

## Privacy As It Relates To Security

By Gregory Leiby

PUBP 726-001, Telecommunications Policy, Wednesday (7:20-10:00 PM)

Assignment 3, Paper 3

### INTRODUCTION

“Security and privacy are two sides of the same coin.” –Richard Clark<sup>1</sup>

Richards Clark’s statement in his keynote speech to the Smart Card Alliance conference in October of this year (2004) elevated privacy rights beyond medical record access, employer reading of employee email, or the police peeking in bedroom windows. It goes beyond W. A. Parent's consideration that the most common views of privacy are "1) the right to be left alone, 2) the right to exercise autonomy or control over significant personal matters, and 3) the right to limit access to the self."<sup>2</sup>

The implication of this elevation of privacy to the level of security is that it is needed to “...establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity...”<sup>3</sup> The significance of this concept can not be underestimated; the only place the word “security” appears in *The United States Constitution* or *Amendments To The Constitution* is in Article II of *Amendments To The Constitution* (the “Second Amendment” or “Right to Bear Arms”). There is no doubt that, based on Richard Clark’s association, “security” and, “privacy” is implicit in the words “establish,” “insure,” “defense,” and “secure

In this paper I will examine how we came to the modern concept of “the right to privacy”. I will then discuss real world examples of Richard Clark’s Privacy/Security statement and address the implications this has for government policies as they pertain to communication issues.

---

<sup>1</sup> Mary Catherine O’Connor, *RFID Journal*, Spotlight on Security, Privacy Issues, October 22, 2004, <http://www.rfidjournal.com/article/articleview/1200/1/1/>.

<sup>2</sup> Mary Chlopecki, *The Freeman: Ideas on Liberty*, The Property Rights Origins of Privacy Rights, August 1992, <http://www.fee.org/vnews.php?nid=2616>.

<sup>3</sup> *The United States Constitution*, <http://www.house.gov/Constitution/Constitution.html>.

## WHAT ARE THE ORIGINS OF “THE RIGHT TO PRIVACY?”

Privacy rights date back as least as far as classical Greece, where:

“The concept of privacy and limited privacy rights was recognized in ancient Athens. Indeed, the language, law, and writings of the period reveal that privacy and property in Athenian society were interconnected, and recognized as such.<sup>4</sup>”

Several cases in Europe moved law in the direction of modern “privacy rights:”

**Pope v. Curl** (1741) - A person has a property right to their written words.

**Yovatt v. Winyard** (1820) - A person has a property right to their personal secrets.

**Prince Albert v. Strange and Others** (1849) - Privacy rights are a type of property right.

As seen from the examples above, “privacy rights” were directly related to property rights. This concept was brought into question in 1890 with Samuel Warren and Louis D. Brandeis’ article *The Right To Privacy*. In this article they argued that privacy issues should not be considered as a part of property issues, but should be considered separately.

Warren and Brandeis cited the growth of technology, especially advances that allowed mass distribution of information, as the greatest threat to privacy. As they stated:

“Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right ‘to be let alone.’ Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction

---

<sup>4</sup> Mary Chlopecki, *The Freeman: Ideas on Liberty*, The Property Rights Origins of Privacy Rights, August 1992, <http://www.fee.org/vnews.php?nid=2616>.

that ‘what is whispered in the closet shall be proclaimed from the house-tops.’<sup>5</sup>

As demonstrated by Warren and Brandeis, concern of technology eroding privacy has been an issue for over a hundred years.

## **TECHNOLOGY ISSUES AT THE FOREFRONT**

Over the past ten years, concerns over information and communication technologies and the relation to privacy and security have increased. Many of the new technologies have not easily fit the definitions in existing legislation, huge amounts of information can easily be mined from networks and databases, and many users do not understand how the technology they use works.

The following examples demonstrate the relationship between security and privacy, as stated by Richard Clark.

### **Workplace Surveillance**

In his article *How Workplace Surveillance Works*, Kevin Bonsor says seventy-eight percent of all companies use some type of surveillance system.<sup>6</sup> Some typical methods are:

- **Packet sniffers:** Programs that read information contained in the individual packets sent on a network.
- **Log files:** Files that keep track of events on a computer.
- **Desktop monitoring programs:** Software that shows and records all keystrokes on a computer.
- **Phones:** Recording phone calls and reviewing voice mail.

