SYRACUSE SCIENCE AND TECHNOLOGY LAW REPORTER

PRIVACY LOST: HOW TECHNOLOGY IS ENDANGERING YOUR PRIVACY

By: David H. Holtzman

Citation: DAVID H. HOLTZMAN, PRIVACY LOST: HOW TECHNOLOGY IS ENDANGERING YOUR PRIVACY (Jossey Bass, 2006).

Reviewed by: Catrina Sveum[1]

Relevant Legal & Academic Areas: Constitutional Law, Computer Law, Telecommunications

Summary: This book provides an overview of how advances in technology are eroding individual privacy. It explores the tension between individual civil liberties and national security. In addition to describing new threats to privacy, the book focuses on the inability of the law to protect individual privacy in the face of rapidly advancing technology.

About the Author: David H. Holtzman received a B.A. in Philosophy from the University of Pittsburgh and a B.S. in Computer Science from the University of Maryland. He previously worked as a cryptographic analyst for the Navy and an intelligence analyst for the Defense Special Missile and Astronautics Center.[2] In addition, he has served as a chief technology analyst and a chief scientist. He has worked for presidential campaigns and several organizations as a security and technology advisor. Mr. Holtzman also worked as the Chief Technology Officer for Network Solutions where he was in charge of the domain name system. He currently runs the blog www.GlobalPOV.com.[3]

Chapter 1 – The Seven Sins Against Privacy

- **Chapter Summary:** This chapter provides an overview of the notion of privacy and the ways in which privacy is currently being violated. Holtzman calls these violations "sins."[4] This chapter describes how these sins affect our society on a daily basis and will continue to do so in the future.

---

[1] J.D. Candidate, Syracuse University College of Law, 2008; Form & Accuracy Editor, *Syracuse Science and Technology Law Reporter*.

[2] Biography of David H. Holtzman, *available at* www.davidholtzman.com/biography.html (last visited Nov. 5, 2007).

[3] *Id.*

[4] DAVID. H. HOLTZMAN, PRIVACY LOST: HOW TECHNOLOGY IS ENDANGERING YOUR PRIVACY 3 (Jossey Bass 2006).

- **Chapter Discussion:** Privacy can be hard to define. Thus, there is "equal confusion about what constitutes a privacy violation."[5] Most violations are examined against a legal backdrop, but this is especially difficult when dealing with technology-based privacy violations because the law has not evolved to keep up with the advancing technology. Holtzman sees three different aspects of privacy: seclusion, solitude and self-determination. Privacy involves some degree of control and autonomy, but technology-based violations may usually involve an unprovoked invasion.

  There are seven main "sins" of privacy. The sin of intrusion is the uninvited encroachment on a person's physical or virtual space. Examples of technological intrusion include wire-tapping and concealed cameras. The number of hidden cameras popping up in large cities is growing all the time. In fact, "the average person is caught on a surveillance camera three hundred times a day in London."[6] Radio Frequency Identification Devices (RFID) and Geographic Positioning Systems (GPS) are improving and becoming more accurate. Libraries and the postal service are experimenting with this technology. The Food and Drug Administration (FDA) has even approved the sale of a Verichip, which is an implantable human identification chip. China is currently experimenting with electronic identification cards for its citizens and even new U.S. passports include a RFID.

  The sin of latency involves the hoarding of personal information in the form of electronic data. Many companies that request personal information from online users save that information, sometimes long after their relationship with the user is terminated or

[5] *Id.*

[6] *Id.* at 6.

inactive. Some companies even sell that information. Many consider Google to be a threat to privacy in the future because the website collects a great deal of personal information whenever a user utilizes one of its many products.

The sin of deception occurs when companies ask for personal information on-line, but do not state what they intend to do with it or how long it will be stored. For example, some credit reporting agencies keep that information on file long after the initial qualification. Other companies say they will not sell personal information, but reserve the right to give it to their "partners" who are often not named.[7] Privacy policies are not meant to protect the consumer, they protect the organization.

The sin of profiling occurs when "data derived from raw information is [somehow] mishandled."[8] Personal information is used to profile consumers and place them in certain demographic groups. Some labels placed on consumers can be benign, but others are insulting. Once a label is applied, it is almost impossible for the individual to change that label.

