Radio Frequency Identification Technology and the Risk Society: A Preliminary Review and Critique for Justice Studies

Brian Sellers, M.S.

Department of Criminology
University of South Florida

and

Bruce A. Arrigo, Ph.D.

Department of Criminal Justice and Criminology
University of North Carolina at Charlotte

ABSTRACT

Radio Frequency Identification (RFID) technology promises to revolutionize the way in which citizens interact with society, guaranteeing heightened security and increased protection speculatively critiques the soundness of this logic, especially mindful of the risk society thesis. Relevant historical background on RFID is provided, several notable applications in the corporate and governmental sectors are delineated, and the ethical and constitutional limitations associated with the technology are explored. On this latter point, concerns for the elimination of individual privacy rights are featured, including an assessment of how the identified applications erode civil liberty and personal freedom for the sake of panoptic surveillance and corporeal discipline. The article concludes with a number of justice policy implications stemming from the overall analysis.

Radio Frequency Identification Technology and the Risk Society: A Preliminary Review and Critique for Justice Studies

"*Until they become conscious they will never rebel, and until after they have rebelled they cannot become conscious.*"

- George Orwell, *1984*

INTRODUCTION

There is little mystery behind the increased efforts to enhance surveillance technologies by governmental agencies, especially in light of recent legislation following the terrorist attacks of September 11, 2001 (DOJ, 2009, 2008; Polaine, Sambei, & Plessi, 2009). Police forces are now adopting preventative law enforcement" roles (Chang, Lu & Jen, 2008) in which federal legislation makes it possible for these authorities to benefit from broader observational capabilities (e.g., Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act [USA PATRIOT Act] and Foreign Intelligence Surveillance Act [FISA]) (NLECTC, 2005 pp. 2-5). These efforts permit collaboration with private commercial enterprises in order to obtain personal data from and eavesdrop on citizens (Bloss, 2007, p. 209). The most significant impetus for this recent shift in surveillance practices by police agencies is the perceived threat of global terrorism (e.g., Arena & Arrigo, 2006; Ball & Webster, 2003). Additionally, similar efforts by European Union (EU) member-states have sought to increase security by strengthening surveillance technologies and by gathering information on individuals and "suspect groups" (Levi & Wall, 2004, p. 199).

The most intriguing aspect of these policy shifts is the apparent apathetic response from the public at large, especially with respect to lawmaking restraints placed on individual privacy rights. Some scholars suggest that the "balancing of competing interests standard" (Bloss, 2007, p. 212) helps to explain societal willingness to sacrifice civil privacy in return for perceived increases in security from "risky groups" (Levi & Wall, 2004, p. 200). Thus, the public's perception of risk, which fuels anxiety about crime, ostensibly is at the heart of the rationale that supports the current interest-weighing formula (Bloss, 2007; Simon, 2007).

Risk society theory has relevance in discussing the ethical and constitutional (i.e., justice studies) dilemmas surrounding the implementation of new surveillance technologies. Risk society theorists argue that criminal justice is about balancing the risk of victimization against otherwise unjustifiable restrictions on liberty or other forms of rights deprivation (Beck ,1999; Giddens, 1999; Hudson, 2003),. In times of instability, this calculus of risk presents society with numerous philosophical and pragmatic quandaries that warrant examination (Arrigo & Milovanovic, 2009; O'Malley, 1998; Wall, 2008). The emerging debate surrounding the use of radio frequency identification (RFID) technology for purposes of monitoring the general public merits such a critique.

In the traditional sense, justice refers to promoting laws, policies, and practices that uphold basic human dignity and promote universal human rights (Arrigo, 1999; Williams & Arrigo, 2005). More specifically, in the pursuit of social justice, we hold the criminal accountable for wrongdoing as well as the state-sponsored systems that help to sustain the very "industry" that both, wittingly or otherwise, co-produce (Arrigo, Milovanovic, & Schehr, 2005). Concerns for liberty, fairness, equality, freedom, mutual respect, and autonomy are, among others, the focus of justice studies (e.g., Capeheart & Milovanovic, 2007). Commenting specifically on liberty, Mill (1859) argued that this is what humans desire most; however, he understood that safety of person and security of property were the necessary conditions that made it realizable. Some observers suggest that our desire here and those essential conditions that actualize it are reconcilable by invoking Rousseau's concept of the social contract (Williams & Arrigo, 2008, p. 193). In this arrangement, some liberty is relinquished to the government so that the state can guarantee protection against predatory acts by others.

The problem with the aforementioned ethical dilemma is determining how much liberty citizens should forfeit in return for security gained. The key, then, is striking an appropriate balance. Some investigators note that equality of liberty is required in order to achieve this balance (Hudson, 2003, p. 40). Prospects for maximizing liberty occur when the state defines what constitutes basic rights; this, in turn, is designed to guarantee freedoms for all. However, in the post-9/11 world, a shift has occurred wherein optimal freedom and liberty are compromised for the sake of containing risk, given perceived and real increased societal dangers (Garland, 2001; Simon, 2007; Wall, 2008). In the realm of criminal justice, the system itself is charged with minimizing the threat of crime and delinquency through innovative means (Hudson, 2003; Presdee, 2001). Interestingly, O'Malley (1998), Beck (1999), and Hudson (2003) argue that risk-thinking has become so all-pervasive that the emphasis on security has made it difficult for people to fundamentally trust one other. In fact, fear of crime has led to the breakdown of solidarity so much that citizens are willing to surrender their liberties and freedoms in order to gain more security (Hudson, 2003, p. 44; see also, Arrigo & Milovanovic, 20009). As such, the respective meanings of security and justice have changed. The former no longer signifies the protection of one's freedoms and the guarantee against governmental intrusion and/or restriction (Hudson, 2003, p. 203). Instead, the notion of security now communicates the hyper-vigilant focus on safety of person and property from violations by potentially (risky) others. Given this signification, "justice" is synonymous with punishment following perceived perilous transgressions (Hudson, 2003, p. 203; see also, Arrigo & Milovanovic, 2009; Presdee, 2001).

