DJIM

Volume 5 – Spring 2009
djim.management.dal.ca

Perceptions of Privacy and the Consequences of Apathy: Biometric Technologies in the 21st Century

Abstract: Privacy, long considered one of our most valuable rights, is at risk. Younger generations are increasingly becoming de-sensitized to the disclosure of their personal and confidential information. With little or no contemplation, this information is bartered in exchange for the conveniences and luxuries that today's technologies offer. Moreover, recent developments in the field of biometrics have created unprecedented opportunities for organizations to observe, gather, and share our personal information. This paper explores the evolution of biometrics, the benefits and challenges of this technology, and the potential threat it poses to future generations.

About the Author: Suzanne van den Hoogen is a second year graduate student in the Dalhousie School of Information Management and Manager of Access Services for the Angus L. Macdonald Library at Saint Francis Xavier University. She holds a combined BA degree in English and French from Saint Mary's University. She will graduate with her MLIS degree in May 2009. This paper was originally submitted for the graduate course INFO 5500, Information in Society.

Perceptions of Privacy and the Consequences of Apathy: Biometric Technologies in the 21st Century

The Spider and the Fly

> "Will you walk into my parlour?" said the Spider to the Fly,
> "Tis the prettiest little parlour that ever you did spy;
> The way into my parlour is up a winding stair,
> And I've a many curious things to shew when you are there."
> "Oh no, no," said the little Fly, "to ask me is in vain,
> For who goes up your winding stair can ne'er come down again." (Howitt, 1829, 1)

Redefining the Information Landscape

Technology is redefining the information landscape. While it offers many opportunities, it also poses several challenges. One of these challenges is keeping up with the advent of new electronic and digital resources. A more important challenge, however, is ensuring that the policies protecting the privacy and confidentiality of citizens are evolving at the same pace as the expanding use of new technologies. The political and legislative response to the attacks on the World Trade Center in 2001 and subsequent advancements in the field of biometrics have garnered much controversy in recent years; making privacy a paramount issue of consideration for today's information managers, policy makers, and global citizens.

Developments in biometric technology have created unprecedented opportunities for organizations to observe, gather, and share information about individuals. Unfortunately, as these types of technologies grow in popularity and become part of mainstream society, less and less consideration is given to the pervasive demands they place upon individuals to submit their personal and private information. Although public awareness has grown with regard to the prolific use of these technologies, critics suggest that younger generations show little concern and are becoming increasingly desensitized to the consequences these technologies may pose to future generations (Brown, 2008; Crampton, 2007; Crews, 2003). What effects will these technologies have on our long-term personal sense of privacy? Are we methodically de-sensitizing our children to accept privacy invasion as the norm of the future? What has happened to our values? Privacy, long considered one of our most valued rights has become the currency of the future and is bartered for services on a daily basis.

The questions that ensue are: What has caused us to adopt such a cavalier attitude towards protecting our personal privacy? Are the consequences of our current decisions so far in the future that they merit little consideration today? Sir Ken Macdonald, the Director of Public

Prosecutions in Great Britain, does not think so. He warns that the penalties of adopting a "Big Brother surveillance state could lead to serious consequences and suggests that "we should take very great care to imagine the world we are creating before we build it. We might end up living with something we cannot bear" (Gibb, 2008 para. 9). Like the fly that is lured into the spider's web, there may be no turning back.

Clearly, there is an overwhelming attraction to the conveniences and personal luxuries that technology provides, all of which can be acquired in exchange for our personal information. The freedom and luxury of these conveniences, however, may cost us more than we are willing to pay. This paper will explore the evolution of biometrics; the benefits and risks associated with this developing technology, and the potential threat biometric surveillance poses to future generations.

Biometrics: An Historical Perspective

Biometrics, the measurement of unique physical and behavioural characteristics used to confirm the identity of individuals, is not a recent discovery. Julian Ashbourn contends that "contrary to popular belief, the concept of using a biometric for identity verification purposes is not new and dates back certainly to Egyptian times" (2005, p. 2). Ashbourn supports this claim by providing an example of Babylonian kings who used hand impressions in clay for identity verification purposes (2005). In comparison, the National Science and Technology Council (NSTC) provides a simpler historical perspective and suggests that one of the oldest and most widely used personal characteristics we have been using to confirm the identity of individuals is the face (National Science and Technology Council [NSTC], 2006). However, this human-to-human form of recognition "became increasingly more challenging as populations increased and as more convenient methods of travel introduced many new individuals into once-small communities" (NSTC, 2006, p .1).