The sin of identity theft has received a great deal of attention in the media. Estimates place the cost of identity-theft losses in the U.S. at about $12 billion a year. Identities can be stolen on-line through phishing scams, where a user receives an email from a bank or other site asking them to update their information. They are directed to a bogus site and asked to enter bank or credit card information, which the phishers receive. As technology

[7] *Id.* at 15.

[8] *Id*. at 17.

advances, so do the scams. Cell phone cloning and "bluesnarfing", where a thief taps into a person's Bluetooth to access information, have also become popular.[9]

The sin of outing occurs as a result of sloppy data handling. Outing refers to "the unwanted connection of an alias to a real identity."[10] Many people create alternate identities for themselves online, sometimes because it allows them to be someone that they could otherwise not be in their personal or professional lives. Outing can also be rationalized because it can involve protecting children from online predators, on sites such as MySpace. Groups like Perverted Justice scour the Internet and set up liaisons with the hope of catching pedophiles and other sex offenders.

The final sin, lost dignity, is the most harmful to individuals and society. This may include the posting of false information about a person online and the surveillance of certain groups, such as felons and even the poor. Governments are experimenting with ways to keep track of the homeless and drug users. Such measures are particularly dangerous because they diminish a person's dignity.

These sins often undermine the benefits of the Internet for individuals and society. Tougher laws are needed to protect against privacy invasions. Holtzman considers the real danger, however, to be corporate abuse because one company can commit thousands of privacy violations.

Chapter 2 – Collateral Damage: The Harm to Society

[9] HOLTZMAN, *supra* note 4,. at 27.

[10] *Id*. at 29.

- **Chapter Summary:** This chapter focuses on how privacy violations affect the society at-large. It discusses how society benefits from a certain degree of privacy. This chapter also looks at how software that labels and segments the population can be damaging to individual reputations.
- **Chapter Discussion:** Privacy violations hurt individuals in a number of different ways. They can even be harmful to society at large. Society benefits from having a secure citizenry, but also one where people are free to share ideas without the fear of privacy being violated. In fact, the recent well-publicized privacy breaches have begun to undermine feelings of security in society.

  The advent of decision-making software is also worrisome. Automated decisions should be subject to human review, but this is becoming difficult as humans know less about how machines make decisions. Creativity and innovation are in danger because individuals may begin to conform to the rules computers have programmed. Labeling by software does not take into account morals, but rather whatever a programmer has decided it should take into account. Labels can be subject to the biases and vagaries of individuals. People are more likely to conform because it is easier than being singled out by surveillance. A lack of privacy can even lead to a society devolving. Finally, privacy is the basis of many other constitutional rights. For example, "in a democracy, privacy makes possible freedom of expression, of choice, of association, of mobility, of thought."[11] Privacy violations in turn endanger these rights.

[11] *Id* .at 54.

Chapter 3 – Technology Affects Privacy: How and Why

- **Chapter Summary:** This chapter looks at the history of privacy and how privacy is closely related to ideas of autonomy and control. It looks at different privacy invasions and how our society has adapted to the violations and even encourages them in some situations.
- **Chapter Discussion:** Privacy also includes some aspect of control and autonomy. Recent advances in technology have diminished this control and the sense of security that comes from this control. Now search techniques are fast and easy. The information cannot be suppressed. Data is more expensive to delete than to store, so a great deal of personal information will continue to be stored in cyberspace regardless of an individual's desire to have it suppressed. Because deletion is expensive, very few companies actually have data-deletion policies.

  Many people have a false sense of internet security. This is the result of internet companies touting new advances in security. Even the U.S. military networks have been hacked. Further, in the era of reality television, invasions of privacy have become entertainment rather than cause for concern. But these technological invasions are still dangerous. Society must create a balance "between the harms and benefits offered by global access to universal information."[12] The invasions will not cease and are likely to become even more intrusive as technology continues to improve.

[12] *Id*. at 69.

Chapter 4 – New Tech, New Crimes: Fresh Wounds

- **Chapter Summary:** This chapter looks at new ways in which privacy is being violated. In particular, it looks at privacy violations on the Internet involving data collection, profiling, digitized pornography and disinformation.
- **Chapter Discussion:** Data collection on the Internet is a huge problem because most websites require users to create accounts. Thus, the danger of privacy invasions increases as we spend more time on the Internet. There is even a danger of people stealing online identities, such as eBay accounts and other online aliases that may be worth something.

