Converging and coexisting systems towards smart surveillance

Katina Michael
University of Wollongong, katina@uow.edu.au

M G. Michael
University of Wollongong, mgm@uow.edu.au

Publication Details
Converging and coexisting systems towards smart surveillance

Abstract
Tracking and monitoring people as they operate within their personal networks benefits service providers and their constituents but involves hidden risks and costs.

Keywords
converging, surveillance, towards, coexisting, smart, systems

Publication Details

This journal article is available at Research Online: http://ro.uow.edu.au/eispapers/85
Tracking and monitoring people within their personal networks as they go about their daily business has a number of benefits for service providers and their constituents but also comes endowed with hidden risks and costs.

Automatic identification technologies, CCTV cameras, pervasive and mobile networks, wearable computing, location-based services, and social networks have until recently served distinct purposes. We have considered the trajectory of all these innovations within the information and communication technology industry and have observed patterns of integration, convergence and coexistence. For example, location-based social networking can draw on a smart phone’s capacity to uniquely identify and locate a user within 1-2 metres of their position and share this data across a user’s social network in real-time.

What is the trajectory to all of this depth-charged surveillance? Business intelligence now means that company data centers share bits and bytes that denote time, location, speed, altitude and temperature stamps used to infer someone or something’s physical, social, economic context or state. The tracking part of the equation is fairly simple, as rich chronicles are kept of discrete events and are limited only by storage, network access, transmission and processing speeds. The monitoring of humans interacting with one another and with resources is more complex, as changes in states have a domino effect throughout systems of systems.

Tracking people is possible through smart phones which house components for identification and geolocation. Using complementary body worn or implantable solutions can tell us what condition someone is in and how we should respond to that condition. Theoretically at least, implants are also not transferable. Animals are now increasingly being microchipped and non-living things have been barcoded/ tagged for decades. Being able to associate people with resources (e.g. vehicles) within a given social network can lead to unforeseen optimization in business processes. Consider the human as the most granular node in an autonomic computing environment. Human actions and interactions have system-to-system reactions.

While we are yet to see fully-fledged self-awareness in autonomic computing systems we have chosen to investigate the area of study using fundamental socio-technical design theory. We are not merely concerned by the proposed technology and what it will be able to achieve once instituted but with the social changes and impacts that will be enacted as a result. We are critically reflecting on the limitations of this “smart” surveillance and how it may be attractive to some constituents and abhorrent to others. The work is interdisciplinary, emphasizing the importance of studying the controllers (ie providers) and the controlled (ie users).

We have investigated emerging technologies within a research, business development, and emergency services context. We have identified the relationships between
stakeholders who have openly declared a financial interest in microchipping people, composed of private companies, institutes, government-funded organisations, and venture capitalists. Multiple sources of evidence have been used to examine the very real possibility that ordinary people will have iPlants (internet-enabled implants) to communicate with each other, with their pets, with the things around them (see Figure 1). Our proposed roadmap has been validated by in-depth interviews with key informants of these organisations to better understand the future vision and ensuing risk-related consequences.\textsuperscript{7}

Filed patents, company web sites, media releases and newsletters, news and industry magazines, social media blogs, even law and policy agendas provide crucial evidence that informs the push to microchip people. For example, the reduction of carbon emissions if every person was tagged, as energy would be drawn only when required. We have taken these vivid qualitative snapshots and narrated a bigger picture view of the possibilities ahead. We have named this “smart” surveillance, überveillance- an omnipresent electronic surveillance facilitated by technology that makes it possible to embed surveillance devices in the human body. Überveillance is reliant on ubiquitous infrastructure.\textsuperscript{8}

In constructing scenarios of what this age of überveillance might look like, we have considered the best and worst case outcomes for a global society. We have focused on scenarios to do with health, insurance, law enforcement and national security. No doubt, the widespread introduction of implants would impact on the digital divide debate. We have also launched transnational surveys to gauge the level of practical interest in adopting these kinds of technologies in more developed countries. Convenience seems to be a preoccupation for many people but more important are human rights,\textsuperscript{9} ethics,\textsuperscript{10} trust\textsuperscript{11} and privacy.\textsuperscript{12} Bodily intrusion concerns particularly abound.

For autonomic computing to work it will require the identification of the “self” in relation to “others” and “things”. The problem with instituting microchip implants to facilitate this new “web of things and people” environment has to do with who is doing the controlling and who will be controlled. It is often about the powerful and the powerless. Future work will investigate the axis of access, the potential for proactive criminalization, the consequences to living off the grid, and the defined limits of überveillance which are misinformation, misinterpretation, and information manipulation.\textsuperscript{13} We will come close to omnipresence but never to omniscience.

Acknowledgments
This research has been funded in part by an Australian Research Council-Discovery grant on location-based services, DP 0881191. The authors of this paper would also like to acknowledge the support of all those who have engaged with them on discussions on überveillance, practitioners and academics alike, towards its application across disciplines.
Figure 1. The microelectrode array used in the Cyborg 2.0 project that was inserted into a guiding tube and placed into a two inch incision made above Kevin Warwick’s wrist and then fired into the median nerve fibers below his elbow joint. The procedure took a little over two hours to complete. Courtesy of Kevin Warwick.
7 Video of a panel debate on microchipping people delivered at the International Symposium on Technology and Society 2010 (IEEE ISTAS10) that was held at the University of Wollongong, Australia. Credit: Katina Michael, University of Wollongong. http://www.youtube.com/watch?v=dl3Rps-VFdo