Somatic surveillance: corporeal control through information networks

Monahan, Torin; Wall, Tyler

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Surveillance & Society
Special Issue on 'Surveillance and Criminal Justice' Part 1, 4(3): 154-173
http://www.surveillance-and-society.org

Somatic Surveillance: Corporeal Control through Information Networks*

Torin Monahan and Tyler Wall[1]

Abstract

Somatic surveillance is the increasingly invasive technological monitoring of and intervention into body functions. Within this type of surveillance regime, bodies are recast as nodes on vast information networks, enabling corporeal control through remote network commands, automated responses, or self-management practices. In this paper, we investigate three developments in somatic surveillance: nanotechnology systems for soldiers on the battlefield, commercial body-monitoring systems for health purposes, and radio-frequency identification (RFID) implants for identification of hospital patients. The argument is that in present and projected forms, somatic surveillance systems abstract bodies and physiological systems from social contexts, facilitating hyper-individualized control and the commodification of life functions.

Introduction

Modern surveillance thrives upon the informatization of life. Nowhere is this more apparent than in emergent technologies and techniques of body surveillance. We identify "somatic surveillance" as the increasingly invasive technological monitoring of and intervention into body functions, which is a type of surveillance quickly becoming dominant in both military and medical domains. Somatic surveillance systems depend upon three interrelated processes: first, the translation of corporeal information (e.g., heart rate, hormone levels, temperature) into data, usually by means

* Acknowledgments: This material is based upon work supported, in part, by the U.S. National Science Foundation under Grant No. SES-0531194. Ideas for this article were developed in conversation with participants at the "Crime, Justice and Surveillance" conference at University of Sheffield, the "Generating Collaborative Research in the Ethical Design of Surveillance Infrastructures" workshop at University of Texas, Austin, and on the "Security, Surveillance and Social Sorting" panel at the International Sociological Association conference in Durban, South Africa (all held in 2006). Special thanks to David Murakami Wood, Kirstie Ball, David Phillips, David Lyon, and Michael Nagenborg.

[1] School of Justice and Social Inquiry, Arizona State University, USA. mailto:torin.monahan@asu.edu

 ISSN: 1477-7487

of sensors applied directly to or embedded within the body; second, the communication of those data across networks, effectively situating bodies as "nodes" on larger information networks; and third, the intervention into body functions through various sociotechnical feedback mechanisms. This last step is the crucial one for marking the point at which the monitoring of bodies turns into surveillance. Within this final part of the process, bodies are not only informatized but controlled in various ways. The systems, in other words, do not merely generate data; they also produce social norms, technical constraints, and network commands.

In this paper, we investigate three developments in somatic surveillance: nanotechnology systems for soldiers on the battlefield, commercial body-monitoring systems for health purposes, and RFID implants for identification of hospital patients. Surveillance can result through the coupling of sensors with control functions, as within the new paradigm of "network-centric warfare" where bodies on the battlefield are recast as network nodes to be manipulated remotely. Control-based feedback can take more subtle, self-applied forms, as with individuals actively plugging their bodies into portable monitoring systems that supply them with detailed body information so that they can alter behaviors, such as exercise or diet, accordingly. Finally, medical devices such as radio-frequency identification (RFID) implants can facilitate the proper identification of hospital patients, but they also catalyze new opportunities for engaging in identity theft, tracking individuals surreptitiously, or simply shifting power to those with the ability to scan embedded chips – all of which may ramify back upon individuals to constrain them in various ways or compel them to alter their behavior.

Each of these forms of somatic surveillance acquires technological momentum and symbolic force through active discursive constructions of the future. Specifically, the systems are marketed as necessary and inevitable developments and are generously funded for their promised revolutionary outcomes. Thus, discursive efforts to construct a "history of the future" are intimately linked to the state of the systems, support for them, and meanings attributed to them. For these reasons, it is crucial to attend to discourses of the future, because oftentimes with such nascent technologies, the symbolic meanings are far more real and operational (in the present) than are the largely fictitious systems (for now). So, whereas RFID implants, for instance, currently do not monitor body functions as such, these "features" are in development, so the systems should be analyzed for their somatic surveillance promise, potential, and threat.

The argument advanced here is that in present and projected forms, somatic surveillance systems abstract bodies and physiological systems from social contexts, facilitating hyper-individualized control and commodification of life functions. Control intensifies and spreads by means of informatizing corporeal systems and then linking those systems to larger networks for goals of capital accumulation, military intervention, or identity regulation (c.f. van der Ploeg, 2005). All the while, it must be noted, many immediate requirements of populations are subsequently neglected in the quest for "preparedness" in the face of future needs or threats (Monahan, 2006c; Lakoff, 2006). There are discernable politics, therefore, in the kinds of systems perceived as valuable, and thus being funded, and in the overlaying of networks for pervasive monitoring onto existing and new infrastructures (Murakami Wood, nd; Murakami Wood and Graham, 2006; Graham and Wood, 2003). The task of this paper is to begin to unpack the assemblage that holds together systems of somatic surveillance. Following from Kirstie Ball's

(2005) research on body surveillance in organizations, our position is not that somatic surveillance systems are negative, perforce, but instead that they are closely connected to political economies, discursive regimes, and cultural mythologies, which are then absorbed into and co-produced by the technologies. We must recognize that technological assemblages such as these persist and propagate through power relations, not just chance networks (Haraway, 1997; Fortun and Bernstein, 1998; Haggerty and Ericson, 2000), and that analyzing those relations is critical for attaining nuanced understandings of emergent social fields and crafting appropriate responses.

'Biomedical Monitoring' on the Battlefield

Nanotechnology is a rapidly growing field of scientific research and product development, which includes the possibility for incredibly miniaturized and pervasive surveillance systems. Typically, nanotechnology refers to the engineering of matter on the molecular level (or on the scale of a billionth of a meter) to create materials with novel properties or devices that can function with great precision. Some examples might be surfaces that are almost completely friction-free or medical treatments that target specific cancer tumors without damaging other cells. To date, it must be noted, most nanotechnology has little to do with revolutionary medical treatments or other social goods; instead nanotech manifests in commercial products such as sunscreen, golf balls, or water-resistant clothing. Nonetheless, government agencies are investing heavily in nanotechnology for surveillance and security purposes, such as detecting chemical agents on crops or in public water supplies with nano-sensors (Thomas, 2003), or through more futuristic uses, such as integrating nano-sensors into paint or "smart dust" so that the built world continuously monitors people through vast nanotech networks (Poste, 2006; Rodrigues, 2006).

