PerAdaMagazine
towards pervasive adaptation
10.2417/2200904.1598

Predicting the socioethical implications of implanting people with microchips

Katina Michael and M. G. Michael

Privacy, security, trust, control and human rights are all concerns that need to be addressed before widespread diffusion of advanced identification technologies.

Implants for humans are not new. The installation of pacemakers in humans and a great number of other medical innovations for prosthesis are now considered straightforward procedures. Today we have even realised the potential for microchip implants to be embedded inside the human body for the purpose of acting as unique lifetime identifiers (ULIs). Tiny radiofrequency identification (RFID) devices with on-board sensors are now being used to identify people uniquely and to provide access to other data such as medical records.

Some of the major problems pertaining to microchip implants are related to who or what is in control of the personal data stored and gathered from such devices. While each new implanted device might well be in accordance with governing regulations for commercial purposes, this does not necessarily mean that the risks associated with that particular application have been nullified. The popular perception is that compliance with common standards and regulations, and adherence to state laws means that the device is not only safe to use but is also certainly not illegal. The question of ethics and ethical practices, however, clouds the technology, which by its very nature is penetrating, trespassing into that most sacred of spaces: the human body. The natural possession of the self becomes to a degree the property of a third-party stakeholder, someone other than the 'I'. This condition beckons new explorations into the traditional world of metaphysics, particularly to do with questions connected to identity and consciousness.

Numerous attempts have been made to clarify and to solve the problems that humancentric implants have created. These fall into a number of categories: self-based assurance controls, like those founded on proprietary standards, and anti-hacking and anti-cloning devices such as metal coverings to obstruct unauthorized reads of the chip; state legislative initiatives such as the anti-chipping bills enacted in Wisconsin and North Dakota in the United States, stipulating that if an individual enforcedly chip-implants another, the commensurate penalties apply; technology assessment such as that conducted in the European Union to explore the question of ethics using a universal panel of experts with diverse backgrounds; use-case analysis whereby active chip-implant trials took place in the United Kingdom and United States, gathering participant feedback (see Figure 1); clinical trials sponsored by private organizations to gauge the potential health side effects of implants in people; and surveys measuring consumer acceptance and attitudes towards microchip implants

Figure 1. *Amal Graafstra has two radio-frequency identification (RFID) implants. The one in his right hand was implanted by a family doctor using an Avid injector kit like the ones used on pets. He can access his front door, car door and log into his computer using his implants. (Photo courtesy of Amal Graafstra, Bellingham, United States, 2007.)*

Continued on next page

for use in national security. All of these approaches have helped to inform research at large, but none has completely addressed the complex issues surrounding the socioethical implications of microchipping people.

Our approach has been to study the usability contexts of humancentric microchip implants to determine a plausible list of applications, including control, care and convenience-based applications within a tag, track and trace paradigm. We have also sought to define the position of various stakeholders in the microchip implant value chain: end user, subscriber (e.g. carer, guardian, parent, spouse, employer, insurance company etc.), call-centre operator, service provider, network provider, device manufacturer, and government agency. The approach is multi-pronged, borrowing methodologies from multiple disciplines to enrich the findings and inform the principal questions. The methodologies adopted for the greater part are qualitative given the exploratory nature of studying socioethical perspectives. But we have also found room for quantitative analysis, such as surveys, spatial logs (e.g. detailed waypoints and routes) and digital chronicles (e.g. time, distance, speed and altitude stamps).

Some of the ethical issues that we address in our research can be discussed in the context of what some modern thinkers have called the precautionary principle. The fundamentals of this approach can be found in Weckert and Moor,[1] who advise that, "[i]f some action has a possibility of causing harm, then that action should not be undertaken or some measure should be put in its place to minimize or eliminate the potential harm." Of course, the niggling question remains: who or what will be trusted to determine which action(s) should or should not be undertaken?

We have grounded the research in the historical case method and devised best case/worst case scenarios on principles founded in commercial offerings. The predictive element has been a strong force in all our studies, and we have captured the auto-ID trajectory within the field of high-tech innovation. We have encouraged, as much as possible, public discourse and critical debate on the matter, reaching out to diverse audiences—researchers, students, citizens, vendors, radio and newspapers, government agencies—in an advocate role to stimulate discussions, albeit which some have considered premature. One might well ask whether we can prejudge ethics before an application has taken root, but post widespread diffusion of microchip implants, there will be no turning back. We have sought comprehensive interviews with key informant implantees to gauge their feelings and attitudes towards the pros and cons of RFID implants, providing hypothetical scenarios, with a focus on user-centred design. We have also simulated trials based not only on microchip implants but also on converging capabilities such as location services and conditional monitoring. The big picture cannot be ignored. It is not sufficient to study implants alone. The early indications are that ID + location + sensors will work in concert to offer subscribers advanced value-added services. With this in mind, we have also studied US case law seeking examples related to the tracking and monitoring of citizens and employees.