Throughout history, several forms of human characteristics have been used as a means of authenticating the identity of individuals. The following examples are intended to provide a brief description and timeline of developments in biometric technologies and their usage:

Prehistoric Cave Paintings & Babylonian Clay Tablets

Familiar to many of us are the cave paintings of prehistoric civilizations. Insurmountable evidence identifying the proprietary rights of these invaluable works of art can be connected to the handprints the artists left behind (NSTC, 2006). As populations multiplied and commercial trade between civilizations increased, the need to identify individuals also grew in popularity. Historical evidence of ancient business transactions can be found in Babylonian clay tablets where fingerprints were used to confirm the identity of individuals (NSTC, 2006; O'Harrow,

2006).

Fingerprinting and 14th Century China

Travels to the Orient in the 14th century resulted in more than silk and spices being discovered. Joao de Barros, a Portuguese historian and explorer, provides accounts of Chinese merchants using fingerprints to record business transactions and identify children (NSTC, 2006; O'Harrow, 2006; Osborn, 2005).

Anthropometrics

In the later part of the 19th century, Joseph Bertillon, a French police official, is credited with developing a new method of identifying individuals. His method of identification is based on detailed anatomical records that include the measurement of physical attributes and the use of photographs. This method of identification became known as the Bertillonage method or anthropometrics; however this procedure was soon abandoned in favour of fingerprinting after it was proven to falsely identify multiple suspects (Ashbourn, 2005; NSTC, 2006; O'Harrow, 2006; Osborn, 2005).

Re-emergence of Fingerprinting

Shortly before anthropometrics were abandoned, Sir Francis Galton, a British anthropologist and cousin to Charles Darwin, developed a classification system for fingerprints based on identifying all 10 fingers. Sir Edward Henry, of Scotland Yard, contacted Galton about his classification system. In consequence, Henry, with his assistant Azizul Haque, developed the precursor to the classification system of fingerprints which is still used today (Ashbourn, 2005; NSTC, 2006; O'Harrow, 2006; Osborn, 2005).

New Technologies: 1960s - 1990s

Research into automated signature recognition began in the latter part of the 1960s (NSTC, 2006; Osborn, 2005). Biometric research continued to expand during the 1980s with significant developments involving retinal scans, hand geometry, and voice recognition technologies (Ashbourn, 2005; NSTC, 2006). Following the successes of previous biometric techniques, further research in the field of forensics and the use of DNA was undertaken in the 1990s. In 1998 the Federal Bureau of Investigation (FBI) launched a Combined DNA Index System (CODIS), a DNA forensic database used for law enforcement purposes. It was also during this decade that biometric identification was implemented on a large scale with the public. For example, hand geometry was used to control physical access to the Olympic Village at the

1996 Olympic Games in Atlanta (NSTC, 2006).

Biometrics in the early 21st Century

Biometric technologies continued to grow in popularity during this period. In 2000, West Virginia University and the FBI established a bachelor's degree in biometric systems. One year later, the bombings of the World Trade Centre prompted the use of face recognition technology to monitor individuals attending the 2001 Super Bowl in Tampa, Florida. Civil rights groups were outraged and this event later became dubbed by the media as the Snooper Bowl. Perhaps, however, the most significant development with the use of biometrics in the early part of 2000 can be attributed to George Bush who, on May 14, 2002, publicly announced the endorsement of biometrics in the US government (Crampton, 2007; NSTC, 2006; Osborn, 2005; Woodward, Orlans & Higgins, 2003).

Biometrics Today

Led by consumer demand for electronic services and the conveniences they provide, data-driven information technologies are escalating. Biometric identifiers, marketed as enhanced forms of identification verification, promise foolproof security. For example, enhanced security protocols, like fingerprint readers, have recently been added to electronic devices such as laptop computers, mobile phones, and car doors. In addition to the widespread use of biometrics in the private sector, government programs requesting the submission of biometric data are becoming increasingly prevalent. In Canada, examples of voluntary government programs that require biometric data include project NEXUS, an enhanced border pass for pre-approved travelers to the US, and the BC Enhanced Driver's License, an ID card that promises to allow BC citizens to travel across the US border without need of a passport.

