Jaime Quinonez

Prof. Rebecca Faery

21W.730 – 06 Imagining the Future

20 November 2003

Government Surveillance in the Digital Age

Imagine walking along a busy street in the middle of a sunny day. Also imagine that someone is following you around, videotaping everything you do. Disturbing thought? Even more disturbing is the fact that the United States government is already doing this, and it's perfectly legal.

According to Robert Trigaux, a reporter for the St. Petersburg times, until August of 2003, in Ybor City, Florida, the Tampa Police Department used thirty-six surveillance cameras that scanned faces of all people walking around the entertainment district. These surveillance cameras captured facial images and then compared them to a police database of known felons. This same surveillance system was also used during the Tampa Bay Super Bowl at the Raymond James Stadium, and other cities are attempting to install such a system. However, even though the cameras are used in public places, they still represent a large violation of privacy.

Also a violation of our privacy is the government's usage of the Carnivore Internet surveillance system that can track all of a person's online activity. The FBI not only has the capability to do so, but in many cases it can lawfully enter a person's home and alter or even steal information form his or her computer, all without the knowledge of the owner of the computer.

Cite as: Jaime Quinonez. Course materials for 21W.730-5: Writing on Contemporary Issues: Imagining the Future, Fall 2007. MIT OpenCourseWare (http://ocw.mit.edu/), Massachusetts Institute of Technology. Downloaded on [DD Month YYYY].

The government's ability to gather personal information on its citizens is similar to methods of surveillance in the novels *The Handmaid's Tale*, by Margaret Atwood, and *1984*, by George Orwell. In order to prevent the extreme cases of surveillance presented in these novels, it is the public's responsibility to remain alert to new developments in law enforcement so as to prevent an unreasonable surveillance system from arising. While it may not be possible to clearly defines people's right to privacy, the public must develop some notion of limits on the government's ability to invade its citizen's privacy, and then the public must constantly monitor the government so as to ensure that it does not cross these limits.

As technology allows for faster forms of communication, the Untied States government is quick to ensure that it can monitor the most popular forms of communication. Telephone calls and Internet communications are the standard medium of expression today, and the methods that may be used to monitor communication through these mediums are very developed. The telephone is a relatively simple technology, so monitoring someone's telephone calls is a rather simple task. Mostly, only very large service providers maintain large networks, and so in order to monitor someone, the government can easily determine the specifics by contacting only a few companies. However, Internet communication is far more technologically advanced, and it is much more difficult to monitor people's Internet communications than it is to monitor their telephone conversations. As the Internet is a relatively new creation, there is little centralization, and even finding someone online can be difficult enough. Still, the Federal Bureau of Investigation has software, nicknamed "Carnivore," that it can use to monitor all of the Internet activity of a suspected felon, and the suspected felon's Internet

Cite as: Jaime Quinonez. Course materials for 21W.730-5: Writing on Contemporary Issues: Imagining the Future, Fall 2007. MIT OpenCourseWare (http://ocw.mit.edu/), Massachusetts Institute of Technology. Downloaded on [DD Month YYYY].

Service Provider is required to provide the FBI with a physical location through which all of the suspect's Internet information flows, and the FBI monitors and records all of the suspect's information that appears suspicious. Furthermore, according to Jim Demspsey, a writer for the Center for Democracy and Technology, the FBI may break any sort of encryption, a coding process used to secure the privacy of the data. This includes not only all emails, but also Internet web traffic and all other forms of communication online. The government thus has the ability to monitor the most common form of communication.

While the government may have the physical ability to invade a person's life online, recording everything they do, many believe that it is prevented from doing so by laws and regulations. Indeed, electronic search warrants are required before using the immense power of Carnivore, and these search warrants must be obtained from federal district court judges, a higher authority than that required for normal search warrants. However, in the endless loopholes of legislation, the FBI can very easily avoid the need for a search warrant. According to Jim Dempsey, The Clinton administration circulated a draft of the Cyberspace Electronic Security Act that included provisions that would allow for secret searches to seize encryption information, disable a computer's encryption capabilities, or plant a keystroke-monitoring program. When the press received details of the bill, the secret search provisions were eliminated, only to reappear hidden in the details of a bill calling for stricter controls on the use of methamphetamine.