The US Department of Defense (DoD) has become extremely interested in the potentials of nanotechnology for military purposes. Of the $1.3 billion annual budget for the US National Nanotechnology Initiative (NNI), DoD's portion is $436 million, surpassing the National Science Foundation's allocation of $344 million (NSTC, 2006). One compelling example of a DoD project is the Institute for Soldier Nanotechnologies (ISN), which is part of a larger US Army project called "Objective Force Warrior." In 2002, the Army Research Office awarded a five-year, $50 million grant to the Massachusetts Institute of Technology (MIT) to establish ISN and conduct scientific research into nanotechnology as it relates to the needs of US soldiers. ISN consists primarily of at least 45 MIT faculty members, several Army scientists, other personnel, and industrial firms. The two prime institutional actors for ISN are MIT and the US Army, while Raytheon, DuPont, and Partners Healthcare are three of the "founding industrial partners" (ISN, 2006). ISN is currently exploring nano-sensor enmeshed "exomuscular" uniforms that harden upon forceful unwanted contact, and arm sleeves that can immediately transform themselves into medical "casts." Developing "active" camouflage through nano-sensors that visibly adapt to changing environments has also been considered as a possibility for military applications of nanotechnology. Most of these projects will probably include nano-sensors inserted into the fabric of uniforms to detect, among other things, the environmental presence of chemical and/or biological agents (Ratner and Ratner, 2004).

Relevant to our exploration of somatic surveillance, another goal of ISN is to enable military command centers to monitor the internal, physiological processes of individual soldiers on distant battlefields. Biomedical monitoring will occur through the use of "battlesuit" sensors to relay information to command centers about the physiological conditions and geographic location of soldiers. This projected networking effect aims to facilitate remote, real-time decision-making during military operations:

> The uniforms of the future could also use nanoscale sensors to detect soldier's physiological signs, monitoring heart rate, blood pressure, levels of hydration and chemical signs of stress. Military commanders could conceivably use the sensors to identify the most alert and battle-ready soldiers to serve as the mission's point people.
>
> (Wolfe, 2003)

However, inserting nano-sensors into the fabric of the soldier's uniform is not the only possibility for body monitoring and control. Daniel Ratner and Mark Ratner (2004) believe that it is possible to inject nano-sensors,

> into a soldier's bloodstream. The sensors would circulate through the bloodstream and could be monitored at a place where blood vessels are closest to the surface, such as in the eye. The monitoring unit could be installed in goggles or on a microphone boom of a communications headset. While quite invasive, these so-called *in vivo* sensors could also have other uses in continuously monitoring the health of a soldier.
>
> (Ratner and Ratner, 2004: 42-43; italics in original)

In addition to conducting battlefield triage from a distance, ISN states that their biomedical monitoring technologies will also have capabilities to control "the delivery and release of life-saving medications," which will again be implemented through some use of battlesuit nano-sensors: "Biomedical monitoring will be able to use ultrasound to detect a hemorrhage in the injured soldier and then cauterize vessels to staunch the bleeding" (ISN, 2006). In this light, biomedical monitoring uniforms are not only about data collection but about using this data as operable assistance for intervening into soldiers' biological systems.

The primary objective of ISN is to create nanotech-laced battlesuits that merge with the bodies of soldiers. Rather than making soldiers' bodies obsolete through automated military devices and weapons, the move instead is to integrate soldiers into information networks so that they can be controlled remotely to a greater degree than ever before, while ostensibly increasing their protection. For instance, ISN presents its work as designing a,

> 21st century battlesuit that combines high-tech capabilities with light weight and comfort. Imagine a bullet-proof jumpsuit, no thicker than ordinary spandex, that monitors health, eases injuries, communicates automatically, and maybe even lends superhuman abilities. It's a long range vision for how technology can make soldiers less vulnerable to enemy and environmental threats.

(ISN, 2006)

Forbes magazine adds to this discursive construction of the future benefits of nano-battlesuits:

> Imagine, if a soldier is in battle and happens to break his [*sic*] leg, nanomaterial could stiffen to form a hardened material that immobilizes the leg like a cast. Or if a soldier was shot in the arm and blood loss was a dire concern, the material could tighten and constrict blood flow around the wound to form a tourniquet. The potential exists for such a system to provide a soldier with superhuman strength.
>
> (Wolfe, 2003)

Such representations are fairly transparent allusions to comic book superheroes, replete with homoerotic overtones of which the scientists and military representatives seem unaware. Indeed, all nano-projects taking place at the Institute are rationalized through this biopolitical discourse of offering enhanced capabilities for surviving life-threatening situations. According to Ned Thomas, director of ISN, the "exomuscular" potential of nanotechnology "…tickles the generals" (quoted in Wolfe, 2003).

The promise of revolutionary technological potential orients all media on nanotechnology, of course, and is not limited to military applications. Nanotechnology is typically presented as a rapidly emerging sociotechnical field that cuts across all branches of science and engineering and therefore possesses the ability to alter all aspects of life (Ratner and Ratner, 2004). Nonetheless, the military applications of nanotech, as with other military technologies, are presented as "dual use," eventually benefiting society at large. As such, so the rationale goes, they should be supported by the public no matter what ethical concerns they raise. The convergence of public and private sectors in research is nothing new (Leslie, 1993), but as it intensifies, many social scientists worry that the public interest is being eliminated as public institutions conform to capitalist (and military) imperatives (Slaughter and Leslie, 1997; Strathern, 2005; Monahan, 2005).

In public statements, it is easy to discern the rhetoric of "what is good for the military is also good for society." For example, a promotional video for ISN concludes with a scene of flag-waving children running through a verdant field, while a voiceover says: "The result will not only be a safer world for soldiers, but a better place for all mankind [*sic*]."[2] Other documents make clear that the practical goal is the mutual benefit of the military and private industry, with industry serving as a problematic synecdoche of society as a whole:

> [ISN] actively looks for transitioning opportunities and commercial applications of the developed technologies. Partnering with industry brings scientific advances out of the laboratory and into the marketplace, accelerating large quantity, affordable production for the soldier.

[2] See the ISN website for a dramatic marketing video presenting potential cases where nanotechnology might assist soldiers: http://web.mit.edu/isn/aboutisn/isnvideo.html [accessed Janurary 11, 2007].

(ISN, 2006).

Will biomedical monitoring from a distance and its related technologies eventually be a practice common within "civil" medical establishments such as hospitals? According to *Forbes*,

> The DoD's sensor funding can be expected to bear fruit for the medical services industry, as advanced remote physiological sensing and monitoring could have an enormous impact on home monitoring in the nursing industry. In the process, it could lead to better at-home care for seniors, cutting health care costs.
>
> (Wolfe, 2003)

According to the former prime minister of Israel, Shimon Peres, "That which has been achieved by the atomic bomb in the field of military strategy will be accomplished in the future by nanotechnology in the field of *civil potential*" (quoted in Ratner and Ratner, 2004: 7; our emphasis).