  As technology advances, so do other online dangers. Lately, simulated pornography has become a hot button issue. This has been especially embarrassing for some people, as it is possible to graft someone's face on another's nude body. Simulated pornography is especially controversial when dealing with children. The prohibition of child pornography is relatively uncontroversial, but controversy exists when it comes to the possibility of creating a digitized child and placing it in pornography. The Supreme Court struck down provisions of the Child Pornography Prevention Act of 1996 that prohibited the distribution of virtual porn and ruled in 2002 that the material is not "intrinsically related to the sexual abuse of children."[13] The law has not been clear on whether old privacy laws apply to fully digital content.

  Another new crime is that of disinformation, where misleading or inaccurate information shows up on a website. Many websites cannot constantly fact-check. User-generated content, such as that of Wikipedia, has become more popular, but has been used to damage some reputations and to inflate the reputations of others.

[13] Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002).

Profiling software has become important for companies to distinguish between millions of customers. However, this software can be shared with other companies, and the facts that led to a certain label or profile can be lost in the transfer. Labels such as "credit risk" or "person of interest" can be particularly damaging to a person's reputation and psyche.[14]

Chapter 5 – Privacy and the Law: A Right Ahead or Left Behind?

- **Chapter Summary:** This chapter looks at various laws devoted to the protection of privacy. It also argues that privacy cannot simply be protected through legal structures because technology advances much more quickly than the law.
- **Chapter Discussion:** While most Americans seem to think that they are entitled to a certain degree of privacy, "the word privacy doesn't even appear in the U.S. Constitution – not once."[15] A huge problem concerning privacy intrusions is that the law simply cannot keep up in order to protect citizens.

  Justice Brandeis was concerned with privacy and even co-wrote a law review article about the dangers of technology.[16] In the nineteenth century, when the article was written, photography was considered to be the most dangerous technology. Brandeis (along with his co-author Samuel Warren) was concerned that "technology would make it impossible for a prudent individual to protect himself or herself against bad publicity."[17]

[14] HOLTZMAN, *supra* note 4, at 85-86.

[15] *Id.* at 93.

[16] Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV., 193 (1890).

[17] HOLTZMAN, *supra* note 4, at 95.

Appropriation is one privacy violation that hurts individuals. This can be as simple as manipulating a picture of someone. Appropriation statutes have different levels of protection for celebrities and non-celebrities. However, this line has been blurred by the Internet, where it is sometimes difficult to discern who should be considered a celebrity. Intrusion, another tort, has also become more of an issue since the Internet became popular. Generally, intrusion is actionable if "it would be highly offensive to a reasonable person."[18] Courts consider whether a person should have an expectation of privacy. In an age of widespread public surveillance, there is concern that violators may argue "that we have no expectation of privacy anyway and therefore there's no intrusion."[19] As surveillance and other privacy violations increase, the areas in which we may reasonably expect privacy are disappearing as well. The tort of private facts, which punishes the publication of information whose intimate nature would offend a reasonable person, continues to fade in the age of technology. A lot of information is now considered part of the public domain and therefore not actionable. The tort of false light, a tort similar to but less stringent than defamation, is likely to be extended for use against web logs. This possibility has created a debate about whether bloggers should be held to a "higher standard", such as that applied to the traditional press.[20] However, this tort has become harder to define as forums for sharing opinions continue to spring up on the Internet.

[18] *Id.* at 99.

[19] *Id.* at 101.

[20] *Id.* at 107.

Although privacy is not expressly mentioned in the Constitution, liberty has more often been thought to ensure some protection for privacy.[21] The Patriot Act has made it easier for the government to collect information on its citizens, but the Freedom of Information Act (FOIA) has in turn allowed citizens to request access to agency records.[22] The Privacy Act of 1974 was meant to give citizens notice about what information is collected about them, but there are huge exceptions for intelligence and law enforcement.[23] Government agencies have even begun to outsource the collection of data to private companies, thus expanding the risk of privacy violations. Individuals often have little recourse against companies that release or misuse personal information. Privacy policies often do not protect the consumer, but shield the company from liability in the case of a privacy breach. Privacy laws need to be re-examined and punishments for privacy breaches must be more severe so that proper measures are taken to avoid them.

Chapter 6 – Privacy and Identity: The Cult of Me

- **Chapter Summary:** This chapter discusses the phenomenon of on-line culture and aliases. Many people have online personalities that may be different than the personality they have in their professional or personal lives. This chapter looks at how these personas may be at risk for privacy violations.
- **Chapter Discussion:** As discussed before, many people have on-line personas. These may be online gaming profiles, dating profiles or simply email accounts. The possibility of having many different personalities can be freeing. However, it also increases the

[21] *Id.* at 109.

