Privacy 2010

Introduction

Ten years ago, I did a Probe radio program called “Privacy 2000.”{1} At the time, American citizens were concerned about some of the new technological advances and government programs that seemed to be threats to their privacy.

So much has happened in the last ten years. Technological developments have provided individuals, companies, and governments with new tools which could be used to violate our privacy. A war on terror has changed our perception of what is or is not appropriate for government to know about its citizens. In fact, I developed a week of radio programs on “Homeland Security and Privacy.”{2}

One thing I have noticed is that most Americans seem less concerned about intrusions into their lives. Part of it may be due to a resigned assumption that we have to give up some of our privacy to fight the terrorists. But another significant reason, I believe, is a younger generation that seems completely unconcerned with threats to their privacy. After all, many of them are sharing intimate details of the lives on Facebook and MySpace. Why be concerned if companies, the government, or the general public knows details of their lives when they voluntarily share those details on social networks?

This is not to say that all citizens are unconcerned about privacy violations. Recent debates about a national ID card and the collecting and centralization of medical information for government health care programs illustrate that many people are concerned about privacy. But the percentage of citizens concerned about privacy seems to be decreasing.

Privacy is something that most of us take for granted until we lose it. And often we lose our privacy in incremental steps so we are less aware of our increased exposure. Some events can shock us back to reality. Identity theft or the posting of embarrassing information on the Internet can quickly remind us how much privacy we have lost.

We should also make a distinction between privacy and secrecy. Whenever someone expresses concern over a violation of their privacy, another is sure to ask, “What do you have to hide?” The question confuses privacy with secrecy. You may not have anything to hide, but that doesn’t mean that you are willing to have companies collect lots of information about you and then sell it to other companies for a profit. You may not want your future boss to know about a medical procedure that was done twenty years ago. You may not want a telemarketer to have your purchasing history so he can call your mobile phone.

In this article we look at various ways we have lost our privacy. These range from intrusion to deception to profiling to identity theft.

Seven Sins against Privacy: Intrusion

Privacy is a common word but often misunderstood because of it various meanings. We know when we feel that someone have violated our privacy, but we can’t always give a definition to it, especially in this age in which new technology allows perpetrators to cross boundaries more easily than in the past.

David Holzman describes three basic meanings for privacy.{3} They are easy to remember because

they all begin with the letter s. The first is seclusion. That is the right to be hidden from the perceptions of others. The second meaning is solitude. This is the right to be left alone. The third meaning is self-determination, which is the right to control information about oneself.

He suggests that privacy violations can be viewed as seven sins ranging from intrusion to deception to profiling to identity theft. Let's look at each one of these sins against privacy.

Sin of Intrusion – The classical form of privacy abuse is intrusion. This "is the uninvited encroachment on a person's physical or virtual space."{4} In previous ages, it took the form of voyeurism or peeping. Technology today allows for a much great intrusion into our lives and is often much more difficult to detect.

In recent years, we have read about how actors, models, and sportscasters have had their privacy violated by people who placed cameras or listening devices in their rooms or on their person and recorded them. But it isn't just the famous that are being recorded. Every day pictures are being taken of us as we walk into banks, into grocery stores, or past ATM machines. We are being recorded on the streets and at traffic lights. It has been estimated that the average person is caught on surveillance cameras three hundred times a day in London.{5}

And it is not just big brother that is watching and listening to you. Voyeurism technology is available to anyone who wants to purchase it. Stores and Web sites "sell remote listening devices, digital optics, scanners for picking up cell-phone conversations, and even infrared scanners."{6}

Radio Frequency Identification Devices (RFID) act like a wireless bar code and is being used more often in stores and other establishments (such as libraries) for inventory control. Geographic Positioning System (GPS) receivers are satellite locating devices that are found in cars, cell phones, and many other devices.

Intrusion violations have been made easier by technology. In the past, someone had to get near to you in order to spy on you. And that increased the possibility that you would find out that someone is watching you. Now we live in a world where your privacy is being violated, and you are probably not even aware that it is happening.

Seven Sins against Privacy: Latency and Deception

Sin of Latency – Most of the damage to your privacy comes from stored information. The harm is minimized if personal information is not retained. The sin of latency comes from the excessive hoarding of information beyond an agreed-upon time. Most companies do not have a data-aging policy.

It is understandable why companies and the government collect excessive information. First, they need to have enough information so they know they have the right person. There are lots of John Smiths in a particular locality. They need to know you are the particular John Smith they want. In the past, a telephone number was sufficient identification. Now we have more than one phone and change numbers regularly. So our Social Security number and other identifiers are necessary.