The above analogy connecting the *actual* revolutionary atomic bomb and the *imaginary* revolutionary potential of nanotechnology for civil society should not be dismissed. The imagination is a potent force that organizes social life and structures experiences of the past, present, and future (Appadurai, 1996). Therefore, discourses about the revolutionary potential of nanotech should also be read as cultural tools for conjuring those worlds into existence,[3] while simultaneously foreclosing alternative pathways for technoscientific development. The power of the imagination can easily be seen within contexts of the development of military technology: "Can any vision of a possible future in which human destiny is intertwined with the development or use of science and technology, most especially weapons technology, *not* be a form of science fiction?" (Franklin, 1988: 168; emphasis in original). As Donna Haraway (1997) notes, science fiction quickly blurs into science fact, so the politics of futurity are also those of scientific truth claims.

By stressing the "new" groundbreaking features of nanoscience and nanotechnology, ISN and other proponents of nanotech biomedical monitoring seek to construct a "break in time" (Jenkins, 2002) or a point at which the future lifts off from the present, transporting us away from current problems and concerns. In this framing, any resistance to such bold futures is seen as increasing national vulnerability to terrorists who might not be as ethically constrained or responsible as the US. As retired Admiral David E. Jeremiah of the United States Navy told listeners at the Fourth Foresight Conference on Molecular Nanotechnology at the end of 1995:

> Somewhere in the back of my mind I still have this picture of five smart guys from Somalia or some other nondeveloped nation who see the opportunity to change the world. To turn the world upside down. Military applications of molecular manufacturing have even greater potential than nuclear weapons to radically change the balance of power. In anticipation of that possibility the

[3] Toumey (2004) raises a similar point about how nanoscientists reinterpret the past to lend historical credibility and mythical weight to their present-day endeavours.

> uninformed policymaker is likely to impose restrictions on development of technology in such a way as to inhibit commercial development (ultimately beneficial to mankind) while permitting those operating outside the restrictive bounds to gain an irrevocable advantage.
>
> (Jeremiah, 1995)

In other words, if policymakers and the public do not support nanotechnology research, the enemies of the US will exploit this gap to inflict harm upon the US, and ultimately the entire world. Therefore, this break in time allows for the construction of a future that is imagined as one where nanotech becomes a common but revolutionary staple of the military profession, one that is critical not only for the survival of individual soldiers but for that of the entire world, which may otherwise fall back into "the Dark Ages" (Jeremiah, 1995).

The ongoing transformation in warfare planning and management is referred to as "network-centric warfare" (NCW). According to the DoD, the governing logic of NCW is increasing the effectiveness of all military missions through "informational superiority," "deep sensor reach," "shared awareness" of information, and speed in making command decisions (Department of Defense, 2005). Therefore, NCW perceives the individual soldier and material weapons technology as disembodied, atomized data to be managed remotely. Sensor technologies partially afford this transformation: "Enable every weapon platform to be a sensor, from the individual soldier to a satellite" (Department of Defense, 2005: 10). To survive future wars and problems, individual soldiers are envisioned as having their physiologies constantly monitored by military-medical personnel.

Nanotechnology systems for soldiers represent one articulation of somatic surveillance. The three processes characteristic of somatic surveillance are all present within ISN's biomedical monitoring paradigm. First, the battlesuit sensor systems translate soldiers' physiological information into analyzable data. Second, this translation process positions the soldier's body as a node within military information networks such that physiological and locational data are communicated to command centers and other pertinent nodes. This process of turning a soldier's body into abstract, communicable data fits well within the US Department of Defense's overall strategic and logistical infrastructure of warfare. Last and most important, the ISN's integrated biomedical monitoring systems aim to produce mechanisms of bodily control. In this case, the life and death of individual soldiers can be regulated through intervening mechanisms built into the uniform. Obvious examples of mechanisms of control are the exomuscular material discussed earlier; the ability for the soldier's uniform to cauterize bleeding blood vessels, or the administering of medications within a localized environment. In addition, analyzing a soldier's physiological information in real time to determine his or her place on the front lines of a battle (Wolfe, 2003) is perhaps the most obvious example of somatic control. Here, the soldier's present physiological conditions, translated into data, directly inform her/his battle position and subsequent possibilities for life or death.

Wearable Body Monitors

Commercial body-monitoring systems represent new modalities in micro-management of the self. Especially for health or fitness purposes, systems proliferate for personalized management of physiological systems. Such systems are designed to monitor an individual's bodily attributes through sensor technologies worn on the human body, enabling individuals to better regulate their behavior. These systems encourage individuals to monitor and manage themselves in what appear to be discrete and objective ways. Nonetheless, health data, even about oneself, become commodities to be purchased by those who can afford them. Somatic surveillance, by this process, entwines with other contemporary mechanisms of social control to reify consumerist approaches to healthcare that subsequently exclude those who cannot afford to pay.

Some examples of body-monitoring systems include VivoMetrics' "LifeShirt System," which provides "continuous ambulatory monitoring" by means of a shirt embedded with sensors and intended to be worn throughout the day and night. The LifeShirt System converts cardiac, physiological, posture and other bodily attributes into data that can then be analyzed by medical professionals. According to VivoMetrics: "Patented sensors monitor patients 24/7 at work, home, play and sleep. The result is a robust suite of files and reports that give researchers and clinicians a diagnostic 'movie' of patient health instead of the traditional office visit 'snapshot'" (VivoMetrics, 2006). VivoMetrics markets the LifeShirt System primarily for use in clinical trials, academic research, and "home sleep diagnostics." A similar body-monitoring system is Sensatex's "SmartShirt System," which was first developed for military use by the Defense Advanced Research Projects Agency (DARPA) and the Georgia Institute of Technology (Sensatex, 2006). HealthGear offers a slightly different technology in the form of a wearable system that "consists of a set of physiological sensors wirelessly connected" via the user's personal cell phone so the body's health data can be displayed on the phone's screen (Oliver and Flores-Mangas, 2005). Finally, the company FitSense sells the "ActiHealth Monitoring System," which relies on an "ultra low-power wireless personal areas network, The BodyLan, which seamlessly connects our wearable & portable body sensors, data transport and feedback devices" (FitSense, 2006). FitSense products are "putting the body online!" by uploading "the data securely via the Internet to the FitSense data servers where the data is warehoused and then fed to the Provider's servers as required" (FitSense, 2006).