However, while these secretive measures may be frowned upon, the terrorist attacks on September 11, 2001, made any such deceit unnecessary as the government became able to openly pass laws that grant authorities such as the FBI the ability to break

Cite as: Jaime Quinonez. Course materials for 21W.730-5: Writing on Contemporary Issues: Imagining the Future, Fall 2007. MIT OpenCourseWare (http://ocw.mit.edu/), Massachusetts Institute of Technology. Downloaded on [DD Month YYYY].

other laws. The Patriot Act, meant to grant the President the power to combat terrorism, openly grants authorities the power to secretly invade a person's home without consent, perform searches, seize property, and not notify the person who was searched. All that is necessary for a search without a warrant is for the authorities to believe there is serious danger to a person or to national security. This loophole existed before September 11 under Title III, the Federal Wiretap Act, as well as under the Foreign Intelligence Surveillance Act. However, after the attacks of September 11, this loophole still exists, yet is often unnecessary, seeing as how courts rarely deny requests for search warrants, almost making the concept of a search warrant obsolete. After September 11, the patriotic fervor and the feeling of the need to protect the nation against outside agents has led to a legal status where the government enjoys the liberty to look into our private communications at will.

While the government's spying on our communications is intuitively seen as a violation of privacy, there is some difficulty in claiming the same about the controversial surveillance cameras in Ybor City. The cameras in Ybor City were not secret and they were videotaping a public place. In essence, they were not worse than store surveillance cameras that no one seems to quarrel with, or a policeman walking down the street, looking at everyone suspiciously. After all, the surveillance cameras were intended to protect people, so why should we complain about the apparently harmless cameras that offer protection? The surveillance cameras were capable of far more than what a simple policeman walking down the street is capable of. By recording images and matching them with a large police database, the surveillance cameras were theoretically capable of monitoring everybody and recording their everyday activities, a capacity which goes far

Cite as: Jaime Quinonez. Course materials for 21W.730-5: Writing on Contemporary Issues: Imagining the Future, Fall 2007. MIT OpenCourseWare (http://ocw.mit.edu/), Massachusetts Institute of Technology. Downloaded on [DD Month YYYY].

beyond the intended scope of the cameras. While it did offer protection, the camera system also made people feel uncomfortable and violated, since the potential for misuse by the authorities was too large. Furthermore, since the software used was still in development, the surveillance system was actually abandoned because authorities weren't able to form conclusive matches leading to any arrests, and so their sole function was simply spying on innocent civilians.

Amy Herdy, a reporter for the St. Petersburg Times, exposes the horror of the surveillance system in the case of Rob Milliron. While Milliron was eating lunch one day in Ybor City, Florida, his image was captured and used to display the function of the surveillance cameras, meaning his image appeared in magazines across the nation. Even though this would be a great enough disturbance to many people, the real disturbance to Milliron was that a random lady in Oklahoma called the authorities, accusing him of being wanted for child neglect. Unexpectedly, Milliron was publicly confronted at his job about the matter, and even though the police eventually concluded correctly that he was not the wanted man, and that this was a case of mistaken identity, the humiliating experience represents a serious misuse of the surveillance system that society should not allow.

The electronic surveillance systems are disturbing because they can lead to a stricter, more powerful surveillance system that encompasses even more of citizen's personal lives than what is currently in place. The novels *The Handmaid's Tale* and *1984* represent such surveillance systems, where people live in fear of the government and know that they cannot reasonably act out against being monitored. In *The Handmaid's Tale*, the government employs many people to monitor everyone who walks on the street

Cite as: Jaime Quinonez. Course materials for 21W.730-5: Writing on Contemporary Issues: Imagining the Future, Fall 2007. MIT OpenCourseWare (http://ocw.mit.edu/), Massachusetts Institute of Technology. Downloaded on [DD Month YYYY].

or appears suspicious. Furthermore, they encourage all citizens to report any deviant behavior, whether it is from someone of a lower or upper class. In essence, that is the same spirit behind legalizing intrusions into people's privacy since those who make and support the laws are encouraging the arrest of anyone with suspicious behavior. However, a much more extreme example of inappropriate government surveillance is that in *1984*, where there are telescreens in all possible places, observing all actions. If someone makes a sign that indicates they are against the government, the ThoughtPolice come and arrest the radical thinker. Even if a person is guilty of saying something against the government while asleep, the ThoughtPolice still come unexpectedly, just as they came for Rob Milliron in Ybor City.

With the increase in technology and electronic forms of communication, the potential for government surveillance forces people to consider how much of their privacy they should be expected to give up for the sake of protecting personal and national security, as well as how much privacy is fundamentally protected by being in a civilized society where notions of privacy are important. The theory behind intrusions of privacy is to better protect the nation, and after September 11, few Americans even considered the intrusions on Middle Easterners as unnecessary violations of privacy. When the airports reopened, few complained about how Middle Easterners had to undergo much more screening than others had to undergo. Under the threat of a real attack, people felt the danger and were eager to embrace legislation that eliminated much of their privacy. However, now the patriotic fervor of September 11 has died down and while most of the public is still concerned with ensuring national security, some people have begun to question the extent to which the government can use reasons of national

Cite as: Jaime Quinonez. Course materials for 21W.730-5: Writing on Contemporary Issues: Imagining the Future, Fall 2007. MIT OpenCourseWare (http://ocw.mit.edu/), Massachusetts Institute of Technology. Downloaded on [DD Month YYYY].

security for violating people's rights to privacy. This oscillating view of privacy rights provides skeptical grounds for any argument either supporting national security or privacy rights, since people fundamentally want both. Therefore, there has to be some reasonable balance between these two important aspects.