This article speculatively, though critically, examines several pertinent theoretical and philosophical issues surrounding RFID technology and its application to the risk society thesis. In order to accomplish this objective, we review the technology's historical development as well as its practical evolution. This commentary includes RFID applications in the retail sales and manufacturing sector, the pharmaceutical and health care industry, the animal and human implantation markets, and the criminal justice system. These observations, although somewhat preliminary, then make it possible to discuss the ethical and constitutional limitations stemming from the proliferation of this technology. Finally, several justice policy reforms are tentatively proposed. These recommendations suggest how to make RFID instrumentation and its manifold uses more effective. Arguably, the proposed reforms hurdle the erosion of those liberties and freedoms that citizens have heretofore enjoyed. Indeed, while RFID technology makes it possible to monitor and, possibly, to productively control human behavior, implementing such practices does not necessarily advance the interests of citizen justice and/or societal accord.

RFID TECHNOLOGY: HISTORICAL DEVELOPMENTS AND PRACTICAL USES

What Is RFID?

Radio frequency identification (RFID) is the use of a combination of radio waves, transistors, transponders, microprocessors, and computerized databases to automatically identify an object, product, animal, or person (Albrecht & McIntyre, 2005; Anderson & Labay, 2006; Deal, 2004). RFID tags or chips are capable of storing information, which can be retrieved via radio waves to a reader that enables the information to be viewed from a distance (Anderson & Labay, 2006; Sangani, 2004). Each RFID contains integrated circuitry. The circuitry stores and processes data that is housed in a small silicon computer chip (usually smaller than a grain of sand), that has a unique identification number (Carlson, 2004; Troyk, 1999). In addition, each RFID has a flat, metallic microcoil that acts as an antenna. When the microcoil is coupled with the integrated circuit, this creates a transponder or tag (Carlson, 2004). Thus, the RFID tag is capable of receiving the radio wave signal from the RFID reader, directing it to the chip, and then transmitting its unique identifier with any other information it stores back to the reader (Albrecht & McIntyre, 2005; Erickson & Kelly, 2007; Troyk, 1999).

RFID technology allows data to be efficiently and effectively transmitted over small or large distances, in order to identify objects and/or retrieve stored information. Currently, two forms of tags exist: active and passive. Active RFID transponders are powered by an internal source of energy, allowing it to actively transmit its information load without relying on a reader to initialize transmission (Albrecht & McIntyre, 2005, Deal, 2004). Passive RFID tags do not contain their own power supply and must rely on a RFID reader to solicit a signal from it (Albrecht & McIntyre, 2005, Deal, 2004). Given the differences in power supply, active and passive RFID tags have different storage and transmission capabilities. Active tags are capable of storing more data and transmitting over larger distances; passive tags can only store small amounts of data and transmit over small distances (Albrecht & McIntyre, 2005, Deal, 2004). Moreover, active tags have "read and write" capability, where data can be read from the device but also written to it so that it can be stored (Albrecht & McIntyre, 2005; Deal, 2004, 24; Ohkubo, Suzuki & Kinoshita, 2005; Sparkes, 2006).

Since RFID technology utilizes electromagnetic energy (radio waves) to communicate information at a distance, it does not need the reader to have line-of-sight for it to be operated (Albrecht & McIntyre, 2006; Deal, 2004; Sangani, 2004; Troyk, 1999). Thus, unlike traditional barcodes and Universal Product Codes (UPCs), RFIDs can be read automatically from a distance (Deal, 2004; Erickson & Kelly, 2007). The unique identification number the RFID tag transmits back to the reader enables the reader to differentiate between tags (Carlson, 2004; Niederman, 2007; Sangani, 2004). The simplicity and efficiency this technology creates allows it to have numerous applications to various fields in the private and public sector.

Origins of RFID Technology

Similar to Geographical Information System (GIS) technology, RFID tags have military roots (Goodchild, 2006), including espionage (Albrecht & McIntyre, 2006; Sparkes, 2006). Soldiers in World War II (WWII) saw the relevance of implementing various new technologies into warfare. Among the new technology were early forms of RFID devices. During WWII, the British Royal Air Force was the first to utilize the concept of RFID when identifying friendly or foe (IFF) aircraft (Angell & Kietzmann, 2006; Carlson, 2004; Niederman et al, 2007). RFID transponders were embedded in the friendly aircraft, enabling ground forces to positively identify British planes from the Luftwaffe during the Battle of Britain. This technological capability greatly enhanced the strategic and tactical advantage of the Allies during their air campaigns (Carlson, 2004; Deal, 2004).

Given these military applications, it was not surprising that RFID technology quickly found its way into the intelligence community where acts of espionage were conducted. For example, in the late 1920s, a Russian physicist, Leon Theremin, used antenna and radio waves to make music, and his invention drew crowds of American music enthusiasts. However, little did the American intellectual elite know that Theremin was using their monetary support to improve his musical invention, the *theremin*, in order to relay U.S. military information to Russia (Albrecht & McIntyre, 2005; Anslow, 2007). Theremin's work with radio waves and the theremin represented the first known RFID devices (Albrecht & McIntyre, 2005; Sparkes, 2006).

Evidence of Theremin's work can be found in the "Great Seal Bug." In 1945, Russian school children gave the U.S. Ambassador, Averell Harriman, a carved wooden replica of the Great Seal of the United States. It was hung in the embassy, close to conference rooms where Cold War secrets were discussed. A precautionary bug sweep in 1952 found an eavesdropping surveillance device hidden in the wooden plaque, with some sort of advanced applied electronics. These "applied electronics" were nothing more than a RFID, capable of transmitting information (Albrecht & McIntyre, 2005; Anslow, 2007).

Practical Applications in Manufacturing and Retail

While the earliest forms of RFID technology were used for surveillance and as a crude form of information warfare, the technology held great potential for other useful applications in various industries. Supply Chain Management is one example. As previously mentioned, RFID tags are much more efficient then UPC barcodes; the latter rely on line-of-sight for a scan reader to detect the item code. RFID tags can be used to automate the supply chain and track products from manufacturers, warehouses, pallets, retail stores, offices, etc (Attaran, 2006; Niederman et al, 2007; Ohkubo, Suzuki & Kinoshita, 2005; Pottie, 2004).

One instance of how RFID is used in retail sales would by the system that retailer, Marks & Spencer, employs in the United Kingdom (UK) (Sangani, 2004). RFID tags are embedded into clothing labels, each with their own unique identifier (Albrecht & McIntyre, 2006; Sangani, 2004). When clothing enters a store, it is scanned by portal readers that update the stock inventory controlled by a secure computer database (Deal, 2004; Sangani, 2004). When clothes are purchased, the computer at the register shows that the items are no longer in inventory and the computer contacts the database at the corporate warehouse with updated information (Deal, 2004; Sangani, 2004). The warehouse team selects which clothing items need to be replenished at the store and has them shipped immediately (Deal, 2004; Sangani, 2004).