Recently, an alliance was formed among major technology corporations[4] to develop such body-monitoring technologies, with hopes of establishing an integrated, networked "ecosystem" of health care and fitness technologies (Medical News Today, 2006). These companies assert:

> Only by making computing intimate to the body can products begin to know our states of mind, our contexts, our states of health, etc. and respond (or have other aspects of the world respond) in intelligent ways. Sympathetic products, driven by computers worn on the body, are coming and **the industry** will grow up with wearable body monitoring at its core.
>
> (Teller and Stivoric, 2004; bold in original)

[4]Corporate founders of this alliance include "BodyMedia, Cisco Systems, GE Healthcare, IBM, Intel Corporation, Kaiser Permanente, Medtronic, Motorola, Nonin, Omron Healthcare, Panasonic (Matsushita Electric), Partners HealthCare, Polar Electro, Royal Philips Electronics, RMD Networks, Samsung Electronics, Sharp, The Tunstall Group, Welch Allyn and Zensys" (Medical News Today, 2006).

Body-monitoring systems translate corporeal information into data, relay this bodily data across information networks, and allow for the intervention of feedback mechanisms upon bodies. In other words, they lend themselves to surveillance functions – whether from medical professionals, personal trainers, automated systems, or oneself. The significant features of these systems, according to designers and promoters, are that they are wireless and comfortable to wear. For example, while individuals are working at their offices, they wear armbands that monitor physiological signs so that their personal data can be recorded and later analyzed at fitness centers or doctors' offices.

The marketing campaign of one company in particular – BodyMedia – underscores the surveillance implications of these types of systems. BodyMedia, founded in 1999 and based in Pittsburgh, Pennsylvania, sells a very popular body-monitoring system. This company claims to be the dominant leader in the design, development and marketing of body-monitoring technologies for everyday use, scientific research, fitness centers, and medical/healthcare institutions. BodyMedia systems collect and monitor "lifestyle information" such as calories consumed and expended, sleep patterns and duration, and other body functions. The company says:

> In order to find meaning in the vast streams of abstract, continuous data being collected, BodyMedia creates sophisticated, proprietary algorithms that accurately interpret and derive meaningful health and contextual information about the individual. By analyzing the raw data being emitted from your body, these algorithms derive useful information, such as the actual number of calories burned by your body, or the actual amount of sleep you got last night.
>
> (BodyMedia, 2006)

Similar to the "biomedical monitoring" features of military nanotechnologies, BodyMedia products rely on the use of biosensors;[5] however, the company prides itself on the implementation of "multi-sensors," which supposedly provide a "much more accurate, multi-dimensional view of the body than competing single-sensor technologies" (BodyMedia, 2006). The company's main body-monitoring products are "SenseWear" armbands, which are strapped around one's upper arm and then connected to computer systems for data tracking and analysis.

Fulfilling the needs of consumers within the context of a changing healthcare environment is one marketing strategy mobilized by BodyMedia. Healthcare is presented as being a domain dominated by elite practitioners in uncomfortable and artificially constrained institutional environments. An alternative vision, propounded by BodyMedia, would give greater agency to individuals to manage their own health continuously throughout their daily lives without depending entirely on professionals. The company argues:

[5]BodyMedia, however, does not use nanotechnology sensors.

> As the urgency of global health issues such as obesity, diabetes, and cardiovascular disease continues to grow, so too will the need for consumer-oriented body monitoring products. We believe that our body monitoring products will offer new solutions for these problems.
>
> (BodyMedia, 2006)

By offering these products and services, BodyMedia claims to "empower" consumers by generating important physiological/health information for them, doctors, personal fitness trainers, or other healthcare professionals (Medical News Today, 2006). In this context, body data are presented as being synonymous with individual empowerment: "Individuals are now empowered by having this timely information at their fingertips, while doctors and fitness pros can benefit from an unprecedented view of their patients'/clients' daily lives in order to make more informed health decisions" (BodyMedia, 2006).

BodyMedia argues that through the generation and analysis of important health information, consumers can attune themselves to their bodies and make better decisions about their health. Constructed as such, BodyMedia systems depend on an individualized, consumerist approach to healthcare, wherein the more plugged-in one is, the better the data will be for health maintenance. Thus, the technologies of BodyMedia are designed to be utilized "outside the hospital," "outside the gym," "outside the lab," "at the kitchen table," "while you sleep," "in the home," "in the nursery," "in the club," and so on. In short, ubiquitous connection of bodies to purchased technological systems and services becomes the hallmark of the healthy subject. Because good citizens are good consumers, anything less than becoming a willing data subject is framed as being irresponsible in some fundamental way. Therefore, BodyMedia technologies are designed to have an all-encompassing trajectory, capable of reaching into virtually every sphere of an individual's life while simultaneously promising to offer better lifestyles and performance enhancement. It is this hyper-extended reach and embeddedness that BodyMedia presents as tapping the "empowering" features of their technologies: "From diabetics to elderly persons living alone at home to individuals trying to lose weight or get fit safely and effectively, we make a difference in the lives of people everywhere" (BodyMedia, 2006).

These body-monitoring technologies can be situated within a neoliberal framework within which individuals mobilize "egoistic interests" to compete for survival within an increasingly "Darwinian world" (Bourdieu, 1998). The structural process of neoliberalism and consumer culture produces hyper-individualized effects of self-control, or what Mike Featherstone (1991) has called *body maintenance*: "The term 'body maintenance' indicates the popularity of the machine metaphor for the body. Like cars and other consumer goods, bodies require servicing, regular care and attention to preserve maximum efficiency" (Featherstone, 1991: 182). The insurance field is one area where the prevalence of body-monitoring technologies could enforce social-sorting functions to filter out those who do not maintain their bodies responsibly and demand that they submit to greater degrees of surveillance. Just like automotive vehicles, so the logic goes, bodies require insurance too. As one medical doctor and "innovation chief" of a company similar to BodyMedia has stated: "These devices will determine the pricing models of the future. Fat people will pay more, so they'll be incentivized to wear the devices" (quoted in Murphy,

2005). Astro Teller, the CEO of BodyMedia, imagines a world where "access to the best care goes to people who did what they could to avoid becoming ill" (quoted in Murphy, 2005).