---

<sup>5</sup> Samuel Warren and Louis D. Brandeis, *Harvard Law Review*, The Right To Privacy, 1890, <http://www.louisville.edu/library/law/brandeis/privacy.html>.

<sup>6</sup> Kevin Bonsor, *How Workplace Surveillance Works*, <http://computer.howstuffworks.com/workplace-surveillance.htm/printable>.

- **Closed-circuit cameras:** Video monitoring of work areas.

Companies use surveillance with good reason. As Nancy Flynn, executive director of the ePolicy Institute states,

"Productivity is a concern; loss of confidential information is still a concern; security breaches are a concern. But...the number one concern is liability. Employers are afraid of being sued."<sup>7</sup>

Companies have certain responsibilities to their investors, business partners, customers, and employees; among these are securing data and preventing their infrastructure from being used in an unsecured manner. Companies must ensure the privacy of information and infrastructure by a variety of methods, including surveillance. Violation of information or infrastructure is a security situation.

Many employees (and civil rights groups) are concerned about corporate surveillance and how it relates to personal privacy. Questions have been raised and courts have ruled on companies reading employee email, monitoring their Instant Messaging, Internet and computer usage, listening to their telephone calls and voice mail, and using video cameras for surveillance.

Three pieces of legislation are typically cited in workplace surveillance cases involving communication technologies; the Wiretap Act, Stored Communications Act, and Electronic Communications Privacy Act. These acts, originally designed for protection from illegal government surveillance, have been used to argue against employer surveillance. However, the court opinions have favored the employers who own the computers and infrastructure that is monitored. However, the law does set specific conditions in which an employer may intercept communication off of a wire (this is different than information which is stored). This means monitoring a telephone call requires a different procedure from voice mail. An interesting note, consent to be monitored by the employee eliminates most issues of legality about surveillance; a simple waiver on the first day of employment could eliminate most of these legal issues for the companies.

---

<sup>7</sup> Dawn Kawamoto, TechRepublic, Mind those IMs--Your Cubicle's Walls Have Ears, October 25, 2004, [http://techrepublic.com.com/5100-22\\_11-5424770.html](http://techrepublic.com.com/5100-22_11-5424770.html).

## **Consumer Financial Information**

Financial institutions collect a great deal of information about their customers (consumers). With the advances in information technology, a tremendous amount of information can be gathered about these consumers. As information becomes easier to cross-reference and mine, the damage that can be done to consumers increases dramatically.

A serious threat to consumers is identity theft. Synnovate, in their 2003 report to the FTC states,

“Including all types of ID Theft, a total of 4.6 percent of survey participants indicated that they had discovered they were victims of ID Theft in the past year. This result suggests that almost 10 million Americans have discovered that they were the victim of some form of ID Theft within the last year.”<sup>8</sup>

The Federal government has passed two pieces of legislation specifically intended to protect consumers:

### **Gramm-Leach-Bliley Financial Modernization Act**

This legislation covers three areas of consumer protection of information:

- **Financial Privacy:** Financial institutions must inform consumers how they collect and share consumer information.
- **Safeguards:** Financial institutions must have a plan to protect consumer data
- **Pretext provisions:** Financial institutions may not collect consumer information under false pretexts.

---

<sup>8</sup> Synnovate, *Federal Trade Commission – Identity Theft Survey Report*, September 2003, <http://www.ftc.gov/os/2003/09/synovatoreport.pdf>.

## **The Fair and Accurate Credit Transaction Act**

This legislation helps protect against, and recover from, identity theft. It contains a number of provisions:

- The victim of identity theft has the right to contact credit-reporting agencies to flag their account.
- A notation that active duty military personnel are deployed, an alert on their credit report, as a way to alert potential creditors to possible fraud.
- If a fraud alert or active duty alert is placed a credit report, any business that is asked to extend credit must take “reasonable steps” to see that the credit application was not made by an identity thief.
- Receipts for credit and debit card transactions may not include more than the last five digits of the card number or the expiration date.
- A business that provides credit to someone who fraudulently uses an identity must provide copies of the documents (such as applications for credit or transaction records) to the victim and law enforcement.
- If contacted by a collection agency about a debt that resulted from the theft of identity, the collector must inform the creditor.
- Financial institutions must adopt procedures designed to spot identity theft before it occurs.
- Any business that uses a consumer report must adopt procedures for proper disposal.

