

*Faculty of Informatics*

*Faculty of Informatics - Papers*

---

*University of Wollongong*

*Year 2008*

---

# Microchip Implants for Humans as Unique Identifiers: a Case Study on VeriChip

K. Michael\*

M. G. Michael†

R. Ip‡

\*University of Wollongong, [katina@uow.edu.au](mailto:katina@uow.edu.au)

†University of Wollongong, [mgm@uow.edu.au](mailto:mgm@uow.edu.au)

‡University of Wollongong

This article was originally published as Michael, K, Michael, MG, & Ip, R, Microchip Implants for Humans as Unique Identifiers: a Case Study on VeriChip, Ethics, Technology and Identity Conference, 18-20 June 2008, Delft, The Netherlands, 1-4.

This paper is posted at Research Online.

<http://ro.uow.edu.au/infopapers/586>

Title:

Microchip Implants for Humans as Unique Identifiers: a Case Study on VeriChip

Authors:

Dr Katina Michael, Dr M.G. Michael, Mr Rodney Ip  
{katina, [mgm](mailto:mgm@uow.edu.au)}@uow.edu.au, [rawdney@gmail.com](mailto:rawdney@gmail.com)

Affiliation: School of Information Systems and Technology, Faculty of Informatics,  
University of Wollongong

Corresponding author: Katina Michael, +61242213937

Extended Abstract:

Microchip 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 body of humans for the purpose of acting as unique lifetime identifiers (ULI). Tiny radiofrequency identification (RFID) devices are now being utilised to store a unique 16-digit identification number.

A significant paradigm shift has occurred in ‘how’ technology is being utilised by humans and ‘where’ it is being applied, requiring a commensurate ethical response from the broader community. For instance, what does it mean for technology to be embedded beneath the skin in a perfectly healthy human being for the purposes of ‘easy’ identification or even amplification? Is an implant for non-medical purposes a basic breach in a human’s rights? Are implant IDs, even if consent has been granted by the recipient, in direct conflict with a State’s privacy laws? And what happens if an implant cannot be removed “on demand” because it has become intertwined with tissue in the body?

It is estimated that there are over two thousand recipients of these tiny identification devices, most of which are sourced back to the Food and Drug Administration approved products of the VeriChip Corporation, based in the United States. The premier implantable VeriChip is used for the VeriMed application, namely patient identification. There are over 900 registered medical facilities that are now equipped with VeriChip readers. The VeriMed system claims to overcome the problems often associated with ‘at-risk’ individuals. For example, to aid patients in times of crisis- if they have collapsed, suffered memory loss, are unable to communicate, or have a complex medical history they cannot recollect.

Corporate marketing identifies the following benefits of the VeriMed system: rapid identification in the emergency response (ER) room, instant medical record access, and improved emergency response. The chip simply stores a unique identification number, and associated medical records are stored in a secure global Verichip subscriber (GVS) registry database. The chip is inserted through a basic medical procedure, in the subdermal layer of the skin in the left or right upper arm, much as in the case of dog or cat implant. VeriChip’s other non-implantable applications are related to infant protection, wander prevention, and emergency management among others.

One of the major concerns of the VeriChip, despite its FDA approval, is that the actual chip consists of a tissue-bonding cap that is designed to prevent the chip from moving around once it has been implanted inside the body. A series of veterinary and toxicology studies have found that chip implants, similar to the VeriChip, had caused malignant tumours in animals. The CEO of the VeriChip Corporation recently refuted the claims of the potential for tumours in humans, stating that the technology had been used for more than 15 years, and that the company had received no complaints about from VeriMed subscribers about the FDA approved anti-migration caps.

RFID do-it-yourselfer implantees, like Amal Graafstra, have indicated that the problem with the VeriChip is the depth of the implantation, and the fact that a given individual cannot remove the device without causing bodily harm. Mr Graafstra indicated the problem with the VeriChip is the propensity for it to become engrained in tissue and muscle, and to become one with the body over a short period of time. Professor Kevin Warwick has also discussed this problem, after his Cyborg 1.0 experiment which lasted only ten days. Others like the not-for-profit MedicAlert information service claim that it is unnecessary to embed an individual with a device when less-expensive non-invasive techniques abound.

This leads to the ethical questions surrounding the technology and the potential for the technology to be used outside medical applications. Is it ethical to embed an individual with a device they cannot remove themselves, even if they are voluntarily subscribing to commercial service at a given point in time? What happens when an individual decides to opt-out of a VeriMed subscription after 12 months? Is the procedure painless or even possible? Who gets to decide who gets chipped, especially in the case of minors or those suffering from mental illness? And what of the potential for RFID, promoted as purely IDentification devices, when they are coupled with cellular or other satellite tracking network capabilities like global positioning systems (GPS)? There are a great number of unanswered questions here. What scientific endeavour has shown us historically, time and time again, is if something is possible, it is inevitable.