Body-monitoring products are an example of potential somatic surveillance in that they transform human bodies into "physiological data" or emitters of "lifestyle information," which in turn allows bodies to be conceptualized as nodes within larger, interconnected sociotechnical infrastructures, susceptible to control prompts. With the goals of pervasive systems, individual compliance, and social-sorting functions, these companies and their technologies threaten to extend and intensify somatic-surveillance capabilities well beyond the domains of hospitals, medical clinics, research labs, and fitness gyms. Human bodies are perceived as resources to be mined for previously untapped but nonetheless valuable data. As the CEO of BodyMedia states: "Your body is spewing off millions of data points a second" and "no one else will be able to understand the signals coming off our bodies the way we do" (quoted in Murphy, 2005). Once rendered into atomized data, human bodies become much more vulnerable to social control mechanisms within larger, more intricate and robust information infrastructures. The nodal body is not merely translated into data for its own sake, but for the possibility of generating profit through control. By generating "lifestyle information," these systems are ultimately designed to prompt, inform, direct, and control individual behavior based on the analyzed data. As a manager of a fitness gym has stated, "when you actually see and measure what happens to your body, it increases your compliance" (quoted in Azzara, 2006). As mentioned in the introduction, it is this process of feedback, or turning the informatized body into a project of control that affords surveillance.

Meanwhile, serious problems of insufficient healthcare spread and intensify but will never be captured as data by these systems. In a climate of "medical neoliberalism" (Frank, 2002), only those who can and do undergo the transformation from citizen to consumer count. Additionally, the goal of these systems is not simply to maintain health but to enhance one's body through "technoluxe" procedures (Frank, 2004) so that one can achieve augmentation to be *better* than well (Elliott, 2003). The human insecurities of others are made invisible by consumerist systems of somatic surveillance and are actively reproduced by policies and rationalities that seek to punish those who cannot pick up the slack left by the state's retreat from social programs such as healthcare (Katz, 2006). Thus, not only does somatic surveillance in the form of body-monitoring systems discipline paying consumers – it also ramifies back upon those who are not paying, subtly justifying their exclusion from all but the basest form of healthcare. As is now the case in the US, such inadequate access compels some to enroll in potentially risky clinical trials in order to receive any semblance of healthcare at all (Fisher, 2005, 2007). In these ways, at least in the US, both successful and failed consumers of body-monitoring systems may encounter enhanced social control as the very category of "citizen" – as one possessing rights to social services – disappears.

RFID Implants

Radio-frequency identification (RFID) implants function through the subcutaneous embedding of small RFID chips into the arms of individuals. These chips contain unique numerical identifiers, which can be scanned by automated readers, medical staff, or others. At least in the context of

healthcare, the numbers are linked with a database of patients' records, which can be accessed through a secure, web-based interface. With the implants, patients effectively carry the 16-digit numerical "key" to their records with them at all times, and through the web-based system patients can selectively grant or deny access to all or part of their medical histories as they see fit. Aside from their management functions, these technologies are marketed as providing health safeguards for patients – such as those with epilepsy, heart disease, or mental impairment – who might be unable to communicate effectively with hospital staff about their medical histories or current complaints when they are in need of immediate treatment.

RFID implants are manufactured by VeriChip Corporation, located in Florida, and were approved for use in humans by the US Food and Drug Administration (FDA) in 2004. According to VeriChip's product literature, the devices were developed in direct response to the identification problems that emerged with the terrorist attacks of 9/11:

> The roots of VeriChip trace back to the events of September 11, 2001 when New York firemen were writing their badge ID numbers on their chests in case they were found injured or unconscious. It was evident there was a desperate need for personal information in emergency situations and that an injectable RFID microchip could help patients.
>
> (VeriChip Corporation, 2007)

With such discourse, national security and health concerns are effectively intertwined to create a certain imperative for the systems that VeriChip produces.

Presently, two hospitals in the US are actively implanting RFIDs into patients who consent and pay to be a part of the system, and as of June 2006 about 100 people had been "chipped" for medical purposes (Foster, 2006). The system is provocative on many levels: (1) it transfers most management responsibilities and ownership of medical records to VeriChip Corporation; (2) if implemented on a wide scale, it can effectively allow for the easy portability of medical records from site to site; (3) it relies on Internet interfaces to access and manipulate patients' records, which are technically located in a central location; (4) it raises a number of ethical concerns about security, privacy, and autonomy, because patients must consent to being chipped and must trust that their personal information will remain secure – whether from surreptitious or unauthorized scanning of their implanted chips, from compromises to the security of the web-based system, or from some other source. At this point, little research exists on the efficacy of RFID implants for improving patient care, the organizational arrangements necessary to support their use, or the ethical issues that may arise from their use.

RFID implants have already distinguished themselves as being multi-purpose and highly controversial. Aside from their uses in medical settings, in 2004 the Mexico Attorney General's Office implanted workers to regulate access to secure areas (Associated Press, 2006). Over 1,000 Mexican citizens have been chipped in efforts to facilitate finding children and others who might, at some point, be kidnapped – even though RFID implants are "passive" technologies and have extremely limited ranges, unlike global positioning systems (McHugh, 2004). A US security company, CityWatcher.com, has also required the chipping of employees wishing

special clearance to work on high-level, secure projects (Associated Press, 2006; Libbenga, 2006). A subsequent media firestorm over this case sparked state legislation currently in Wisconsin, but being considered elsewhere, prohibiting the involuntary chipping of anyone (Songini, 2006). This of course does not directly address the coercion associated with companies demanding RFID implants as a necessary condition for work. CityWatcher.com, subsequently clarified its position, stipulating that no employees will be fired for not being implanted, but employees may not be able to work on the best – and presumably higher-paying – projects if they do not agree to be chipped. Finally, RFID implants have also gained notoriety for their use by the Baja Beach Club in Barcelona, where implanted patrons can carry their credit card information around in their arms, obviating the need for purses, wallets, or much clothing (McHugh, 2004). If customers desire a drink, all they need to do is have their arms scanned for payment. In some senses, the human embodiment of capitalism that theorists have traditionally spoken about metaphorically has now become quite literal.

Perhaps the most intriguing dimensions of RFID implants are the cultural meanings attributed to them. With these technologies, one dominant history of the future is constructed by cautionary religious discourses reverberating with dire overtones. Most notably, some fundamentalist Christians in the US have singled out these technologies as signifying the "mark of the beast," as foretold in the Book of Revelation in the Bible (Albrecht and McIntyre, 2006). The mark of the beast is a number that individuals voluntarily take upon their bodies, thereby forging a pact with the anti-Christ, allowing them to continue living on Earth but ultimately dooming them to eternal damnation in hell. While a primary worry expressed by people of this belief is that of unwittingly accepting "the mark," the very existence of RFID implants in the first place is cause for grave concern, because in their view, this technology may be a harbinger of the apocalypse.

