/hi/health/1981026.stm.

Graafstra, A., K. Michael, et al. (2010). Social-Technical Issues Facing the Humancentric RFID Implantee Sub-culture through the Eyes of Amal Graafstra. International Symposium on Technology and Society, Wollongong, Australia, IEEE Computer Society.

Klein, N. (2007). Shock Doctrine. New York, Metropolitan Book.

Kurzweil, R. (2005). The Singularity Is Near: When Humans Transcend Biology. London, Penguin.

Magnet, S. (2011). The Audible Body. Corpus: An Interdisciplinary Reader on Bodies and Knowledge. C. Monica and P. Currah. New York, Palgrave MacMillan**:** 139-153.

Masters, A. and K. Michael (2007). "Lend Me Your Arms: the Use and Implications of Humancentric RFID." Electronic Commerce Research and Applications **6**(1): 29-39.

Michael, K. and M. G. Michael (2010). The Diffusion of RFID Implants for Access Control and ePayments: A Case Study on Baja Beach Club in Barcelona. International Symposium on Technology and Society, Wollongong, Australia, IEEE Computer Society.

Michael, K. and M. G. Michael (2012). Implementing Namebers Using Microchip Implants: The Black Box Beneath The Skin. This Pervasive Day: The Potential and Perils of Pervasive Computing. J. Pitt. London, Imperial College Press**:** 100-145.

Reynolds, M. (20 July 2004). Despite the Hype, Microchip Implants Won't Deliver Security. Gartner Research, Gartner.

Six Sigma. (2010). "Six Sigma Security." Retrieved 19 June 2009, from http://www.sixsigmasecurity.com/index.html.

VeriChip. (9 October 2003). "VeriChip Corporation Launches First in a Planned Series of ``VeriGuard'' Secure Access Control Applications; First VeriGuard System Now Installed and Functioning." Retrieved 30 November 2010, from http://findarticles.com/p/articles/mi_m0EIN/is_2003_Oct_9/ai_108679224/.

Warwick, K. (2002). I, Cyborg, Century.

WND. (10 February 2006). "Employees get microchip implants: Company requires controversial device for certain workers." Retrieved 19 October 2010, from http://www.wnd.com/?pageId=34751.