Mass Production and Public Consumption

We have seen that research and development in the field of biometrics have grown significantly within the last few decades. While fingerprints have remained one of the oldest and most widely collected forms of biometric data, research in this area has made it possible to measure the nature of our gait, the dynamics of our keystrokes, and the vascular patterns of our hands. Biometric surveillance technologies have become ubiquitous. Their popularity and relative affordability has meant that they are now found in schools, airports, libraries, shopping malls, private businesses, cities, towns, and most public spaces. As the title of Robert and O'Harrow's 2006 book on privacy and the emerging use of surveillance technology suggests, there is *No Place to Hide*. Consequently, advancements in this area have garnered considerable attention and controversy. Two dominant schools of thought have emerged: one supporting the use of biometrics as an acceptable form of security and the second denouncing

the use of biometrics as both an invasion of privacy and a violation of human rights.

Both schools of thought agree that biometric technologies are becoming a standard form of authenticating personal identity in the digital age. Irma van der Ploeg (2003) observes that technology has replaced "physical and face-to-face encounters, depriving the interacting partners of traditional, trusted ways of establishing to each other who they are" (van der Ploeg, 2003, p. 86). She further suggests that, unlike physical identification cards or PINs, "biometric characteristics cannot be faked, lost or stolen" (p. 86); thus the potential for fraudulent financial transactions and identity theft is avoided. Julian Ashbourn also observes the wide scale introduction of biometrics within the public sector but cautions that to blindly accept these technologies without questioning the potential threat they pose to individual privacy and human rights would be negligent (2005). Furthermore, Ashbourn warns that "if we embark upon this journey under a cloud of deception, then that cloud will follow us for a long time" (2005, p. 9).

Despite the growing concerns surrounding these technologies and the risk they pose to personal privacy, critics suggest that most individuals are willing to exchange personal information for the services and conveniences they offer (Brown, 2008; Crews, 2003; Freeman, 2003; Jain, Hong & Pankanti, 2000). Sharing personal information with outside sources seems to have become the norm. It allows us to shop online, travel from one country to another, and do our banking from the convenience of our home. The catch, however, as Edward Freeman astutely points out, is that "there is an expectation of privacy that this information will not be used for any other purpose" (2003, p. 6).

Perceptions of Privacy: Much Ado about Nothing?

Are expectations of privacy and confidentiality a must in today's sensitive information society? Peter Brown (2008) suggests that, when it comes to privacy, expectations vary depending on age demographics. Brown points out that despite all the controversy surrounding this issue, "many young adults find all the anxieties about privacy to be much ado: many in the new generation are only too happy to trade their parents' version of 'private information' for a rich life in the fishbowl of social networking" (para. 5). "People, especially the young," according to Clyde Crews, "will likely adapt to tomorrow's cashless, keyless, wallet-less society very easily" (Crews, 2003, p. 18).

Another reason why so many individuals within this age group are willing to relinquish their personal information is that they have become accustomed to having information about themselves collected. So, with little or no contemplation, personal information is provided in exchange for services – information that has the potential to be shared between databases and transported across national boundaries. What remains to be seen is whether or not we are systematically de-sensitizing an entire generation to the value of protection of privacy.

When it comes to biometric surveillance technologies, one of the biggest risks associated with accepting this technology as part of our daily lives is that we begin to adopt a level of social indifference. Jeremy Crampton claims that "many people now accept being under surveillance as a natural state of affairs" (2007, p. 394). For example, on a recent trip to London my husband noted that he was very cognisant of the numerous closed-circuit televisions (CCTVs) monitoring the city; however, friends of ours who reside in London have become completely oblivious to their presence. Can we assume from this observation that society's indifference to the CCTVs in London has made it easier for the British government to increase their surveillance over this city?

Technology is evolving at an alarming pace. The globalization of the digital landscape provides access to markets and social networks around the world. Regrettably, it is this interconnectivity with the digital world that poses the greatest threat to our privacy and confidentiality. Without strong security measures and explicit policies to protect our private and confidential information, we risk exposing ourselves to the policies of other organizations and nations. John Woodward, Nicholas Orlans, and Peter Higgins are hopeful that the tides may be changing:

"While not yet enjoying the media stature and public controversy associated with such high-tech issues as genetic cloning and cyberspace, the increasingly extensive use of biometrics in both the public and private sectors will force the public to take notice and to confront the accompanying legal and policy challenges" (2003, p. 198).