The use of RFID tags provides speed and efficiency in monitoring inventory management. Because the tag automatically alerts managers that supplies are low without them having to check shelves or receive customer complaints, the tag enables retailers to always have products available (Deal, 2004; Erickson & Kelly, 2007). In addition to simplifying inventory tracking, RFID automates quality control and data collecting processes by making it easier to locate products that must be recalled (Harris, 2006). The retail market merits of this technology are further illustrated through the use of loyalty cards.

Currently, millions of customers use loyalty cards to receive discounts on products purchased in their favorite retail stores. The customer information connected to such cards permits retailers to market particular items and discounts to certain patrons (Erickson & Kelly, 2007). Loyalty cards also keep track of how much shoppers spend in their stores, so retailers may reward their best consumers with continuity gifts or vouchers to encourage regular shopping. RFID tags speed up this process and help managers monitor what products individuals buy (Erickson & Kelly, 2007). For example, a woman in the UK often used a loyalty card with the retailer, Tesco, which supplies a list of favorite, frequently purchased products to its customers alerting them of relevant sales (Anslow, 2007; Smith, 2004). One day the woman found condoms listed on her favorites list, but she was puzzled because she and her husband did not use them. However, Tesco had data showing multiple purchases of condoms over a period of time. The Tesco Corporation knew that the customer's husband was cheating on her before she did (Smith, 2004).

<u>Practical Applications in the Pharmaceutical Industry and Health Care System</u>

The Food and Drug Administration has urged the pharmaceutical industry to tag medicines with RFIDs by 2007, in order to help authenticate FDA approved drugs at pharmacies and deter drug counterfeiting ("Tagging Toothpaste and Toddlers," 2004). Controlled substances that are highly targeted for counterfeiting, such as Viagra, will most likely carry RFID tags. The tags will give each prescription package a unique electronic product code (EPC) to track and trace its movement through the supply chain (Erickson & Kelly, 2007; "Tracking the Little Blue Pill," 2006). The RFID tags will help the FDA collect data to increase regulatory controls and reduce drug theft and counterfeiting. Moreover, the RFID technology will likely aid FDA officials in quickly identifying, quarantining, and reporting suspected counterfeit drug use, significantly increasing efficiency in product recalls (Young, 2004).

Given the RFID trend in the pharmaceutical industry, the technology's application in the health care delivery system seems equally plausible and useful. The tag technology offers a beneficial way to monitor patients, ensures that they receive proper care, and regulates quality in pharmaceutical drugs administered in hospitals, clinics, and other community-based facilities (Hanson, 2009). Government-backed agencies, including the FDA, will likely continue to advocate for the dissemination of the technology in these health care settings, making the monitoring and data collection of controlled substances more consumer-efficient and cost-effective.

Additionally, RFID tags are very useful to nurses and physicians who work in chaotic emergency rooms and clinics. RFID tags can be placed in wristbands to identify patients; update patient status; match blood samples; and manage or track medical devices, such as operating tools or wheelchairs (Albrecht & McIntyre, 2006, p. 159; Attaran, 2006; Erickson & Kelly, 2007). Recently, an infant abduction was prevented at Presbyterian Hospital in Charlotte, N.C., because the hospital had implemented VeriChip's Hugs Infant Protection System. The hospital used RFID tags on wristbands to monitor babies and to detect the unauthorized removal of them ("RFID Saves Baby," 2005).

Practical Applications in Animal and Human Implantation

Commercialized animal tagging first occurred in the 1980s by Amtech Corporation. The company used injectable tags encapsulated in a minuscule glass tube (Niederman et al, 2007; Troyk, 1999). In 2003, these RFID tags monitored and tracked roughly 100 million pets and 20 million livestock worldwide (Angell & Kietzmann, 2006). The glass capsule protects the active RFID tag that uses analog and digital hybrid circuitry so that memory can be stored and a microcoil can act as a transponder (Troyk, 1999). Thus, similar to manufactured products, livestock farmers can use RFID tags to monitor their stock from birth to slaughter, while keeping track of animals that go astray. Similarly, in order to locate and reunite lost household pets with their owners, tags are now employed (Erickson & Kelly, 2007, p.108). Additionally, environmental and ecological groups use RFID technology when tagging endangered species or animal populations threatened by urban sprawl, thereby tracking changes in their overall numbers (Attaran, 2006; Troyk, 1999).

The application of RFID technology to humans is also readily apparent, especially given VeriChip Corporation’s perfection of an implantable RFID tag for such use (Anderson & Labay, 2006; “Human ‘Chipping’ Takes Off,” 2003; Troyk, 1999). The VeriChiptag tag is the size of a grain of rice and is usually inserted into the triceps of the right arm just under the skin (Anderson & Labay, 2006; “Human ‘Chipping’ Takes Off,” 2003; Troyk, 1999). Comparable to the technology used for consumer products, VeriChip transmits a unique personal verification number to identify the individual with the RFID tag (Anderson & Labay, 2006; “Human ‘Chipping’ Takes Off,” 2003; Troyk, 1999). The RFID implant can store all sorts of useful information, such as medical records, financial information, citizenship, and even current location (Albrecht & McIntyre, 2006; Anderson & Labay, 2006; Deal, 2004). This technology has the potential to revolutionize human surveillance.

Since financial data can be stored and retrieved from the human RFID implants, it is quite possible to use the technology to replace paper currency

(Angell & Kietzmann, 2006). The Exxon-Mobil Speedpass was developed with this notion in mind. Specifically, RFID tags are located in personal key chains that are flashed at the gas pump. The system authenticates the ID code and looks up the customer's credit card number in the database and then processes the transaction automatically (Deal, 2004, p. 25). A similar "EZ-Pass" can be used at toll booths throughout America without having to slowdown and search for cash (Bono, Rubin, Stubblefield, & Green, 2006). Currently, credit card companies, such as American Express, Visa, and MasterCard have used RFID tags. This allows for "ez-pay" similar to the Speedpass, making the activity of card swiping obsolete (Albrecht & McIntyre, 2005). The credit cards are embedded with the RFID and automatically look up transaction information in the database after the personal ID code is authenticated; thus, a digital transaction record is made and product returns and exchanges occur without paper receipts (Albrecht & McIntyre, 2006; Deal, 2004).