Discourses about the mark of the beast are thoroughly imbricated with other "end of days" omens and fear-inspiring prophecies, which are amazingly profitable ventures. There are television shows, movies, games, touring sermons, and best-selling book series directed at Christian audiences about the apocalypse. There is even a book series for children so that they can learn about how all their non-Christian friends will be "left behind" when the rapture occurs. To give a sense of the flavor of these media, take the following example. A glossy color brochure sent to one of the author's houses advertised a series of sermons that would be televised live from a theater in Phoenix, Arizona. The brochure asked "Has the Future Arrived?" and informed readers of upcoming sermons to learn about "The Four Horsemen," "The Mark of the Beast," and "The Last Night on Earth," among other topics. The agenda for these televised events was made quite clear: "The Bible predicts cataclysmic signs we can't ignore. Are they coming to pass right now? ... With trouble brewing in the Middle East many people are wondering, 'Are we on the verge of Armageddon?'" Because entrepreneurial, capitalistic ventures are the privileged mode of mark-of-the-beast fervor, it may be more appropriate to call it "marketing the beast" (Monahan, 2006b). Nonetheless, as a cultural phenomenon, opposition on religious grounds to technologies such as RFID implants is highly influential and is perhaps much more of an impetus than privacy concerns for US legislation proscribing mandatory implants in employees, immigrants, or others.

To begin to address the surveillance potentials of RFID implants, it helps to look at other contexts where RFID technologies are presently being used. Many hospitals, for example, are implementing RFID systems to track inventory, patients, and personnel, with the goals of improving "workflow management" and reducing medical errors. One notable outcome is the shifting of power relations so that nursing staff have less control over their workplaces and are subject to increased scrutiny by management (Fisher, 2006). Hospitals that safeguard nurses' privacy (or provide them with the ability to turn off their RFID badges during breaks, etc.) seem to be much more successful, and their systems less subject to sabotage (Fisher, 2006). RFIDs have also been used to track merchandise in large-chain stores such as Wal-Mart and Tesco. These schemes have attracted a great deal of opposition from people concerned that items embedded with RFIDs will eventually allow for the continual tracking of individuals once they leave the store or when they return to it (Cameron, 2004). Boycott campaigns have even sprung up around certain companies that have embraced RFIDs. One campaign against the razor-blade manufacturer Gillette proclaims: "I would rather grow a beard."[6] Opposition notwithstanding, concerns about surveillance made possible by pervasive RFID systems and tags do not seem to have slowed the production of them.

Several key vulnerabilities in RFID systems have already emerged. A 2006 computer science study documented the susceptibility of individual RFID tags to computer viruses, which can be spread through radio waves (Knight, 2006). Thus, systems for the management of luggage at airports, for example, could be completely incapacitated just by introducing one infected tag, which could then infect all the other luggage that came within range of it, and those tags would infect any other tags that came in range of them (whether on luggage tags or embedded in one's arm). Therefore, the vulnerabilities of these systems to hacking or information warfare are severe, especially if institutions become dependent upon their functionality. On the topic of RFID implants specifically, the chief information officer at Harvard Medical School, John D. Halamka, identifies additional problems and inconveniences with implants. He has received an implant for what he says are personal safety reasons but are more likely connected to promotional interests, because his hospital is one of the two in the US that implants RFIDs in humans. According to an in-depth story on Halamka in the *Chronicle of Higher Education*:

> Dr. Halamka says he knew before getting the chip that it came with some risks. He could develop an infection or experience pain if his body rejected the implant – neither of which happened. And he had read about how the chip could compromise his privacy. But it wasn't until the device was inside him, he says, that he realized how easily it can set off security alarms or be susceptible to identity theft.
>
> (Foster, 2006: A32)

As with other RFIDs, in their current form the chips hold too little data for effective encryption or other data protection measures (Cameron, 2006). They can easily be read, rewritten, or destroyed by anyone with the technical means.[7] Indeed, identity theft is already occurring with

[6] http://www.boycottgillette.com/ [Accessed June 18, 2006]

[7] RFIDs are especially susceptible, so it seems, to counter-surveillance disruption, such as homemade "RFID-

RFIDs used to access buildings or other secure areas or systems: just by walking near a person with a "skimmer," RFID data on a card can be read and then written to another card, allowing for the relatively easy compromising of security (Newitz, 2006).

RFID implants represent a crude type of somatic surveillance, but one with amazing potential for growth. Presently, they do not measure body functions, but augmentations are already in the works for them to detect body temperature, heart rate, and other vital signs and then communicate that information to computer systems outside the body. As well, RFID implants do not currently allow for modulations of body systems or human behavior, such as the release of medication or electrical impulses, but these types of complementary medical devices do exist and are already being used to treat "diseases" such as severe depression (Carey, 2005).[8] RFID implants are a form a somatic surveillance nonetheless because they situate bodies in relation to information systems that reduce personal identity or experience into data, such that bodies can be managed by means of abstract data rather than in their full human complexity. For example, if a patient's medical history and records can be obtained by scanning an embedded chip, this also has the potential to alter social relations among patients and medical staff – why listen to what a patient is saying about his or her history or current complaints when a technical system can provide information that is seen as much more objective and accurate? Obviously empirical research needs to be done to document the uses and effects of RFID systems, but the potential of these technologies to shift social relations and reconfigure institutions is already apparent.

Many times academics, the media, and politicians bemoan the fact that ethics, policy, and sociological understandings of risk lag so far behind technological developments. The case of RFID technologies demonstrates that many of the pitfalls of new technologies are already discernable in advance of their widespread implementation or future growth. Systemic vulnerability and risk of sabotage are clear threats to the systems and to any institutions that rely upon them. Risks of privacy loss and compromised security are woven into the technologies themselves, by nature of their facile interlinking with other systems and their small size. Aggravation of existing power asymmetries can be seen as a likely undesirable outcome whether between nurses and administrators, patients and hospital staff, customers and retail outlets, or citizens and the state. Somatic surveillance bubbles forth from this cauldron of sociotechnical dependencies, trajectories, and contingencies. Whether nanotechnology, body media, or RFID implants, there is ample advance knowledge to mitigate negative social outcomes should we so desire.

Conclusion

Zappers," which can be constructed by modifying cheap disposable cameras so that they emit an electromagnetic field (similar to an EMP) that permanently destroys proximate RFID tags without damaging the products within which tags are embedded (22C3, 2006). We understand "counter-surveillance" to mean "intentional, tactical uses or disruptions of surveillance technologies to challenge institutional power asymmetries" (Monahan, 2006a). Thus, RFID-Zappers lend themselves to counter-surveillance practices to the extent that they destabilize networks of pervasive surveillance that lie outside the control of most people.