We have discovered that the act of 'chipification' has been founded on four main motivations: the do-it-yourselfer implantee, such as Amal Graafstra,[2] who can be considered a hobbyist implantee; the pioneer cybernetics participant-researcher, such as Kevin Warwick,[3] who conducted the Cyborg 1.0 and Cyborg 2.0 experiments seeking biomedical breakthroughs; the commercial organization offering patient ID for wander alerts, drug delivery and biosensing, such as the VeriChip Corporation[4] and the Digital Angel Corporation;[5] and the government that seeks to maintain social security, like Indonesia's Papua Legislative Council, which in 2007–08 hoped to implant HIV/AIDS sufferers for the purpose of monitoring their actions through a unique ID.[6]

In each of these settings the power relationship is disproportionate: first because of the dynamics between stakeholders and second because RFID implants are a matter to do with people and machines. Inevitably during the research we have had to create a small number of new terms to capture the essence of what we've discovered. We have tested notions such 'electrophorus' (a bearer of technology),[7] 'uberveillance' (neverending surveillance, a type of big brother on the inside looking out),[8] and 'electromagneticus' (a person's ability to interact with their environment using an embedded machine through electromagnetic principles).

The research will continue to address complex ethical questions in a predictive manner so long as diffusion of microchip implants remains ethically questionable. Issues such as whether it is ethical to embed an individual with a device they cannot remove, even if they have given their prior consent to be implanted, will be further explored. Already the infrastructure surrounding implants for identification is growing in some nation-states. In the United States alone, 1000 medical facilities have embraced RFID implant technology for patient identification. We will also interview an even greater cross-section of key informants, pioneering figures from across the disciplines and general public, to ascertain the potential use and misuse of inter-

Continued on next page

connected tracking and monitoring technologies.[9] The convergence of implantable devices with mobile phones and satellite and spatial technologies will inevitably have an impact on the surveillance field. It is our hope that we will continue to run our own small-scale trials using pinpoint positioning systems whereby we may be able to specify the consequences of emerging technologies for different contexts.

This research has been partly funded by the Research Network for a Secure Australia (2006–08), which sponsored three national workshops and proceedings on the theme of national security. We would also like to acknowledge the support of the Australian Research Council for a discovery grant (DP 0881191) on the regulation of the location-based services industry, and the University of Wollongong for an infrastructure grant towards establishing an RFID/LBS laboratory.

Author Information

Katina Michael and M. G. Michael
School of Information Systems and Technology
Faculty of Informatics
University of Wollongong (UOW)
Wollongong, Australia

Katina Michael received her PhD from the UOW, where she is now a senior lecturer. She is a senior member of the IEEE and a board member of the Australian Privacy Foundation.

M. G. Michael is a theologian and historian who brings a unique perspective on information technology. He is an honorary senior fellow in the School of Information Systems and Technology at UOW. He is also a member of the American Academy of Religion.

References

1. J. Weckert and J. Moor, *The precautionary principle in nanotechnology*, **Nanoethics 20** (2), pp. 191–204, 2006.
2. A. Graafstra, *Hands on*, **IEEE Spectrum 44** (3), pp. 14–19, 2007.
3. K. Warwick, **I, Cyborg**, Century, London, 2002.
4. http://www.verichipcorp.com Verichip Corporation home page. Accessed 2 January 2009.
5. http://www.digitalangel.com Digital Angel home page. Accessed 15 January 2009.
6. http://www.rnzi.com/pages/news.php?op=read&id=33896 Papua Legislative Council deliberating microchip regulation for people with HIV/AIDS, Radio New Zealand International. Accessed 12 October 2007.
7. K. Michael and M. G. Michael, *Homo electricus and the continued speciation of humans*, in M. Quigley ed., **Encyclopedia of Information Ethics and Security**, 1st ed., pp. 312–318, IGI Global, Hershey, PA, 2007.
8. K. Michael and M. G. Michael, **From Dataveillance to Uberveillance and the Realpolitik of the Transparent Society**, 1st ed., University of Wollongong, Wollongong, 2007.
9. K. Michael and M. G. Michael, **Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants**, 1st ed., Information Science Reference, Hershey, PA, 2009.