Building on this particular application, RFID technology as human implants is used to automate purchase transactions without the use of money, checks, or credit cards. For example, nightclubs in Rotterdam, Edinburgh, and Miami Beach implant volunteer patrons with RFID tags (Goodchild, 2006). This technology enables customers to pay for drinks and alerts the staff of the user's club membership without having to worry about credit cards, cash, or identification (Albrecht & McIntyre, 2006). Not surprisingly, human implantation of RFID tags pose numerous ethical concerns centered principally on privacy and liberty (Angell & Kietzmann, 2006; Nisbet, 2004; Ohkubo, Suzuki & Kinoshita, 2005; Pottie, 2004; Smith, 2006; Stajano, 2005). The moral complexities behind the use of RFID human implants becomes most acute when speculation mounts that this form of tagging may become mandatory to either assign citizenship or replace currency (Albrecht & McIntyre, 2006; Foster, 2005). .

Practical Applications in Criminal Justice

The potential applications of RFID technology for criminal justice systems use are abundant, accessible, and immediate. Several such eventualities and possibilities are described below. Perhaps what is most troubling about the ensuing observations is just how problematic the liberty/security tension is rendered, particularly when risk avoidance (heightened security by way of RFID surveillance) co-opts justice (understood as ethics-making and rights-claiming) transforming it into nothing more than proliferating expressions of punishment.

If a thief steals an item that contains an RFID tag, then it would be easy for police officers to track or trace the stolen item using RFID readers (Albrecht & McIntyre, 2006, p. 127), assuming the criminal had not already destroyed or removed the tag. Moreover, RFID tags could be placed in engine castings of automobiles to help officers track stolen vehicles (Attaran, 2006). In this instance, law enforcement personnel would need the proper technology to track the stolen merchandise using RFID readers. Presently, police science lags behind private industry in cultivating these capabilities (Foster, 2005). Still further, retail sales loss prevention managers could rely on RFID instrumentation to determine if an item a customer returned for a refund was stolen or properly purchased. Along these lines, the RFID tag can hold store warranty and ownership rights information (Angell & Kietzmann, 2006). If the customer used a credit card with a RFID chip for contactless payment, then the transaction could be retrieved digitally, ensuring lawful use.

Additional potential law enforcement applications of RFID technology are worth noting. What if the U.S. Mint decided to embed RFID tags in currency notes (Albrecht & McIntyre, 2006)? Cash registers equipped with RFID readers could flag counterfeit currency, thereby reducing the work of the Secret Service (Angell & Kietzmann, 2006). Admittedly, counterfeiters would likely become more innovative in their criminality by implanting their own RFID tags; however, encryption of unique identification codes could eliminate this option altogether. Japan has already tagged 10,000 yen bills, and the European Union and Swedish National Bank have also considered something similar (Angell & Kietzmann, 2006). Currently, the price of RFID tags range between ten cents to fifty cents, depending on whether it is passive or active (Deal, 2004). However, as the technology improves the cost may soon decrease, making the RFID tags more affordable for such endeavors.

While RFID tags present novel possibilities for law enforcement to track stolen goods, human RFID implants offer still more intriguing prospects. Presently, RFID technology is used by authorities to electronically monitoring offenders on parole or probation. Ex-incarcerates are fitted with an anklet that contains RFID transponders, alerting officers when an individual has gone out of range of the receiver (Mair, 2006; Padgett et al., 2006; Nellis, 2006). Use of RFID tags linked to a Global Positioning System (GPS) could allow law enforcement to track and even pinpoint the location of probation/parole violators (Deal, 2004; Mair, 2006). Interestingly, an application of this more integrative technology was recently proposed, challenged, and halted in Orlando, Florida.

Orlando law enforcement authorities wanted to conduct a pilot test of a RFID system combined with GPS technology that would track the whereabouts of officers for safety purposes. The proposal was met with resistance by the police union. The union asserted that such a program was too intrusive and the project was eventually shutdown (NLECTC, 2005, p.3). Clearly, the action taken by the unionized officers to prevent the continuous monitoring of units in the field suggestively foreshadows future litigation from private citizens, especially if RFID and GPS systems are promoted for the monitoring of civilians.

Human implantation of RFID chips would only increase the capabilities of law enforcement to observe and inspect citizens considered a threat to public safety. Known child molesters could be chipped with RFID technology enabling the police to know if and when a convicted pedophile was lurking near playgrounds or schools (Anderson & Labay, 2006). Indeed, tagging could revolutionize how sex offender registries were managed altogether. Sex offenders could be continuously monitored in order to ensure that unsuspecting targets were not (re)harmed. Still further, human implants could allow police to locate missing persons, kidnap victims, runaway youth, abducted babies or children, etc (Anderson & Labay, 2006; "RFID Saves Baby," 2005).

Then, too, correctional facilities could use RFID implants to heighten surveillance of criminal populations and even collect data on their recidivism. In fact, correctional facilities in California, Michigan, Illinois, and Ohio already use a RFID tracking system. This tracking system includes "a tamper-detecting wristwatch-sized transmitter for inmates, a belt-mounted transmitter worn by officers, a strategically placed array of receiving antennae, a computer system, and proprietary application software" (NLECTC, 2005, p. 2). The transmitters worn by both officers and inmates send out radio signals every 2 seconds, allowing the location of individuals to be pinpointed in real time (NLECTC, 2005, p. 2).

Soon passports will be embedded with RFID tags making it possible for Homeland Security to monitor and track those persons walking through airports that are or are not United States citizens (Albrecht & McIntyre, 2006, p. 132-133; Attaran, 2006). Of course, other national governments or terrorist organizations could use RFID passports to single out American citizens as well (Albrecht & McIntyre, 2006, p. 132-133; Attaran, 2006). A human implant could make this process more efficient for security personnel at various travel venues. In fact, RFID implants could be used by Immigration and Naturalization Service (INS) agents to control the transnational flow of people into the U.S. (Angell & Kietzmann, 2006). National borders could also be equipped with readers in a fashion that might reduce the entrance of illegal aliens. Consistent with this thinking, former U.S. Secretary of Health and Human Services, Tommy Thompson – a board member of VeriChip Corporation – publicly announced that Americans should get chipped with their medical records stored on the RFID (Anderson & Labay, 2006, p. 268). This technology would enable emergency medical responders to locate citizens if a terrorist attack occurred (Albrecht & McIntyre, 2006).