[8] http://www.vagusnervestimulation.com/ [Accessed June 18, 2006]

Somatic surveillance is characterized by a triple movement: micro-monitoring the body with increasingly invasive technologies, recasting bodies as nodes on vast information networks, and intervening back upon bodies through automated responses or network commands. Body information or identification is translated into data by means of somatic devices. Whereas the current orientation of soldier nanotechnology and commercial body sensors is toward the generation of information and the orientation of RFID implants is toward the unique identification of bodies, it is improbable that these distinctions will hold for long. Detailed information about body systems can easily serve as biometric identifiers, on one hand, and RFID implants will soon yield personal information about vital signs, on the other.

The networks within which bodies become nodes are valenced toward objectifying and extracting value from individuals while stripping away social context. Network-centric warfare perceives bodies as discrete, autonomous entities that can be controlled remotely for strategic ends. Military use of nanosensors is rationalized as serving a dual use of helping the military to function more efficiently in the near future and eventually trickling down to benefit society in civil arenas. In non-military realms, networks for body data become products unto themselves that afford certain services for those who are willing and able to pay, whether in the form of customizable reports by BodyMedia or assurances of accurate identification and treatment through VeriChip's system for medical information. Both of these systems charge users on an ongoing basis for their services. Social context is strangely invisible yet – at the same time – individualized data are rich within these systems. This is one way that the systems support neoliberal forms of governance, because social problems are simply not represented, so they cease to exist as phenomena that society is responsible for addressing. At the same time, responsibility for healthcare falls upon the shoulders of individuals, which is a responsibility that can be met especially through the purchase of devices or services, and if something goes wrong, individuals have only themselves to blame.

Finally, somatic surveillance controls individuals. Control can occur through the modulation of body functions and capabilities or through individualized self-monitoring and behavior modification, or both. Nanotechnology systems under development by the military may allow for remote intervention into bodies on the battlefield or for automated, localized responses to body conditions (e.g., the need for medication or splints for broken bones). The network-centric warfare paradigm also encourages soldiers to internalize their role as nodes on a larger network, serving ends greater than themselves. While this message may not be a new one, the technologies and techniques for enforcing it are. In other domains, body sensors for commercial use are true technologies of the self (Foucault, 1988). They encourage the active monitoring and regulation of the body, but – perhaps more importantly – they cultivate *value* in the ongoing self-maintenance of individuals as discrete social units. RFID implants operate similarly. On a network level, they seem to be much more progressive, providing individuals with greater degrees of control over who has access to their medical records and to what extent. In the hospital context, however, the risk is that patients will be further disempowered because their voices will be seen as communicating less reliably and objectively than their implanted chips. More important, from a political and economic perspective, somatic surveillance in the commercial sector neatly transfers responsibility to individuals for contending with social needs. As Cindi Katz (2006) has noted about the child-protection industry in the US, when the

responsibility for social reproduction is removed from the domain of the state, commercially profitable and hyper-individualized alternatives dominate while most people live in increasingly unstable conditions (without adequate healthcare, childcare, education, etc.). Somatic surveillance, in its present and projected incarnations, rationalizes such a re-scripting of citizens as consumers or as militarized nodes, the result of which is a corresponding increase in mechanisms of social control, sorting, and exclusion.

References

22C3. (2006) *RFID-Zapper(EN)* [Website - Wiki]. 22nd Chaos Communication Congress 2006 [cited June 18 2006]. Available from http://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN)

Albrecht, K., and L. McIntyre. (2006) *The Spychips Threat: Why Christians Should Resist RFID and Electronic Surveillance*. Nashville, Tenn.: Nelson Current.

Appadurai, A. (1996) *Modernity at Large: Cultural Dimensions of Globalization*. Minneapolis, Minn.: University of Minnesota Press.

Associated Press. (2006) ID Chips not Just for Pets Any More. *CNN.com*, February 13.

Azzara, N. (2006) Gadgets Give Boost to Fitness Routine. *Bradenton Herald*, March 9, 9E.

Ball, K. (2005) Organization, Surveillance and the Body: Towards a Politics of Resistance. *Organization* 12 (1):89-108.

Bourdieu, P. (1998) The Essence of Neoliberalism. *Le Monde Diplomatique* December. Available from http://mondediplo.com/1998/12/08bourdieu

Cameron, H. (2004) CCTV and (In)dividuation. *Surveillance & Society* 2 (2/3):136-144. Available from http://www.surveillance-and-society.org/articles2(2)/individuation.pdf

Cameron, H. (2006) Where's My Bus?: Surveillance Technology in Urban Transit in Canada and the UK. Paper read at Crime, Justice and Surveillance, April 5-6, at Sheffield, UK.

Carey, B. (2005) F.D.A. Considers Implant Device for Depression. *New York Times*, May 21.

Department of Defense. (2005) The Implementation of Network-Centric Warfare. Washington, DC: Department of Defense: Office of Force Transformation. Available from http://www.oft.osd.mil/library/library_files/document_387_NCW_Book_LowRes.pdf

Elliott, C. (2003) *Better than Well: American Medicine Meets the American Dream*. New York: W.W. Norton.

Featherstone, M. (1991) The Body in Consumer Culture. In M. Featherstone, M. Hepworth and B. S. Turner (eds.) *The Body: Social Process and Cultural Theory*. London: Sage, 170-196.

Fisher, J. A. (2005) Pharmaceutical Paternalism and the Privatization of Clinical Trials. Doctoral Dissertation, Science and Technology Studies, Rensselaer Polytechnic Institute, Troy, NY.

Fisher, J. A. (2006) Indoor Positioning and Digital Management: Emerging Surveillance Regimes in Hospitals. In T. Monahan (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge, 77-88.

Fisher, J. A. (2007) "Ready-to-Recruit" or "Ready-to-Consent" Populations?: Informed Consent and the Limits of Subject Autonomy." *Qualitative Inquiry* 13 (8): forthcoming.

FitSense. (2006) *FitSense Technology, Inc.* [website] 2006 [cited June 28 2006]. Available from http://www.fitsense.com/

Fortun, M., and H. J. Bernstein. (1998) *Muddling Through: Pursuing Science and Truths in the 21st Century*. Washington, DC: Counterpoint.

Foster, A. L. (2006) The Bionic CIO. *Chronicle of Higher Education* LII (41):A30-A31.

Foucault, M. (1988) Technologies of the Self. In L. H. Martin, H. Gutman and P. H. Hutton (eds.) *Technologies of the Self: A Seminar with Michel Foucault*. Amherst: University of Massachusetts Press, 16-49.

Frank, A. W. (2002) What's Wrong with Medical Consumerism? In S. Henderson and A. Petersen (eds.) *Consuming Health: The Commodification of Health Care*. New York: Routledge, 13-30.

