Mark Weiser, the founding father of ubiquitous computing, once said that the problem surrounding the introduction of new technologies is *often couched in terms of privacy, but is really one of control*. Indeed, given that humans do not by nature trust others to safeguard their own individual privacy, in controlling technology we feel we can also control access to any social implications stemming from it. At its simplest, this highlights the different focus between the end result of using technology and the administration of its use. It becomes the choice between the idea that I am given privacy and the idea that I control how much privacy I have. Sweeping legislative changes in the United States have meant that visitors must now have their biometric registered before they are allowed to enter the country. Even despite a dim general acceptance of biometrics in recent years, the new border-entry scheme (stipulated in the Enhanced Border Security and Visa Entry Reform Act) has not stopped the majority of travelers from visiting the U.S. This is perhaps because there is a bargain of exchange - *I'll give you what you want if you let me do what I want*. Privacy is traded for access.

While this border security scheme does provide a certain level of social control to the end-user (there is always the option not to travel to the U.S. at all), what some civil libertarians fear, beyond privacy, is a government-driven mandatory introduction of invasive technologies based on the premise of national security. While the safety and security argument has obviously paved the way for some new technologies in response to the new environment of terrorism and identity fraud, there is now a concern that further advancements will begin to infringe on the freedoms that security paradigms were originally designed to protect.

The question is- what next? Mandatory census-based DNA sampling or even chip implants? Though most believe that government-imposed mandatory

implantation is a highly unlikely scenario, private enterprises have already introduced radio-frequency identification (RFID) subdermal implants in employees, inmates and other distinct population groups.

Regulation is necessary. When data collected for a given *voluntary* service (using a device above or beneath the skin), is then subsequently used for law enforcement or government surveillance purposes, consumers may think twice about employing the technology. These *unintended consequences* are those that may well have the greatest impact on end-users. In regulating them we do not want to allow unrestricted deployment and unparalleled capabilities for commercial data mining, but nor should we allow a doomsday scenario where all citizens are monitored in a techno-totalitarian state. G.J. Pottie echoes these sentiments by stating that without appropriate architecture and regulatory controls democratic values are at risk of being subverted, claiming that *information technology is not in fact neutral in its values* and that *we must be intentional about design for democracy*. Any scope for such design of regulations must further be considered in light of the privacy / security trade-off.