The potential and eventual applications of RFID technology for purposes of criminal justice systems use also have relevance for crime-related activities. Five strategies that neutralize the effectiveness or efficiency of this instrumentation have been noted in the literature. The first method is “sniffing” in which an offender steals personal information from an RFID tag used in identity theft or fraud (Angell & Kietzmann, 2006; Sparkes, 2006). Sniffing is possible if a criminal uses a RFID reader within reading distance of a potential victim. The second method is “spoofing” in which an attempt is made by criminals to clone the RFID tag by copying its information onto a different chip so that it can be used for a variety of crimes (Bono et al, 2006; Neumann & Weinstein, 2006; Sparkes, 2006). One example of spoofing is cloning the RFID code off of an entry swipe card and then using the code in the commission of a theft. The third method that compromises the technology is “tracking.” Similar to law enforcement personnel who use RFID instrumentation to track offenders or ex-incarcerates, criminals could use the technology to plan attacks on or otherwise stalk unsuspecting citizens. The fourth method is “service denial.” By utilizing signal jammers, criminals could disrupt communication between RFID tags and readers. Among other things, this application would prohibit employees from entering their respective workplaces, would prevent shoppers from purchasing items, and would deny auto owners access to their cars (Sparkes, 2006). The final neutralization strategy is the creation of a computer-generated virus. It is possible to infect an RFID and crash an entire control system, or use a virus to wipe the information from RFID tags entirely (Sparkes, 2006). Similarly, a “cracker” could illegally access a centralized database that stores RFID data, such as credit card information, and plant a virus that would then wipe the data clean.

RFID TECHNOLOGY AND JUSTICE STUDIES: A SPECULATIVE CRITIQUE

The issue of surveillance is not an uncommon topic in the discourse on penology and social control (Arrigo & Milovanovic, 2009; Garland, 2001). In fact, the almost limitless monitoring capabilities of RFID technology closely reflect the goals of Jeremy Bentham's proposed panopticon prison (Angell & Kietzmann, 2006). For example, its initial purpose was to grow efficiency in observing inmates, while maximizing the utility of the criminally confined as a potential workforce (Rusche & Kirchheimer, 1968). Moreover, the panopticon systematically stripped prisoners of all privacy (Semple, 1993, p. 144). Under these continuous screening conditions, incarcerates were veiled without knowledge of when they were observed. Conversely, the correctional facility's "governor" and guards were given unrestricted inspection capabilities (*Ibid*., p. 140). Arguably, the function of RFID tags is similar to that of the panoptiocn. Specifically, the intention behind the manifold tagging applications is to bolster surveillance efficiency in both the private and public sectors. Additionally, RFID technology grants private industries and governmental agencies an unprecedented (and seemingly limitless) capacity to intrude upon the privacy of individual citizens without their requisite knowledge of such encroachments (Erickson & Kelly, 2007).

Bentham (1995) ethically justified the panopticon’s use, arguing that it “would enforce social conformity, coercing self-regarding men to consider the interests of others” (Semple, 1993, p. 140). Consistent with this utilitarian rationale, Bentham believed that the panopticon would enable prisoners to realize that it was in their best interests to ensure the good behavior of fellow inmates (*Ibid*. p. 141). Thus, security through the panopticon was achieved once individuals relegated their own needs as second to those of the majority. Foucault (1977) maintained that the panopticon actually manipulated its subjects to the point that they were persuaded to become the agents of their own subjugation; thus, the panopticon established a surreptitious authority to control, inspect, and discipline (Garland, 2001).

Foucault (1977; see also, Mathiesen, 1997) also recognized that one principal aim of the panopticon was that it allowed a single guard to observe several prisoners while remaining completely unseen. This omnipresent type of surveillance (“invisible omniscience”) is consistent with the asymmetrical power that RFID technology would make possible for a sovereign government, especially since those implanted with a tag would not know when or by whom they were being scanned. Along these lines, consider Foucault’s (1977) cogent perspective:

“Discipline may be identified neither with an institution nor with an apparatus; it is a type of power, a modality for its exercise, comprising a whole set of instruments, techniques, procedures, levels of application, targets; it is a 'physics' or an 'anatomy' of power, a technology" (p. 215).

In other words, panopticism functions as a disciplinary mechanism that grows power for those in control, while transforming society into a culture rife for inspection. This occurs through the generalized surveillance of society by way of "subtle coercion" (Foucault, 1977, p. 209). The rhetoric promoting the human implantation of RFID has been strategically thrust upon the public, and this technology does not require institutional walls to exercise its constant monitoring. The accumulation of power that awaits those regulating this disciplinary mechanism of subjugation is seemingly endless. Indeed, as Foucault lamented when discussing the panopticon, "[It] is a marvelous machine which, whatever use one may wish to put it to, produces homogeneous effects of power" (*Ibid*., p. 202). Although RFID tags and chips do not resemble ominous penal structures, they still embody several key characteristics of panopticism where citizens become objects to discipline. Through these normalizing efforts, individual behavior is targeted for routine inspection, constraint, and alteration wherein subjects are rendered docile (Arrigo & Milovanovic, 2009). This is the *micro-physics* of power whose totalizing effects seep deep into and through the subject's body such that they discipline the corporeal soul (Mathiesen, 1997).

Interestingly, however, it is the principle of utility (Bentham & Mill, 1973; Mill, 1957) that supporters of RFID technology turn to when attempting to convince the public that safety of self and security of property are paramount, notwithstanding individual privacy and collective liberty concerns. Admittedly, technology that allows authorities to pinpoint missing persons, abducted children, escaped convicts, international terrorists, and registered sex offenders is socially desirable. Still, we question the *quality* of human social interaction that follows given society's steadfast reliance on such instrumentation. While the popular sentiment may very well become that those opposed to the promises of RFID are the very criminals for whom the technology was designed in the first place, the perils of this science cannot be readily ignored or easily dismissed. Just as Foucault (1977) warned that the panopticon's proliferating use would lead subjects to eventually manipulate and subjugate themselves, the same ominous possibility exists with the widespread dissemination and implementation of RFID technology. Indeed, the wholesale networking and interfacing of RFID instrumentation with existing surveillance technologies requires social and political conformity from the public (Pottie, 2004). This tacit consent may very well signal the genesis of abject control for one and all.