Information as a Commodity

Why are private industry and government investing so much effort into collecting our private information? According to an article in Fortune Magazine, personal information is a growing commodity. In June, 2004 Nicholas Stein reported that the United States government awarded a $10 billion dollar contract to Accenture (an outsourcing company) to develop its US-VISIT program. "US-VISIT is the futuristic and controversial new initiative that will use fingerprinting, retinal scans, and other so-called biometric data to monitor the flow of visitors across America’s borders" (Stein, 2004, p. 1). He further remarks that "it's a clear sign that the nascent homeland-security business, which companies have eyed since 9/11 as a potential gold mine, has finally come into its own. Arguably, our personal information is a valued resource. Why then, do we give it away so freely?

Benefits of Biometric Technologies

Clyde Crews (2003) suggests that, fundamentally, biometrics is about increasing convenience and service more than invading privacy. In addition to the profits gained by private industry,

and the enhanced security biometrics provides to individuals, the contributions that biometrics have made to the field of law enforcement are indisputable. For example, the creation of fingerprint and forensic DNA registries have enabled law officials to maintain criminal records, positively identify and convict criminals, and successfully solve criminal cases.

Research in the field of biometrics is ongoing. Although considered by some to be ethically questionable, emerging Radio Frequency Identification (RFID) technologies and implantable microchips containing biometric information are now used to help track lost family members suffering from Alzheimer's. The same technology is also used to find lost pets and promises to be able to provide parents with the same ability to locate a lost or missing child. In addition, fingerprint readers are gaining in popularity and are now being used in guns as a means of reducing the unintentional as well as the intentional misuse of these weapons by children and criminals. These examples briefly illustrate some of the benefits and contributions that biometric technologies have made to society. On their own, these examples are fairly innocuous. Why, then, is there so much controversy surrounding this technology? Can biometric surveillance go too far? What happens when governments step in? Do the benefits continue to outweigh the risks?

Challenges and Risks of Biometrics

The attacks of September 11, 2001 on the World Trade Centre created an environment of fear and vulnerability. In the wake of this event, "the public expressed a willingness to give government officials more investigative and surveillance powers to fight terrorism" (Magi, 2007, p. 459). Unfortunately, it is during times of crisis, like this tragic event, that we as citizens become vulnerable and are more inclined to compromise our freedoms to protect the security of our country. We react to current events and put our trust in government officials to protect our rights. In response to this public outcry, governments in the United States, Canada, and abroad increased border control and developed a renewed interest in biometrics.

The proliferation of biometric technologies in recent years has generated much debate. Based on the literature reviewed for this paper, and personal observations, the following examples have been selected to briefly illustrate the potential threat of this technology to society and future generations:

Identity Theft

The digital format of biometric records creates an extremely efficient medium for accessing, storing, and retrieving information. Ironically, it is this same feature which makes this information the target of serious privacy and security risks. This is especially true for systems that are not properly designed and/or regulated. Unlike credit cards or other types of traditional

identification, which can be replaced if lost or stolen, a biometric cannot be replaced. According to the Canadian Internet Policy and Public Interest Clinic (CIPPIC), "once a biometric identifier is compromised, it stays compromised" (CIPPIC, 2007, p. 43). Arguably, recent security breaches have led many of us to believe that our private information is not as safe as we would like to assume. When we consider the irreplaceable nature of our biometric information, the loss of this data becomes a very frightening pill to swallow.

Tracking

Although there are a number of surveillance technologies capable of tracking and locating people, none can match the precision of biometric technologies (CIPPIC, 2007). Tracking individuals through this technology poses a significant threat to their right to privacy. Imagine if our employers were able to track our exact location at any given point during the day. Eventually, after an appropriate amount of time has passed, enough information is collected to accurately predict our every move. This information, in the hands of the wrong people, poses a serious threat to the freedom and security of individuals in a free society. Ironically, tracking is also described as a positive feature of biometrics when applied to the infirm, pets, and children. Although it may provide comfort to loved ones, my concern with this technology is that it is forced upon vulnerable populations who cannot speak for themselves. Furthermore, I fear that this technology will slowly creep into our everyday lives and become an accepted system of surveillance for all citizens.

