# Chapter XV
# Uberveillance

## INTRODUCTION

Uberveillance, also überveillance, is an *above* and *beyond*, an *exaggerated*, an almost omnipresent 24/7 electronic surveillance. It is a surveillance that is not only "always on" but "always with you" (it is *ubiquitous*) because the technology that facilitates it, in its ultimate implementation, is embedded within the human body. The problem with this kind of bodily invasive surveillance is that *omnipresence* in the 'physical' world will not always equate with *omniscience*, hence the real concern for misinformation, misinterpretation, and information manipulation (Figure 1).

*Uberveillance* is an emerging concept, in the full sense of both its application and power it is not yet entirely arrived (Michael & Michael, 2006; Michael, McNamee, Michael & Tootell, 2006; M.G. Michael, 2007; M.G. Michael & K. Michael, 2009; K. Michael & M.G. Michael, 2009). For some time Roger Clarke's (1988, p. 498) *dataveillance* 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 (Snow, 2005), that there was a pressing need to formulate a new term to convey both this present reality, and the *Realpolitik* (policy primarily based on power) of our times (Michael & Michael, 2007). It should be said, however, that if it had not been for dataveillance, uberveillance could not be. And for that matter, it must be emphasized that dataveillance will always be- it will provide the scorecard for the engine being used to fulfill uberveillance. The word itself gained entry into the *Macquarie Dictionary* in 2008 and the noun is defined as: "an omnipresent electronic surveillance facilitated by technology that makes it possible to embed surveillance devices in the human body" (Macmillan, 2009; McIlwain, 2009).

Uberveillance takes that which was "static" or "discrete" in the dataveillance world, and makes it "constant" and "embedded". Consider it not only "automatic" and to do with "identification" BUT also about "location"- that is, the ability to automatically locate AND identify- in essence the ability to perform *automatic location identification* (ALI). It has to do with the fundamental "who" (ID), "where" (location), "when" (time) questions in an attempt to derive "why" (motivation), "what" (result), and even "how" (method/plan/thought). Uberveillance can be a predictive mechanism for one's expected behavior, traits, characteristics, likes or dislikes; or it can be based on historical fact, or something in between. The inherent problem with uberveillance is that facts do not always add up to *truth* (ie as in the case of an exclusive disjunction T+T=F), and predictions based on intelligence are not always correct.

*Figure 1. Mr Amal Graafstra has two RFID implants, one in each hand, as shown by this x-ray. His left hand contains a 3mm by 13mm EM4102 glass RFID tag that was implanted by a cosmetic surgeon using a scalpel to make a very small cut, into which the implant was placed. His right hand contains a 2mm by 12mm Philips HITAG 2048 S implant with crypto-security features and 255 bytes of read/write memory storage space. It 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. Courtesy of Mr Amal Graafstra.*


## BIG BROTHER ON THE INSIDE LOOKING OUT

### Microchip Implants

Uberveillance is more than closed circuit television (CCTV) feeds, or cross-agency databases linked to national identity cards, 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 automatic identification technologies that we carry with us. It has to do with "under the skin" technology that is embedded in the body like microchip implants (Offman, 2007); it is that which cuts into the flesh- a charagma ("mark"). Think of it as Big Brother, on the inside looking out (Figure 2). This charagma is virtually meaningless without the hybrid network architecture which supports its functionality: to make the person a walking online node, beyond luggable mobile phones, PDAs and smart cards. We are referring here, to the lowest common denominator, the smallest unit of tracking- presently a tiny chip in the body of a human being.

Implants cannot be left behind, cannot be lost, 'cannot' be tampered with, they are always on, can link to objects, 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 (Swedberg, 2007;