Frank, A. W. (2004) Emily's Scars: Surgical Shapings, Technoluxe, and Bioethics. *Hasting Center Report* 34 (2):18-29.

Franklin, H. B. (1988) *War Stars: The Superweapon and the American Imagination.* New York: Oxford University Press.

Graham, S., and D. Wood. (2003) Digitizing Surveillance: Categorization, Space, Inequality. *Critical Social Policy* 23 (2):227–248.

Haggerty, K. D., and R. V. Ericson. (2000) The Surveillant Assemblage. *British Journal of Sociology* 51 (4):605-622.

Haraway, D. J. (1997) *Modest_Witness@Second_Millennium.FemaleMan_Meets_OncoMouse: Feminism and Technoscience*. New York: Routledge.

ISN (Institute for Soldier Nanotechnologies). (2006) *MIT Institute for Soldier Nanotechnologies* [website] 2006 [cited June 28 2006]. Available from http://web.mit.edu/isn/index.html

Jenkins, D. (2002) *The Final Frontier: America, Science, and Terror.* New York: Verso.

Jeremiah, D. E. (1995) Nanotechnology and Global Security. Paper read at Fourth Foresight Conference on Molecular Nanotechnology, November 9-11, at Palo Alto, CA. Available from http://www.zyvex.com/nanotech/nano4/jeremiahPaper.html

Katz, C. (2006) The State Goes Home: Local Hypervigilance of Children and the Global Retreat from Social Reproduction. In T. Monahan (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge, 27-36.

Knight, W. (2006) RFID Worm Created in the Lab. *New Scientist*, March 15. Available from http://www.newscientist.com/article/dn8854-rfid-worm-created-in-the-lab.html

Lakoff, A. (2006) Techniques of Preparedness. In T. Monahan (ed.) *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge, 265-273.

Leslie, S. W. (1993) *The Cold War and American Science: The Military-Industrial-Academic Complex at MIT and Stanford*. New York: Columbia University Press.

Libbenga, J. (2006) Video Surveillance Outfit Chips Workers. *The Register*, February 10. Available from http://www.theregister.co.uk/2006/02/10/employees_chipped/

McHugh, J. (2004) A Chip in Your Shoulder: Should I get an RFID implant? *Slate*, November 10. Available from http://www.slate.com/id/2109477/

Medical News Today. (2006) Leading Health And Technology Companies Form Alliance To Improve Personal Health Through Connected Devices. June 7. Available from http://www.medicalnewstoday.com/medicalnews.php?newsid=44649&nfid=rssfeeds

Monahan, T. (2005) Globalization, Technological Change, and Public Education. New York: Routledge.

Monahan, T. (2006a) Counter-surveillance as Political Intervention? *Social Semiotics* 16 (4): 515-534.

Monahan, T. (2006b) Marketing the Beast: Surveillance and the Apocalypse. Paper read at Society for Social Studies of Science, November 2-4, at Vancouver, BC.

Monahan, T. (2006c) Securing the Homeland: Torture, Preparedness, and the Right to Let Die. *Social Justice* 33 (1): 95-105.

Murakami Wood, D. (nd) Technology, Territory and Transgression: Towards a Geography of Pervasive Computing. Unpublished Paper.

Murakami Wood, D. and Graham, S. (2006) Permeable Boundaries in the Software-sorted Society: Surveillance and Differentiations of Mobility, in M. Sheller and J. Urry (eds.) *Mobile Technologies of the City*. New York: Routledge, 177-191.

Murphy, V. (2005) Future Teller. *Forbes*, June 6. Available from http://www.forbes.com/free_forbes/2005/0606/071.html

National Science and Technology Council (NSTC). (2006) The National Nanotechnology Initiative. Washington, DC. Available from http://www.nano.gov/NNI_07Budget.pdf.

Newitz, A. (2006) The RFID Hacking Underground. *Wired Magazine*, May. Available from http://www.wired.com/wired/archive/14.05/rfid.html

Oliver, N., and F. Flores-Mangas. (2005) HealthGear: A Real-Time Wearable System for Monitoring and Analyzing Physiological Signals. Redmond, WA: Microsoft Research. Available from ftp://ftp.research.microsoft.com/pub/tr/TR-2005-182.pdf

Poste, G. (2006) What is Nanotechnology? Paper read at Launch of Center for Nanotechnology in Society at Arizona State University (CNS-ASU), January 30, at Tempe, AZ.

Ratner, D., and M. A. Ratner. (2004) *Nanotechnology and Homeland Security: New Weapons for New Wars*. Upper Saddle River, NJ: Prentice Hall/PTR.

Rodrigues, R. (2006) The Implications of High-Rate Nanomanufacturing on Society and Personal Privacy. *Bulletin of Science, Technology & Society* 26 (1):1-8.

Sensatex. (2006) *Sensatex* [website] 2006 [cited June 28 2006]. Available from http://www.sensatex.com/

Slaughter, S., and L. L. Leslie. (1997) *Academic Capitalism: Politics, Policies, and the Entrepreneurial University*. Baltimore: Johns Hopkins University Press.

Songini, M. (2006) Wisconsin Law Bars Forced RFID Implants. *Computerworld*, June 12. Available from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=111542

Strathern, M. (2005) Robust Knowledge and Fragile Futures. In A. Ong and S. J. Collier (eds.) *Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems*. Malden, MA: Blackwell Publishing, 464-481.

Teller, A., and J. I. Stivoric. (2004) The BodyMedia Platform: Continuous Body Intelligence. Paper read at International Multimedia Conference: Proceedings of the 1st ACM workshop on Continuous archival and retrieval of personal experiences, at New York. Available from http://portal.acm.org/citation.cfm?id=1026653.1026674

Thomas, J. (2003) Little Brother's Watching You. *The Ecologist*, October 31.

Toumey, C. (2004) Narratives for Nanotech: Anticipating Public Reactions to Nanotechnology. *Techné* 8 (2):88-116.

van der Ploeg, I. (2005) *The Machine-Readable Body: Essays on Biometrics and the Informatization of the Body*. Maastricht: Shaker.

VeriChip Corporation. (2007) VeriChip Corporation: Company. [website] 2007 [cited January 21, 2007]. Available from http://www.verichipcorp.com/company.html

VivoMetrics. (2006) *VivoMetrics: Continuous Ambulatory Monitoring* [website] 2006 [cited June 28 2006]. Available from http://www.vivometrics.com/

Wolfe, J. (2003) Nanotech on the Front Lines. *Forbes*, March 19. Available from http://www.forbes.com/2003/03/19/cz_jw_0319soapbox.html