The Ethics of Unspecified Exposure

Class Final: Ethics and the Professional

Ethics and the Professional

Final Paper

Professor: Dr. Richard Ward

Victoria Xavier-Freyr

Ethics Unspecified Exposure

Ethics and the Professional

Professor Richard Ward
01 November 2009 13:31:00

The Ethics of Unspecified Exposure

Ethics and the Professional

ABSTRACT:

The reason for surveillance of civilians lies in the interests of national security, crime prevention, and law enforcement. Biometric, RFID, and scanning technologies have demonstrated their efficiency and usefulness in tracking and monitoring potential threat concerns. However, the decision to employ these advanced technologies routinely and in civilian venues has caused considerable controversy and adverse public opinion. Therefore, we should review not only methods, applications, and effectiveness (as determining or measuring success) in securing the nation and providing a state of civil orderliness.

The purpose of this paper is to consider the potential advantages, harms, and social losses from implementing high-tech surveillance, which is used widely in civilian venues to monitor potential security threats and crime. Do "the (intended) ends" justify "the means" applied? Where will these surveillance trends lead us? Is the greater good best served for citizens through the cost (compromises to our civil liberties and privacy)? Does pervasive surveillance render an atmosphere of perceived certainty and safety? These are some of questions that will be explored.

Victoria XAVIER-FREYR
02 September 2010 13:38:34

INTRODUCTION

The United States Government has used surveillance in the detection of subversive acts and the apprehension of criminals since the days of our Founding Fathers. Efforts in more recent times were focused on bringing in gangsters and drug dealers which escalated and increased dependence of stakeouts and wiretaps that were employed routinely, yet governed closely by legal procedure. White-collar crime escalated, globally, and triggered measures that are more sophisticated which have been used within the United States and by cooperating law enforcement groups around the world, such as INTERPOL. In all instances, the ethical value was to protect the general populous from exposure to or connection with these criminal elements which might otherwise go unchecked.

There were many occasions when criminal activity flowed across U.S. borders and became international matters of interest that required broader attention than internal affairs typically warrant. Primarily, drug trafficking and cartels prompted the need for closer attention and cooperation among government law enforcement agencies —all directed at illegal activities or organizations with multiple streams of money tainted by drugs, black market and various types of money laundering. The occasional scheme with international reach did not achieve the sustained awareness or concern generated by the up rise in terrorist activity throughout the 20th century which culminated in the 2001 World Trade Towers incident. Reliance on advanced, technology-supported measures is proven, if controversial as they affect the general public's access to or rights from aspects of liberty, privacy, and justice.

S1: SECURITY CONCERNS

Even at Court in ancient times through the Middle Ages, kings had to fear the encroachment of spies and malevolent interests. The king had a trusted person, or group, watching those who were not trusted in the military or political circles, to include the religious authorities of the times. These surveillance methods were defensive in nature and matched with general precautions and security to keep the king, their family, and their countries safe from any forces wanting their possessions or territory. Clearly, surveillance is nothing new to the world —only the means and increasing stealth, by or with which it is carried out. Likewise, we have a concept of the neighbourhood —perhaps taking on a broader meaning in the 20th and 21st centuries with the transient nature or life and work as well as the interests of the individual being spread across multiple regions, industries, or countries. The "neighbourhood" is no longer simply the walking distance around our homes which gives us the need to have a sense of ethics that encompasses the needs and interests and rights of many

people, simultaneously wanting to secure their liberties and well-being, to include their privacy. Our social provincialism incited suspicion to arise whenever newcomers presented themselves and often led to having them scrutinized by locals, sheriffs, and other protectors of a certain territory, frequently within a small, enclosed area. Modern circumstances are not so different when it comes to surveillance except the area requiring coverage, the sheer number of unknown individuals, and the vehicles used for transport —all of which make effectiveness and efficiency important in the techniques used to monitor activities which have the potential to pose a risk to individuals, businesses, or governments.

However, most of these dangers and infringements on individuals for the greater good (as defined within context) were security-focused endeavours pointed toward targeted crime organizations or individuals connected to dubious circumstances. The new element is the "sweep factor" a broad and **unspecified** surveillance of the general public, without provocation.

S2: INTRUSIVENESS

Technology Overview

Law enforcement has used fingerprinting since the 1920s and before which uses impressions of the unique ridges of the fingertips to ensure the identification of individuals. There are new finger-specific capabilities such as finger and vein authentication, and hand geometry all of which require some manual or digital contact. Furthermore, there are ocular-based methods of identification that require procedures which depend on the same acceptance of the need for surveillance (as a part of the retinal or iris scan procedures), both of which necessitate the knowledge and cooperation of the individual in question. [Surprisingly, the retinal scan concept was identified back in the 1930's although the actual, perfected capability has been acquired only recently.]