Perhaps most troubling is that in its attempt to provide greater security through this new technology, governments may be acting instrumentally to achieve their desired end. In this instance, the ultimate objective would be the elimination of risk through intensified surveillance over and control of the general public. Immanuel Kant staunchly warned against treating individuals as a means to an end, noting that such conduct violated human dignity – a dignity which he found to have the highest moral significance (Williams & Arrigo, 2008, pp. 224 & 239). If the government were to manipulate the populace into pervasive adoption of RFID technology where individuals relinquished more of their freedoms to a state power that promised greater security and safety in return, then such action would violate Kant's maxim. Indeed, following Kant, when we allow our treatment of others to fulfill desires for domination that merely serve personal (though beneficial) interests, other people are not our equals in terms of respect and freedom (Hudson, 2003, p. 12). This is why morality "cannot be a matter of fulfilling desire," and justice must constitute "something other than promoting what is generally desired or desired by a majority of people" (including punishment) (*Ibid.*, p. 13). Accordingly, we take the position that while RFID technology holds the potential for a government to accomplish its understandable interest in more control and better security, it does so unjustly.

As some scholars note, modern Western societies such as the United States of America and the United Kingdom have become so entrenched in their efforts to contain risk that traditional values regarding the universality of human rights no longer occupy a significant place in the discourse on criminal justice policy (Beck, 1999; Hudson, 2003; Wall, 2008). In fact, risk society theorists believe that "the richest, longest-lived, best-protected, most resourceful civilization, with the highest degree of insight into its own technology, is on the way to becoming the most frightened" (Wildavsky, 1979, p. 32). The fear that underscores the utilitarian logic of "sacrificing one for many" (Hudson, 2003, p. 217) also increases the prospect that individuals will be used as a means to an end. As a result, only those citizens who are in good communal standing may be guaranteed presumably universal human rights while those who are members of a suspect group will not benefit from such a guarantee. The denial of basic human rights, even to those who commit heinous crimes, creates instability within society and encourages the abandonment of solidarity to the extent that alleged or perceived wrongdoers are deemed unworthy of due process. This type of thinking leads individuals to further subjugate themselves willingly to the whims of the state or a state sanctioned system that seeks to control its citizens by constraining civil liberties and curtailing personal freedoms. Included among these liberties is the right to privacy.

Although RFID technology may, in the interests of convenience, allow more efficiency in many industries and public services, it is based on surveillance implicating privacy issues. Privacy advocates often look to the First, Fourth, and Fifth Amendments of the U.S. Constitution to locate support for such a right. In fact, the Privacy Act of 1974 clearly prevents the unauthorized disclosure of personal information held by the federal government (Rotenberg, 2007). "Moral philosophers maintain that respecting the many forms of privacy is paramount [if] respect for human dignity and personhood, moral autonomy, [and] a workable community life" are to follow (Allen, 2003, p. 491-492; Anderson & Labay, 2006). Therefore, many citizens believe that privacy is an implied right lodged in the Constitution that should not be abridged by lawful intrusion, regardless of any potential gains.

Notwithstanding this perspective, the U.S. Ninth Court of Appeals found that "the government may seek and use information covered by the right to privacy…if it can show that its use…would advance a legitimate state interest and that its actions [would be] narrowly tailored to meet [that] legitimate interest… [T]he more sensitive the information, the stronger the state's interest must be" (*Doe v. Attorney General*, 1991; also see Anderson & Labay, 2006). Following this ruling, a government may only curtail an individual's privacy if a bona fide state interest is at stake, such as public safety or national security. A similar judgment was reached in *Katz v. United States* (1967), where the government's intrusion was limited by the public's legal "expectation of privacy."

However, recent modifications to counter-terrorism policies and practices infringe upon the privacy guarantees recognized by the U.S. Supreme Court (Arena & Arrigo, 2006; Ball & Webster, 2003; Polaine, Sambei, & Plessis, 2009). As such, the utilitarian interpretation of RFID instrumentation suggests that supporters of human implantation (and other tagging applications) believe the benefits of the technology advantage society's collective interests. The calculus of an interest-balancing argument thus ensues wherein the state's security needs ostensibly outweigh individual privacy rights. We question the philosophic and pragmatic costs that attach to citizens and society in the wake of this determination.

Currently, the Patriot Act makes it possible for warrantless wiretaps and unprecedented surveillance of the public to occur (Albrecht & McIntyre, 2006; Angell & Kietzmann, 2006). In addition, the Foreign Intelligence Surveillance Act (FISA) has made it possible for the intelligence gathering community – in cooperation with telecommunication providers – to eavesdrop on citizens engaged in conversations considered important to national security (Ball & Webster, 2003; Smith, 2006). The concept of RFID human implants will only increase the government's ability to track and profile individuals based on their habits, tastes, and/or preferences. Indeed, state authorities (law enforcement agencies) could use this technology to identify potential terrorists, as much as they could employ it to monitor anyone who spoke out against the government. Regrettably, by allowing ourselves to be chipped, we surrender our locational privacy (Goodchild, 2006, p. 689). Moreover, the prohibition against "unreasonable searches and seizures" (U.S. Constitution, Amendment IV) will increasingly be disregarded if human implantation is transformed into an acceptable and customary practice. The problem here is that no one will really know if they are being scanned or if their personal information is being read. The legacy of George Orwell‛s *1984* reappears in technologically sophisticated though omnisciently invisible brilliance. “Big Brother” is everywhere digitally; our docility ensures homogenized security, our acquiescence guarantees the dissolution of the self, and our resistance renders societal justice an artifact of punishment.

IMPLICATIONS AND CONCLUSIONS

Some commentators suggest that if RFID advocates wish to grow public approval, they must ensure the implementation of comprehensive security measures, consumer education, enforcement guidelines, and empirical research in the development and implementation of chip and tag technology (Ohkubo, Suzuki & Kinoshita, 2005, p. 68). In addition, other investigators recommend the insertion of a “kill” function in RFID tags, in order to disable them after a product is purchased (Angell & Kietzmann, 2006, p. 94; Erickson & Kelly, 2007, p. 112; Ohkubo, Suzuki & Kinoshita, 2005, p. 68; Stajano, 2005, p. 32). Unfortunately, the “kill command” would have to be operated manually, increasing the likelihood of human error. However, the real obstacle with such a proposal is that the tag’s destruction is not in the RFID stakeholder’s best interest (Angell & Kietzmann, 2006, p. 94; Erickson & Kelly, 2007, p. 112; Ohkubo, Suzuki &

Kinoshita, 2005, p. 68; Stajano, 2005, p. 32). After all, the durability and rewrite capabilities of active tags hold many rewards for those with a vested interest in this instrumentation.