Invasion of Privacy

Currently, most programs offering biometric privacy enhancements are voluntary; however, this could change at any time. For many, the act of collecting biometric information has become closely associated with criminal activity and it is considered personally and morally offensive (CIPPIC, 2007). In addition, religious and cultural customs can interfere with the collection process. For example, Muslim women wearing a full burqa would find it extremely offensive to show their face. On top of all of this, there is something de-humanizing about reducing individuals to a number, and I find it difficult to imagine any of us wanting to be treated like human barcodes.

Surveillance State

The very mention of the term "surveillance state" or "police state" brings to mind images of totalitarian governments run by dictators who use fear and repression to enforce absolute control over their citizens. Government control of biometrics has the frightening potential to put our essential freedoms at risk (Ashbourn, 2005; Clarke, 2001; Crampton, 2007). "Governments can use the technology to restrain us and violate our liberty and privacy" (Crews, 2003, p. 16).

Our history books are riddled with examples of government brutality and abuse of power, but none are as vivid as the atrocities suffered by the victims of World War II Nazi concentration camps. Rob Fixmer reminds us of this heinous government and its malevolent abuse of power:

> In Western democracies, where George Orwell's *1984* is taught with apocalyptic zeal, the notion of an all-knowing government is terrifying. In a world committed to never forgetting the victims of Nazi concentration camps, the grotesque image of numbers tattooed on human beings has forever equated forced identification with sheer evil. (As cited in Freeman, 2003, p. 6)

Apathy

Perhaps the most terrifying threat of accepting biometrics comes from our failure as citizens to question the application and infiltration of this technology into our everyday lives. Ostensibly implemented as a means of fighting terrorism, biometric technologies have grown in popularity with the global community. For a society that proclaims to hold privacy and freedom in such high regard, our apathy speaks volumes. Left unchecked, governments and private industry have the potential to track and control every aspect of our lives under the guise of providing services and conveniences. Given our current climate, George Orwell's revolutionary tale of a world governed by a corrupt and all-knowing government seems too close for comfort.

The Spider and the Fly: The Lure of Biometric Technologies

In Mary Howitt's children's poem, "The Spider and the Fly", the spider cunningly tempts and eventually persuades the fly to come into his parlour. At first the fly is hesitant; knowing that all who enter never return. Before long, however, the fly's curiosity and vanity get the better of him and he enters the parlour. Are we like the fly; slowly being lured into an intricate web of deception? Are governments and private industry introducing biometric technologies on a volunteer basis to gain our trust and prepare us for a future without this choice? Are we being drawn in by the promise of improved and enhanced security systems, or are we more interested in acquiring the newest gadget on the market? What about our children? Are they being targeted by marketing agencies preying on a generation's indifference? Are we sentencing the privacy of future generations to the same untimely end as the fly in Mary Howitt's poem? The poem ends with the spider warning readers to think before acting:

> And now dear little children, who may this story read,
> To idle, silly flattering words, I pray you ne'er give heed:
> Unto an evil counsellor, close heart and ear and eye,
> And take a lesson from this tale, of the Spider and the Fly (Howitt, 1829, p. 7).

The poem teaches its audience a valuable lesson about manipulation and getting caught up in the moment. Perhaps this is a lesson that we would all do well to consider before rushing out to adopt new biometric technologies.

Conclusion

Global usage of biometric technologies has undergone significant growth since the events of September 11, 2001. Ostensibly introduced by governments as a method of increasing public security, advancements with this technology have generated a lucrative market for biometrics manufacturers. Although many positive outcomes have resulted from these developments, the threats and challenges that are associated with this technology are very real. While biometrics can provide an additional level to personal and national security, it can also increase the potential for deliberate surveillance. In fact, Steven Spielberg's portrayal of personalized advertising in the futuristic biometric-world of *Minority Report* has made its debut in the real world. Jennifer Schenker (2008) recently reported in an article for *Business Week* that YCD Multimedia, an Israeli company that manufactures digital display systems, is changing the future of retail advertising. Tiny cameras use facial recognition to "scan shoppers' faces to determine their sex, race, and approximate age, and then flash appropriately targeted ads" (Schenker, 2008, p. 4).

With little or no contemplation, we willingly surrender our personal information every day – information that is potentially shared between databases and transported across national boundaries – information that knows no borders. Younger generations, as we have established, have adopted a laissez-faire attitude and are willing to provide their personal information without question. This has to stop. We need to be introspective and question why industry and government are placing more value on our personal information than we do.