## **The USA PATRIOT Act**

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act is one of the most controversial issues in regards to privacy today. The act was voted into law by a by an overwhelming majority of Congress (87 percent

voted in favor)<sup>9</sup> after the September 11<sup>th</sup> terrorist attack. Charles S. Morford states:

“The USA PATRIOT Act...amended a number of existing statutes and enacted new provisions covering a wide range of topics. Although much attention has been focused on the amendments to surveillance and immigration laws, the USA PATRIOT Act also provides for...consumer protection from fraud by requiring disclosure in solicitations for charitable contributions after a terrorist attack...and resources to study critical infrastructure.<sup>10</sup>”

Although there are many areas covered by the act, privacy advocates are most concerned about the expansion of the Federal government to tap telephones and track Internet usage. This expansion extends existing statutes to include electronic communication. In additions, Internet service providers must make their services more wiretap friendly. These expansion are necessary because:

"The law provides law enforcement the tools to respond to the ever-evolving communications technology in this country. Heretofore, there was some uncertainty whether law enforcement wiretapping and surveillance powers covered new forms of electronic media and the internet. Current laws were written decades ago, crafted for rotary telephones – not email, the Internet, mobile communications, and voicemail...Many of the changes enacted in USA Patriot are in response to the fact that terrorists are trained to change mobile phones frequently and to route email through different Internet computers in order to defeat surveillance. Prior laws were ill-adapted for reaching communications over multiple mobile phones and computer networks in different jurisdictions. Now a federal court with a substantial connection to the suspected criminal activity can issue a single order allowing surveillance that would apply to all providers in the

---

<sup>9</sup> Charles S. Morford, *Eastern District of Michigan Counterterrorism Webpage*, Questions and Answers About the USA PATRIOT Act, August 23, 2004, [http://www.usdoj.gov/usao/mie/ctu/FAQ\\_Patriot.htm](http://www.usdoj.gov/usao/mie/ctu/FAQ_Patriot.htm).

<sup>10</sup> Charles S. Morford, Questions and Answers About the USA PATRIOT Act.

communications chain of a suspect, including those outside the particular court's jurisdiction."<sup>11</sup>

The concern of privacy advocates can be summed up by Jerry Berman of the Center for Democracy and Technology:

"The trouble with the bill is that it's very sweeping and it can apply not just to suspected terrorists but people and organizations that may be engaged in lawful actions."<sup>12</sup>

The USA PATRIOT Act expanded a number of pieces of legislation, including the Wiretap Statute (Title III), Electronic Communications Privacy Act, and Computer Fraud and Abuse Act. The purpose was to expand the authority of law enforcement and intelligence authorities to investigate terrorist's activities, especially in regards to wiretapping, electronic surveillance, and access to stored electronic information. A significant addition is the ability for government authorities to access communications on cable networks (before the act, cable communication was covered under the Cable Act, which made it much more difficult to obtain warrants for wiretaps and surveillance). Also significant is the ability law enforcement and intelligence agencies to share information, whether electronic, wire, or oral. These changes will result in the increase of government monitoring of electronic crime.

## CONCLUSION

As communication technologies continue to progress, the old definitions and concepts have become blurred. We must work to keep them relevant; the concept of privacy was, at one time, inexorably linked to property. In our modern "information age," privacy is becoming linked to security. As technologies becomes more sophisticated, and with that, the criminals and enemies of the state, security will continue to a vital concern. Because of the

---

<sup>11</sup> Alan Charles Raul and Amanda L. Tyler, BNA Electronic Commerce & Law Report, Volume 6 Number 46, The "USA Patriot Act of 2001": Electronic Surveillance and Privacy, November 2001, <http://www.sidley.com/cyberlaw/features/patriot.asp>.

<sup>12</sup> Osen, Stefanie, Patriot Act Draws Privacy Concerns, October 26, 2001, <http://news.com.com/2100-1023-275026.html>.

link, the issues of privacy must also be sorted and acted upon in a relevant and effective way.