The public must decide on a limit to the extent to which the government can invade the privacy of its citizens. However, this limit cannot be clearly defined, since people would demand different minimum levels of privacy given different situations. Not seeing any immediate danger, a person would only allow a small intrusion on their privacy. If a country were about to win a war, its citizens would not see a heavy intrusion on their privacy as being justified. However, for the country that is losing a war, its citizens would freely surrender most, if not all, of their privacy rights if doing so will help the state protect the citizens against being invaded and probably killed. Innocent people are likely to complain against an intrusion on their own privacy, but might happily agree to the intrusion of the privacy of a known child rapist. These two levels of acceptable violations of privacy, while being two opposite extremes, both seem acceptable. It is thus difficult for there to be any fixed standard for minimum privacy rights. The only basis for judgment on whether an act by the state unreasonably violates the privacy of its citizens is an intuitive analysis of whether or not the outcomes justify the violations. People will accept major violations of privacy in order to protect their own lives, yet they should not accept major violations if there is no such important reason for accepting those violations.

The public must continuously observe the actions of the state and people must object when they feel there has been an unjustified violation of privacy. If the

Cite as: Jaime Quinonez. Course materials for 21W.730-5: Writing on Contemporary Issues: Imagining the Future, Fall 2007. MIT OpenCourseWare (http://ocw.mit.edu/), Massachusetts Institute of Technology. Downloaded on [DD Month YYYY].

government declares a state of emergency and violates people's rights in order to ensure national security, but it is later discovered that there was no real reason for believing in any sort of danger, then the public should criticize the government and should demand that if people acted outside of their power, those people should be removed from office. If enough people voice their opinion and it is evident that there was an unjustified violation of privacy, the people should be able, under the principles of democracy, to change the government so as to try to better protect the public in the future. Even if it is concluded that the government unjustifiably violated people's rights and yet everyone in office acted properly within their jurisdiction, voicing public opinion and spreading these concerns still help protect against future invasions of privacy. The key to ensuring a suitable system for the government to protect the nation is for the public to speak out and voice its opinion. The people must take some responsibility in the management of their nation, or else the people will only have themselves to blame if an all-powerful government arises.

Cite as: Jaime Quinonez. Course materials for 21W.730-5: Writing on Contemporary Issues: Imagining the Future, Fall 2007. MIT OpenCourseWare (http://ocw.mit.edu/), Massachusetts Institute of Technology. Downloaded on [DD Month YYYY].

Works Cited

Atwood, Margaret. *The Handmaid's Tale*. Houghton Mifflin Company, 1986.

Dempsey, Jim. **CESA lives: Secret searches provision in the meth bill**. 23 May 2000. Center for Democracy and Technology. 27 Oct. 2003. <http://www.cdt.org/security/cesa/000523cesalives.shtml>.

Federal Bureau of Investigation – Carnivore. 24 July 2000. Federal Bureau of Investigation. 26 Oct. 2003. <http://www.cdt.org/security/carnivore/000724fbi.shmtl>.

Herdy, Amy. **Tampabay: They made me feel like a criminal**. 8 Aug. 2001. St. Petersburg Times. 2 Nov. 2003. <http://www.sptimes.com/News/080801/TampaBay/_They_made_me_feel_li.shtml>.

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. July 2002. Computer Crime and Intellectual Property Section. 26 Oct. 2003. <http://www.cybercrime.gov/s&smanual2002.htm>.

The Nature and Scope of Governmental Electronic Surveillance Activity. Sep. 2001. Center for Democracy and Technology. 27 Oct. 2003. <http://www.cdt.org/wiretap/wiretap_overview.html>.

Trigaux, Robert. **Tampabay: Cameras scanned fans for criminals**. 31 Jan. 2001. St. Petersburg Times. 2 Nov. 2003. <http://www.sptimes.com/News/013101/TampaBay/Cameras_scanned_fans_.shtml>.

Orwell, George. *1984*. New York: Signet Classic Printing, 1950.

Cite as: Jaime Quinonez. Course materials for 21W.730-5: Writing on Contemporary Issues: Imagining the Future, Fall 2007. MIT OpenCourseWare (http://ocw.mit.edu/), Massachusetts Institute of Technology. Downloaded on [DD Month YYYY].