Recent acknowledgement of the vulnerability of the secret encryption algorithm that most RFID tags employ indicates that they can be cloned, decrypted, and used for illegal or fraudulent purposes (Albrecht & McIntyre, 2006; Bono et al, 2006; Sparkes, 2006). Presently, the U.S. Federal Communication Commission's (FCC) efforts to regulate or prevent the unauthorized use of equipment that clones or decrypts the security measures of RFID technology, includes numerous fiscal problems and bureaucratic limitations that are not easily addressed or hurdled (Bono et al, 2006). Additionally, efforts to pass legislation that would criminalize activities such as spoofing, sniffing, tracking, service denial, or virus attacks will most likely have no deterrent effect on potential criminal activity (Bono et al, 2006). Thus, RFID proponents cannot rely on legality alone to prevent the misuse of this technology; instead, they must lobby for front-end security that is built into the system (Bono et al, 2006; Sparkes, 2006).

Other researchers have suggested that governmental regulation is essential if information privacy rights are to be secured for the public (Anderson & Labay, 2006; Erickson & Kelly, 2007). For instance, restrictive policies are needed that control the data collected and that protect against its use for discrimination or profiling purposes (Anderson & Labay, 2006;

Erickson & Kelly, 2007). However, if the government is doing the regulating, then who is monitoring its own technological abuses? The answer may be that there is no way to safeguard against the state's intrusion into the public's privacy once extensive RFID implementation is adopted. Indeed, what incentive exists that could dissuade the state from fully seizing upon a scientific application that allowed it to better maintain total dominion over its citizens? The public should be extremely cautious about the promise of heightened security through increased surveillance, especially if such regulation and control does not adequately prevent unbridled governmental power and authority. Absent this public vigilance, the risk society thesis will ensure that our experience of democracy will never provide for what we need but, instead, will provide for what we deserve. In our estimation, the pursuit of justice demands far more than what panoptic surveillance warrants. To this end, infringements on privacy rights by way of RFID technology cannot guarantee safety and maximize security any more than they can grow liberty or enhance freedom. Indeed, as Benjamin Franklin poignantly noted, "Any society that would give up a little liberty to gain a little security will deserve neither and lose both." Thus, it is time to acknowledge the often hidden debate surrounding the use of RFID technology; otherwise, the very analysis and critique undertaken in this article may itself be identified as a "thought crime" (Orwell, 1949, p.19) necessitating surveillance, inspection, and disciplining.

REFERENCES

Albrecht, K. & McIntyre, L. (2005). *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID.* Nashville, TN: Nelson Current.

Anderson, A.M. & Labay, V. (2006). Ethical considerations and proposed guidelines for the use of radio frequency identification: Especially concerning its use for promoting public safety and national security. *Science and Engineering Ethics*, 12(2): 265-272.

Angell, I. & Kietzmann, J. (2006). RFID and the End of Cash? *Communications of the ACM,* 49(12): 91-96.

Anslow, M. (2007). Creepy Technology. *Ecologist*, 37(5): 16.

Arena, M. P., & Arrigo, B. A. (2006). *The terrorist identity: Explaining the terrorist threat*. New York, NY: NYU Press.

Arrigo, B. A. (Ed.) (1999). *Social justice/criminal Justice: The maturation of critical theory. In Bruce A. Arrigo (ed.). Law, Crime, and Deviance*. Belmont, CA; Wadsworth.

Arrigo, B. A., & Milovanovic, D. (2009). *Revolution in penology: Rethinking the society of captives*. Lanham, MD: Rowman & Littlefield.

Attaran, M. (2006). RFID pays Off. *Industrial Engineer,* 38(9): 46-50.

Ball, K., & Webster, F. (2003). *The Intensification of Surveillance: Crime,* *Terrorism, and Warfare in the Information Age*. London, UK: Pluto Press.

Beck, U. (1999). *World Risk Society*. Cambridge, UK: Polity Press.

Bentham, J. & Mill, J.S. (1973). *The Utilitarians*. New York: Anchor Press (Original work published 1789).

Bentham, J. (1995). Panopticon (Preface). In M. Bozovic (Ed.), *The panopticon writings* (pp. 29-95). London: Verso.

Bloss, W. (2007). Escalating U.S. Police Surveillance after 9/11: an examination of causes and effects. *Surveillance and Society*, 4(3): 208-228.

Bono, S., Rubin, A., Stubblefield, A. & Green, M. (2006). Security through legality. *Communication of the ACM*, 49(6): 41-43.

Capeheart, L., & Milovanovic, D. (2007). *Social justice: Theories, issues, and movements*. New Brunswick, NJ: Rutgers University Press.

Carlson, S. (2004). Talking tags: New high-tech labels helps libraries track books, but worry privacy advocates. *Chronicles of Higher Education,* 50(48).

Chang, W., Lu, C. & Jen, W. (2008). A Study of Integrated Criminal Justice Data Base System. *Intelligence and Security Informatics*. Retrieved February 6, 2009, from IEEE Xplore.

Deal, W.F. (2004). Resources in Technology: RFID: A Revolution in Automatic Data Recognition. *The Technology Teacher*, 63(7): 23-27.

Doe v. Attorney General, 941 F.2d 796, (9th Cir, 1991).

Erickson, G.S. & Kelly, E.P. (2007). International aspects of radio frequency identification tags: Different approaches to bridging the technology/privacy divide. *Knowledge, Technology, and Policy*, 20(2): 107-114.

Foster, R. E. (2005). *Police technology*. Upper Saddle River, NJ: Pearson Prentice Hall.

Foucault, M. (1977). *Discipline and punish: The Birth of the Prison* (A. Sheridan, Trans.). New York: Vintage Books, a Division of Random House, Inc. (Original work published 1975).

Garland, D. (2001). *The culture of control: Crime and social order in contemporary society*. Chicago: The University of Chicago Press.

Giddens, A. (1999). "Risk and responsibility." *Modern Law Review*, 62: 1-10.