While the VeriChip Corporation has documented an explicit privacy policy on its website, pertaining to implantable chips in humans, a privacy policy does not really address the total question of ethics. The company claims, “privacy is our ethical responsibility”, and while this paper does not refute the organisation’s intent, it does point out that privacy is merely one aspect of ethics. The VeriChip system, like any technology is not foolproof. Human error is ever present, and errors in data entry on the GVS may even have a detrimental effect on an incapacitated individual. And the VeriChip system is rendered useless if emergency services or hospitals are not adequately fitted with the right technology to read unique IDentification numbers. There are also all too common network disruptions, power failures, and other technical issues that render the implantable technology completely ineffective. Again, this is not to say that the technology cannot save lives but in its present form, there are obvious problems, many of which are bound to legislative concerns. The long-standing debate over biometrics as unique identifiers have subsided more recently as legislators have ruled that given the level of intrusiveness of biometrics is minimal, i.e., it does not break the skin, it is permissible to be collected for the purposes of national security.

One of the underlying issues of the VeriMed system is the control aspect. In VeriChip's privacy policy it is outlined that "the content of the database itself [health records] and eligibility for access to the database are under the control of the VeriMed patient." Control however is a separate matter to consent. The organisation also claims that the VeriMed is tamper-proof and loss-proof. This may be the case with the actual database but the actual chip implanted in the subscriber is not without tampering and loss. There have already been numerous RFID trials that show how a subscriber attack can render an RFID chip useless (e.g. ePassport), then what? Even during seemingly harmless information technology trade fairs, repeated warnings are noted to delegates who have pacemakers or cochlear implants to "not approach" certain exhibits.

Today we have verified accounts of the VeriChip system being used for law enforcement personnel identification, VIP club lounge entry, as an anti-kidnapping technology, and even for employee physical secure access. Though these cases are admittedly limited, the potential for widespread use of microchip implants in humans is real and possible. The cost of getting a VeriChip is merely US\$200 with an additional \$10 monthly fee to store the information on the company's web site. To early adopters of technology this would seem like another telecommunications subscription plan.

This paper explores the ethical concerns related to semi-permanent implantable microchips for unique human identification. The paper uses secondary qualitative resources and three primary interviews with implantees to explore ethical issues. It also considers the potential for widespread adoption of RFID transponder implants, beyond voluntary subscription, or niche applications such as prison inmate tracking, and even national security.

## REFERENCES

- Banbury, C. M. (1997), *Surviving Technological Innovation in the Pacemaker Industry 1959-1990*, Garland Publishing, New York.
- Lewan, T. (2007). "Chip Implants Linked to Animal Tumours" *The Associated Press*, [http://www.washingtonpost.com/wp-dyn/content/article/2007/09/08/AR2007090800997\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2007/09/08/AR2007090800997_pf.html) [Accessed 24 October 2007].
- Masters, A. & Michael, K. (2007). "Lend me your arms: The use and implications of human-centric RFID," *Electronic Commerce Research and Applications*, 6(1), pp. 29-39.
- Michael, K. (2007). Interview with Mr Amal Graafstra, conducted by Dr Katina Michael, and transcribed by Mr Rodney Ip together with Katina Michael.
- Michael, K. (2004). "Location-based Services- a vehicle for IT&T convergence" in *Advances in E-Engineering and Digital Enterprise Technology*, Professional Engineering Publishing, UK, pp. 467-477.

Michael, K. & Michael, M.G. (2004). "The social, cultural, religious and ethical implications of automatic identification", *Proceedings of the Seventh International Conference in Electronic Commerce Research*, Dallas, Texas, USA, 10-13 June, pp. 433-450.

Michael, M.G. (2007). Interview with Professor Kevin Warwick, conducted by Dr M.G. Michael, and transcribed by Mr Rodney Ip together with Katina Michael.

Michael, M.G. (2007). Interview with Professor Chris Toumazou, conducted by Dr M.G. Michael, and transcribed by Ms Sarah Fusco with Katina Michael.

VeriChip. (2007). "Company: Privacy Policy", *VeriChip Corporation*  
<http://www.verichipcorp.com/content/company/privacy> [Accessed at 7 December 2007].

VeriMed. (2007). "Solutions: VeriMed", *VeriChip Corporation*  
<http://www.verichipcorp.com/content/solutions/verimed> [Accessed at 7 December 2007].