[22] Freedom of Information Act, 5 U.S.C. § 552 (2002).

[23] Privacy Act of 1974, 5 U.S.C. § 552a (1974).

chances of falling victim to privacy violations. It is almost impossible to conduct all online business under one alias.

Also, financial transactions, browsing, and communication require different levels of authentication. For example, financial transactions need authentication. It is almost impossible to conduct any financial transaction online without authentication, although in the future they may be able to be processed anonymously. Browsing, on the other hand, should remain anonymous. Some people benefit from the reputation attached to a particular alias or pseudonym. For example, on eBay, feedback scores allow one to build trust. Individuals have had their eBay accounts hacked simply because they have had a high level of feedback, which can be valuable to scam artists.

Chapter 7 – Privacy and Culture in a Technological World: Shoji Screens

- **Chapter Summary:** This chapter examines the idea of privacy in various cultures. Holtzman argues that one's ideas about personality may be influenced by culture, age and even geographic location. A person's online personality may be very different than their professional personality. Uncovering online personalities may be damaging to a person's reputation and relationships.
- **Chapter Discussion:** There is no clearly defined form of privacy among different cultures. However, privacy can be "more effectively policed by culture than by the law."[24] But ideas about privacy can differ in the same country between urban and rural areas. Likewise, ideas about privacy also differ between generations. For example, younger people are much more likely to use new technology and thus feel less threatened

[24] HOLTZMAN, supra note 4, at 139.

by it. Older people generally have a higher expectation of privacy, whereas Generation X may have few expectations when it comes to privacy simply because the "youngest adult generation grew up with computers."[25]

Chapter 8 – Voyeurism: Surveillance Technology

- **Chapter Summary:** This chapter discusses how technology has made it easier to observe people when they are not aware of it. It examines how technology will continue to become more prevalent and how even internet communications have become more susceptible to surveillance.
- **Chapter Discussion:** New advances in technology, mostly in the form of sensor technology, have made it possible to observe people from greater distances than ever before. Technology has advanced such that computers can sense many things just as well as humans. Almost all cameras are digital now and are getting too small to detect. Cost is no longer a proper deterrent. In fact, "anyone can take thousands of pictures of anyone else for next to nothing."[26] Likewise, cell phones have grown increasingly popular and it is possible to intercept many phone calls through a scanner. Internet communications have also become more susceptible to surveillance through recent laws, especially the Patriot Act.[27] Software used by the National Security Administration is even rumored to be "capable of detecting and breaking most commonly used forms of encryption almost instantaneously."[28]

[25] *Id.* at 144.

[26] *Id*. at 157.

[27] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered titles of U.S.C.).

[28] HOLTZMAN, *supra* note 4, at 165.

Chapter 9 – Stalking: Networks, Tags, and Locators

- **Chapter Summary:** This chapter explores how the risk of privacy violations grows exponentially when it involves networked computers. Some of these technologies are so small or seem so unobtrusive that they can go unnoticed, increasing the risk of privacy intrusion.
- **Chapter Discussion:** Networking increases the risk of privacy violations because it can transfer personal data outside of an individual's direct control. Due to networking, computers can work together rather than having to rely on individual capabilities. Likewise, the use of RFID and GPS technologies relies on networking. As these technologies become less expensive, they will only become more prevalent.

Chapter 10 – Marketing Invasions: Garbos and Greed

- **Chapter Summary:** This chapter discusses how marketers use invasions of privacy to gather information on potential customers. It looks at how individuals can be placed into groups for marketing purposes and how it can be difficult to get out of a group once placed there by sorting technology.
- **Chapter Discussion:** Marketers are constantly creating new methods for reaching potential customers. One way in which this happens is segmentation. Segmenting the population allows marketers to target communication toward a specific audience. This practice actually helps marketers by allowing them to target those people more likely to buy the product.

  Marketers keep huge databases with information on millions of people. This information is often sold by other websites or companies. Marketers have indexes of these databases, sorting people into groups based on common attributes. Marketing companies have even

begun to keep databases with information on children, often "acquiring their birth announcements" or from hospitals that "sell birth records to any company willing to pay the price."[29]

The danger with this data and segmentation is that the data never goes away. This means that marketers can keep profiles of individuals, gathering information from many sources over an entire lifetime. So much intimate personal information can be used that the target feels violated. As advertising on the Internet increases, data collection and profiling will also become more valuable to marketers. Some companies have even experimented with spyware to track customers' on-line browsing and shopping habits.