Goodchild, M.F. (2006). GIScience ten years after ground truth. *Transactions in GIS,* 10(5): 687-692.

Hanson, W. (2009). *The edge of medicine: The technology that will change our lives.* New York, NY: Palgrave.

Harris, A. (2006). Frozen chips. *Computing & Control Engineering*, 17(3): 16-21.

Hudson, B. (2003). *Justice in the risk society: Challenging and re-affirming justice in late modernity*. London: Sage Publications.

"Human 'Chipping' Takes Off." (2003). *Industrial Engineer*, 35(12): 18.

Katz v. United States, 389 U.S. 347 (1967).

Levi, M. & Wall, D.S. (2004). Technologies, security, and privacy in the post-9/11 European information society. *Journal of Law and Society*, 31(2): 194-220.

Mair, G. (2006). Electronic monitoring, effectiveness, and public policy. *Criminology & Public Policy,* 5(1): 57-59.

Mathiesen, T. (1997). The viewer society: Michele Foucault's 'panopticon' revisited. *Theoretical Criminology*, 1(2): 215-234.

Mill, J.S. (1859). *On liberty*. London: J.W. Parker.

Mill, J. S. (1957). *Utilitarianism* (O. Piest, Ed.). Indianapolis: Bobbs-Merrill Educational Publishing (Original work published in 1861).

MIT Auto-ID Center. (2002). "The New Network: Identify Any Object Anywhere Automatically," promotional brochure, MIT Auto-ID Center, (Cambridge, MA).

National Law Enforcement and Corrections Technology Center. (2005). *Technology Primer: Radio Frequency Identification* (TechBeat, NLECTC Cooperative Agreement #96-MU- MU-K011 by U.S. Department of Justice). Rockville, MD: Author.

Nellis, M. (2006). Surveillance, rehabilitation, and electronic monitoring: Getting the issues clear. *Criminology & Public Policy*, 5(1): 103-108.

Neumann, P.G. & Weinstein, L. (2006). Risks of RFID. *Communications of the ACM*, 49(5):136.

Niederman, F., Mathieu, R.G., Morley, R. & Kwon, I.W. (2007). Examining RFID applications in supply chain management. *Communications of the ACM,* 50(7): 93-101.

Nisbit, N. (2004). Resisting surveillance: Identity and implantable microchips. *Leonardo,* 37(3): 210-214.

O'Malley, P. (1998). *Crime and the risk society*. UK: Ashgate.

Ohkubo, M., Suzuki, K. & Kinoshita, S. (2005). RFID privacy issues and technical challenges. *Communications of the ACM*, 48(9): 66-71.

Orwell, G. (1949). Nineteen *Eighty-Four, a novel.* New York: Harcourt, Brace.

Padgett, K.G., Bales, W.D. & Blomberg, T.G. (2006). Under surveillance: An empirical test of effectiveness and consequences of electronic monitoring. *Criminology & Public Policy*, 5(1): 61-91.

Polaine, M., Sambei, A., & Plessis, A. (2009). *Coutern=terrorism law and practice: An international handbook*. New York, NY: Oxford University Press.

Pottie, G.J. (2004). Privacy in the Global E-Village. *Communications of the ACM*, 47(2): 21-23.

Presdee, M. (2001). *Cultural criminology and the carnival of crime*. London, UK: Routledge.

"RFID Saves Baby." (2005). Industrial *Engineer,* 37(11): 12.

Rotenberg, M. (2007). Technology and Privacy. *Human Rights: Journal of* *the Section of Individual Rights & Responsibilities,* 34(1).

Rusche, G., & Kirchheimer, O. (1939/1968). *Punishment and social structure*. Totowa, NJ: Transaction Publishers.

Sangani, K. (2004). RFID Sees All. *IEE Review*, 50(4): 22-24.

Semple, J. (1993). *Bentham's Prison: A study of the panopticon penitentiary.* Oxford: Clarendon Press.

Simon, J. (2007). *Governing through crime: How the war on crime transformed American democracy and created a culture of* fear. New York, NY: Oxford University Press.

Smith, J. (2004). Every Little Helps. *The Ecologist,* 34(7): 48-54.

Smith, J.R., Fishkin, K.P., Jiang, B., Mamishev, A., Philipose, M., Rea, A.D., Roy, S., & Sundara-Rajan, K. (2005). RFID-Based Techniques for Human-Activity Detection. *Communications of the ACM*, 48(9): 39-44.

Smith, L. (2006). Warrantless wiretaps and your EZ pass. *The Humanist*, 66(2): 38-39.

Sparkes, M. (2006). Gambling on Chips. *Manufacturing Engineer,* 85(4): 10-11.

Stajano, F. (2005). RFID Is X-Ray Vision. *Communications of the ACM*, 48(9): 31-33.

"Tagging toothpaste and toddlers." (2004). *Information Management Journal,* 38(5): 22.

"Tracking the Little Blue Pill." (2006). *Industrial Engineer*, 38(3): 16.

Troyk, P.R. (1999). Injectable electronic identification, monitoring, and stimulation systems. *Annual Review of Biomedical Engineering,* 1(1): 177-209.

U.S. Department of Justice. (2008). *Solicitation: research and evaluation on justice system responses to violence against women* (Grants.gov Funding Opportunity No. 2008-NIJ- 1739, SL#000824, CFDA No.16.560). Washington, DC: U.S. Department of Justice, Office of Justice Programs.

U.S. Department of Justice. (2009). *Solicitation: Technology research and development for law enforcement and corrections application.* (Grants.gov Funding Opportunity No. NIJ-2009-2012, SL# 000862, CFDA No. 16.560). Washington, DC: U.S. Department of Justice, Office of Justice Programs.

U.S. Const. amend. IV.

Wall, D. S. (2008). *Cybercrime: The transformation of crime in the Information Age* Cambridge: Polity.

Wildavsky, A. (1979). "No risk is the highest risk of all." *American Scientist*, 67: 32.

Williams, C. R., & Arrigo, b. A. (2005). *Theory, justice, and social change: Theoretical integrations and critical applications*. New York, NY: Springer.

Williams, C.R. & Arrigo, B.A. (2008). *Ethics, crime, and criminal justice.* New Jersey: Pearson Prentice Hall.

Young, D. (2004). FDA Embraces RFID to Protect Drug Supply. *American Journal of Health-System Pharmacy,* 61(24): 2612-2613.