There is a measure of convenience involved in these efficient advancements in surveillance. Current technologies such as scanning and infrared for biometric identification (used for facial or voice recognition and speech pattern authentication), allow for undetectable surveillance, at a distance and without visibility to the subject under surveillance. Unfortunately, there are drawbacks as well which originate from the technology's sophistication and inherent stealth. The newer technologies that are being used are highly advanced and contactless, i.e., there are no requirements for the subject being scrutinized to be physically touched, probed, or even aware that the surveillance is taking place. For instance, before scanning and biometric surveillance was available, the subject of an investigation had to submit to review. Likewise, an approval was needed as a part of legal

procedure to conduct the review which might lead to self-implication. These steps protected the individual's constitutional rights and due process. Besides the technology aspects of surveillance, the problem (if not danger) has become that surveillance could be used to confirm an individual's location at a specific time meaning that a prosecutor could establish opportunity in the commission of an alleged crime(s). The risk is that anyone present at the scene of a crime or locations with proximity or crime-related or bearing interest could be targeted for prosecution without other suspicions based on evidence or motive.

Public v. Private Places

In the twentieth century and before, the public thought of security measures and surveillance as an inconvenience that seldom affected them personally —only offenders or criminal elements were targeted for monitoring. Moreover, walking into a non-government or military building or a private home meant that no one who was not present had access to the actions or conversations which took place. The post-9/11 world saw many changes in the government and security forces, especially in the reconfiguration of intelligence and enforcement agencies as well as modifications and enhancements to tracking database and monitoring devices which were upgraded to include advance technologies. Likewise, many civilian venues such as airports, shopping malls, and sports stadiums had security upgraded as a response to finding themselves on the civilian target list of the extremists who had carried out bombings and other attacks which would endanger non-military or government structures. [In military terminology, bringing civilian targets into play, which puts the general population at greater risk, is considered "counter-value" hostility meaning that the area poses no certain threat. In hostile circumstances, such as a declared war, there is an expectation for "counter-force" or "hard target" aggressions by the opponent at the least as defensive measures (or, as pre-emptive strikes that would decrease the aggressor's vulnerability and potential for causalities). Therefore, military areas and government buildings are accepted targets because these areas would be the source of counter-attacks or resistance.] Regardless of the circumstances, physical security has not been the only concern. Computer network and data security has posed a major threat to individual, business, and government confidentiality and privacy. Watchdog groups have grown in popularity to monitor government activity in surveillance as well as the cooperation (information sharing) between governments, businesses, and corporations that includes sensitive consumer or employee information as well as copious amounts of innocuous (that might serve in establishing behaviour patterns and personal habits) information that is available through social networking, especially on the Internet. The surveillance, security, and intrusion detection software industries have enlarged

their market share as well. Furthermore, non-profits such as Electronic Frontier Foundation (EFF) and Forensics Magazine serve the public's interests to challenge unnecessary or excessive surveillance from the government and corporate sources.

Reasonable Expectation of Privacy

The advancements in technology have encroached of every aspect of life, especially in individual rights and privacy. The public venues mentioned, from traffic cameras to monitor speed and manoeuvring violations to libraries and coffee shops have encouraged the public to surrender the privacy that they once had in the hope of safety from terrorists. The average citizen could now appreciate -- more empathetically -- the privacy concerns that once belonged only to rock stars and super spies who had constant fans, stalkers, or enemies pursuing them or perusing their trashcans to uncover their personal information. To counteract the upswing in surveillance (not all from expected or legitimate sources such as authorities or employers), groups such as Privacy and Privacy International (the organization that makes Big Brother Awards) have been popularized where they used to be of interest to a much smaller, cyber community.

S3: LEGAL CONSIDERATIONS

Security and privacy concerns (in public places and at residences) have been issues for governments, officials, businesses, and individuals since ancient times. In medieval times the answer as to build a castle with a fortress and a mote. Yet, even then, physical security was not enough to protect personal interests and ensure the safety of a country or business. Just as common law addressed many aspects of personal rights, and government or property security, when American law was written by our founders, they made reference to security, the need for law enforcement and the rights of individuals as well as the concept of civil liberties.

United States Constitution

Fourth Amendment (1791, a part of the U.S. Bill of Rights)

An Amendment to the U.S. Constitution that gives us significant implications of the rule of law and the procedures or indictors that would illustrate the reasonableness of a warrant or circumstance for lawful search and seizure. This Amendment outlines the legal right of individuals related to gathering evidence that might be used in litigation. Therefore, it has a high impact of the use of surveillance, information that can be used as testimony, and sources that law enforcement can use to establish appropriate suspicion to allow search or seizes to take place.