Privacy must be built into the policies governing biometric identification systems. Moreover, every effort should be made to ensure that these technologies and policies evolve at the same pace. Without strong enough legislation to ensure that outsourcing agencies are securely protecting our private and confidential information; we may soon find ourselves swallowed up by the policies of other nations. "If government agencies misuse these advances, it can create a situation where those freedoms can be challenged or even destroyed" (Freeman, 2003, p. 8). Roger Clarke makes the following observation:

> The once-free world is submitting to a "technological imperative", and permitting surveillance technologies to change society for the worse. Biometrics tools are among the most threatening of all surveillance technologies, and herald the severe curtailment of freedom, and the repression of "different-thinkers", public interest advocates and "troublemakers." (2001, p. 66)

As responsible citizens, we must recognize both the benefits and threats that this technology poses to future generations. We must be proactive citizens and support public awareness. We must learn from our past and teach our children to ask questions. Otherwise we risk compromising their freedom of inquiry. If this freedom is lost, the results are not only devastating to us as individuals, but they also pose a potential risk to the global community.

References

Ashbourn, J. (2005, January). The social implications of the wide scale implementation of biometric and related technologies. Retrieved November 10, 2008 from http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/SocialImplications_Ashbourn.pdf

Brown, P. (2008, August 18). Privacy in an age of terabytes and terror. *Scientific American*. Retrieved November 23, 2008 from http://www.sciam.com/article.cfm?id=privacy-in-an-age

Canadian Internet Policy and Public Interest Clinic (CIPPIC). (2007, June 2). *Biometrics*. Retrieved November 21, 2008 from http://www.cippic.ca/biometrics

Clarke, R. (2001, April 15). Biometrics and privacy. Retrieved November 10, 2008 from http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html

Crampton, J. (2007, July). The biopolitical justification for geosurveillance. *Geographical Review, 97*(3), 389-403.

Crews Jr., C. (2003, July). Monitoring biometric technologies in a free society. *USA Today Magazine, 132*(2698), 16-18.

Fixmer, R. (2001, October 1) Getting to know you. *Interactive Week, 8*(38), 6.

Freeman, E. (2003, July/August). Biometrics, evidence, and personal privacy. *Information Security Journal, 12*(3), 4-8.

Gibb, F. (2008, October 21). DPP chief Sir Ken Macdonald attacks Big Brother state surveillance. *Times Online*. Retrieved from http://www.timesonline.co.uk/tol/news/uk/article4984788.ece

Howitt, M. (1829). The spider and the fly. Retrieved on November 23, 2008 from http://www.love-poems.me.uk/howitt_the_spider_and_the_fly_funny.htm

Jain, A., Hong, L. & Pankanti, S. (2000, February). Biometric identification. *Communications of the ACM, 43*(2), 91-98.

Magi, T. (2007). The gap between theory and practice: A study of the prevalence and strength of patron confidentiality policies in public and academic libraries. *Library*

and Information Science Research, 29(4), 455-470.

National Science and Technology Council (NSTC). (2006, August 7). Biometrics history. Retrieved November 10, 2008 from http://www.biometrics.gov/Documents/BioHistory.pdf

O'Harrow, R. (2006). No place to hide. New York: Free Press.

Osborn, A. (2005, August 17). Biometrics history: Looking at biometric technologies from the past to the present. *Video Surveillance Guide*. Retrieved November 10, 2008 from http://www.video-surveillance-guide.com/biometrics-history.htm

Schenker, J. (2008, September 22). Point-of-sale advertising goes high tech; New in-store digital ads are using the latest technology to target messages to individual buyers, boosting sales and even helping to manage inventory. *Business Week Online*. Retrieved February 19, 2008 from http://www.businessweek.com/globalbiz/content/sep2008/gb20080922_109810.htm

Stein, N. (2004, June 28). The fruits of safety Accenture's $10 billion contract marks a water-shed: The homeland-security market has hit the big time. Stand by for much, much more. *Fortune.* Retrieved November 19, 2008 from http://money.cnn.com/magazines/fortune/fortune_archive/2004/06/28/374384/index.htm

van der Ploeg, I. (2003). Biometrics and privacy: A note on the politics of theorizing technology. *Information Communications & Society, 6*(1), 85-104.

Woodward, J., Orlans, N. & Higgins, P. (2003). Biometrics: Identity assurance in the information age. Berkley: McGraw Hill Osborne.