Chapter 11 – Government Invasions for Security: Mugwumps and Momists

- **Chapter Summary:** This chapter explores how the government is responsible for some privacy invasions and how these invasions are justified in the name of national security. It looks at recent government programs and their effects on individual liberties.
- **Chapter Discussion:** In government matters, privacy often gets side-stepped in favor of security. If the need for certain information is great enough, privacy will generally not be considered in the government's quest for it. There is always a danger that the willingness of citizens to give up privacy for security will be abused by politicians, especially when it is framed as protecting a "higher value [such as] national security."[30]

  Since the Alien and Sedition Acts were passed in 1798, there has been a tension between protecting national security and civil rights. In the modern era, Watergate and even the

[29] *Id.* at 192.

[30] *Id.* at 212.

Patriot Act have shown that even politicians can be guilty of privacy violations. After the 9/11 terrorists attacks, debate has raged over to what extent privacy "as a way of averting future terrorist attacks."[31] While most Americans accept some degree of privacy violation in the name of security, there is no evidence thus far of the effectiveness of profiling procedures at stopping terrorist attacks. There is also no public record of how these procedures work or, for example, how many people are on the government's no-fly list. The Patriot Act even includes measures such as the "library provision," which allows the government to search the records of bookstores and libraries to see who is buying certain reading material.[32] The broad provisions of the Patriot Act have even been used to "fight organized crime…go after pranksters…[and] against the homeless".[33] The recent disclosure of wire-tapping programs further illustrates the tension between privacy and security. It is doubtful that these programs will end up helping more than harming because so many innocent people are targeted everyday.

Chapter 12 – Fighting Back: Gandhis, Curmudgeons, and Vigilantes

- **Chapter Summary:** This chapter discusses who, if anyone, will be able to protect individual privacy. It looks at how various groups including the media, the government, and companies use personal information.
- **Chapter Discussion:** Some have argued that the legislature is in the best position to protect our privacy. However, the legislature represents the people, most of whom do not give privacy much thought on a daily basis. Even laws such as the Health Insurance Portability and Accountability Act (HIPAA) have not really improved or significantly

[31] *Id.* at 215.

[32] 50 U.S.C. § 1861 (2006).

[33] HOLTZMAN, *supra* note 4, at 227.

protected privacy.[34] The executive branch of the government is also not likely to protect privacy because privacy policies may be at odds with other policies on the agenda of the administration. The judiciary seems the most likely to protect privacy; however, it is difficult for laws to keep up with the advancement of technology. Further, most judges are older and may not "really understand technology, and probably never will."[35]

The media is also guilty of privacy violations, often using the First Amendment as justification for invading the privacy of individuals.[36] This is unlikely to change unless the media is "faced with lawsuits and hefty financial penalties."[37] Corporate America might be in the best position to do something about privacy invasions due to extensive lobbying resources, but many companies actually benefit from more access to personal information because they use it for marketing. Therefore, individuals must protect their own privacy by either refusing to give anything but the most vital information or by being vigilant in the fight for privacy.

Chapter 13 – The Panopticon: See the Bars, Rattle the Cage

- **Chapter Summary:** This chapter discusses possible ways to counteract the loss of privacy and the effect of new technology. Holtzman argues that technology will continue to improve, which is necessary to our society, but that a balance must be achieved between the ability of technology and the protection of privacy.

[34] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 29 U.S.C.).

[35] HOLTZMAN, *supra* note 4, at 248.

[36] U.S. CONST. amend. I.

[37] HOLTZMAN, *supra* note 4, at 249.

- **Chapter Discussion:** We have to find a balance between privacy and security. Privacy is necessary for ideas to flow in a democracy. Clearly, too much privacy leaves open the possibility of another terrorist attack. But we must realize that little privacy will be damaging, both to individuals and to the growth of society. We cannot stop marketers and the government from collecting data, but there should be changes in how the data is used and stored to avoid privacy violations. Companies need to be held accountable for large-scale privacy breaches. Privacy violations are inevitable, but must be done in such a way that violations are less invasive to fewer people. Finally, any violation of privacy that is justified as necessary for a higher value such as national security must only be used for that purpose, and even then, in consideration of individual civil liberties.