Fifth Amendment (1791, a part of the U.S. Bill of Rights)

An Amendment to the U.S. Constitution that gives us due process (procedural and substantive) to protect our right, as U.S. citizens to life, liberty, and property which cannot be denied without specific legal procedures. This concept was derived from an earlier English document, the Magna Carta (1215). Many argue that within the **Fifth Amendment** there is an "implied" right to privacy as well. However, this implication is much debated and needs clearer statement to further acknowledge and specify the rights of an individual. Another argument made regarding the **Fifth Amendment** is that even though deprivation of private property and seizure of property naturally applies to physical possessions, there are intangible possessions as well, such as ideas, talents, etc.

Fourteenth Amendment (1868)

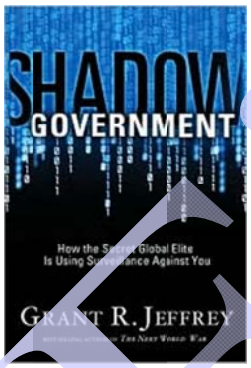
An Amendment to the Constitution that outlines additional privileges of individuals such as protections to civil liberties and the right to own property (extended to everyone after slavery had ended). These amendments represent the primary references for establish law related to surveillance. Despite the substance of these constitutional laws, there are many questions and challenges on the legality of surveillance and the rights of individuals to privacy and property. Additionally, many people think that our written laws did not adequately anticipate the pervasiveness of modern surveillance technologies. Considering America's experience with terrorists in recent years, it would be remiss not to mention the fact that, primarily, our constitutional laws were intended for and concerned with the lives and activities on the citizens of the United States as a free and democratic society. However, in the century and moving forward, an increasingly present factor in law will be the disposition and treatment of the non-citizen (their rights and benefits obtained from the Government). Clearly, there is concern as well for the potential or existence of sympathetic or complicit interests which might favour the activities of subversives or enemies of the country, from within its borders.

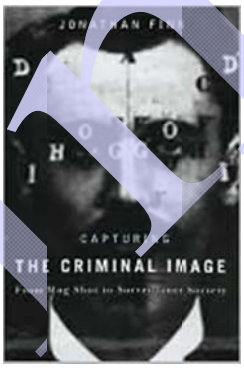
CONCLUSION

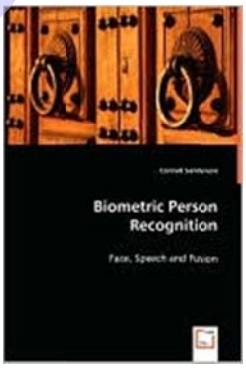
Unlike security efforts that involve terrorists, the picture for the needs and limitations for surveillance is much more difficult and unclear ethically, when the surveillance snares, without criminal considerations, otherwise law-abiding citizens. Surveillance is everywhere to monitor and protect us, not just the suspect activities of adults —children, without provocation. The government has to meet its moral obligations to secure the country for the general public as well as it constitutional duty to protect their civil liberties. Technology has supported these law enforcement and security objectives to the satisfaction of some (who have experienced large-scale, domestic terrorist attacks and the intimidation and the

uncertainty —or fear, which accompanies it) and the dismay of others who are more resilient to the unprecedented internal threats or more focused on the liberties which they feel are compromised beyond what could be considered as prudence or vigilance in offering the public security. The greatest question being how does the government official, the military officer, the law enforcement officer, the legal community, the business professional, or the average citizen respond to the need for security on the one hand with the desire to maximize the freedoms of the citizens on the other? These ethical choices exist in grey areas where the lives of civilians and their personal freedoms are held hostage in the balance.

We are living in a period of extreme transitions and worldwide change. Our reactions to those changes will not be definitive: they will be an extended process that would, ultimately, transform us and deliver us into the future. The question that we have to confront, together, is whether constant surveillance through technologies enables or cripples us as a society.







ANNOTATED BIBLIOGRAPHY

Best, Richard A., Jr. (2008). Satellite Surveillance: Domestic Issues. CRS Report for Congress.

Scaros, Constantinos E. (2008). Appendix B. *Learning about the law*. (3rd Ed., pp. 245-263). New York: Aspen Publishers.

Pavesic, Nikola. (2009). Hide—Homeland Security. Biometric Identification and Personal Detection Ethics. University of Ljubljana. Faculty of Engineering. Retrieved 2009 October 11 from http://www.hideproject.org.

Viera, Tudor. (2009). Japan to Build Hi-Res Optical Surveillance Satellite: The Nation Seeks to Beef-up Security. Retrieved 2009 October 9 from http://news.softpedia.com/news/Japan-tp-Build-HiRes-Optical-Surveillance-Satellite-103513.shtml.

Biometric Standards 2005 —Status, Progress, and Plans. (NBSP 2004, updated 2009 February 06). Retrieved 2009 October 9 from http://www.securityinfowatch.com/national-biometric-security-project-releases-biometric-standards-2005.

The State of Surveillance. (2005 August 8). Business Week. Retrieved 2009 October 11 from http://www.businessweek.com/magazine/content/05_32/b3946001_mz001.htm.