A second reason for companies to collect information is so they can more effectively sell their products and services to you. They collect that information from the forms you fill out and even place cookies on your computer in order to catalogue your visits to their Web site.

We might assume that a company would delete your information when you close your account. Most companies merely mark your file as inactive. And many of them sell your information to others. "A

consumer record with up-to-date information is worth around $200 for cell phone information. Social Security information sells for $60 and a student's university class schedule goes for $80."{7}

One of the largest collectors of personal data is Google. When you search for items on the Internet, Google collects that information, and that reservoir of information can begin to paint a picture of your interests, opinions, and worldview. And because Google saves that information for a long time, it can do extensive database matching.

Google was involved in a legal battle with the U.S. Department of Justice that subpoenaed their log files. They wanted to use them to make the case that pornography constitutes a substantial part of Internet searching. A judge ruled that Google needed to only turn over a limited set of information with identifying notations stripped off.{8}

Sin of Deception – With so much electronic information available in databases, it is tempting for individuals, companies, and even bureaucrats to use personal information in a way that was not authorized by the person.

Here are some principles that arise from our discussion so far. When a company or governmental agency asks for personal information we should have the right to know three things: what they are going to do with it, how long they will keep it, and whether they will make it available to others. When we fill out a form for a credit card or enter into a contract for a car or house, we reveal lots of information. We may naively assume that they will be the only ones who will see that information. That is not so. Regularly we see stories in the news about companies selling consumer data to third parties. Most of us would be shocked at how much information about us in the hands of people who have never met or done business with.

Seven Sins against Privacy: Profiling and Identity Theft

Sin of Profiling – Past behavior is not always a perfect predictor of future behavior, but it can be a surprisingly accurate one. That is where profiling comes in. Collecting information about what goods and services someone purchases can enable companies to predict a consumer's future purchases.

Profiling is often used to predict more than that. David Holzman says that he worked with one credit card company that said "it was able to pinpoint when its consumers were having life crises such a mid-life depression by psychographically analyzing their buying patterns."{9}

One of the best known examples of profiling is credit scoring. Equifax, Experian, and TransUnion rely on FICO scores. A high score will help you get a home loan. A low score may result in being denied a home loan and even having to pay higher interest on other forms of credit. Most Americans don't know their credit score (only about two percent), and most do not understand the algorithm used to calculate it.

Profiling is also used to fight terrorism, but have also caught innocent people in their profiling net. For some time my name was on a watch list, and people like columnist Cal Thomas and Senator Ted Kennedy were on a no-fly list.

These mistakes prove an important point: profiling is a guessing game. And sometimes a wrong guess can have a detrimental impact on citizens and consumers.

Sin of Identity Theft – Most of us know what identify theft is because it has happened to someone we know or else we have heard commercials about how to protect ourselves from identity theft. Although this crime did exist in the past, it has exploded on the scene now because of technology

and the changing nature of transactions. Personal information is readily accessible on the Internet. And in the electronic marketplace of today, purchases are not made face-to-face. It is easy for someone to assume your identity and leave you with the consequences.

How easy is it? A New York busboy was caught stealing the identities of people on the Forbes 400 list. He used the Internet to do the research and had been successful in stealing the identities of famous people like Steven Spielberg, Oprah Winfrey, and Ted Turner.{10}

Sometimes all a hacker or thief needs is your Social Security number and your mother's maiden name. Unfortunately it is relatively easy to obtain this information. Universities, banks, and all sorts of institutions use your Social Security number as your identification number. Genealogy files online most likely have your mother's maiden name. Once a theft has that information, he or she is ready to access your financial accounts.

Sometimes we inadvertently give out that information. A phone call from someone pretending to be a bank executive can often elicit confidential information. "Phishing" is a mass e-mail with a message pretending to be a bank or brokerage. People who believe that it is genuine will enter information that the theft can use to drain their bank accounts.

Seven Sins against Privacy: Outing, Lost Dignity

Sin of Outing – Some privacy violations are deliberate and can take place when someone reveals information that another person would like to remain hidden. The term "outing" is usually used to describe a public revelation of a closet homosexual, but we can use the term to describe any information that is published about a person they do not want to be public.

Citizens, politicians, and even corporations have been the targets of Internet messages that have been used to damage their reputation. A number of court cases have attempted to force Web site managers to reveal the identities of those who are spreading false and libelous information.

Sometimes outing is a good thing. Think of all the potential pedophiles that have been caught because they thought they were chatting online with a potential underage victim. Sting operations by the police have successfully revealed the motives of some who intend to proposition their young victims.

Sin of Lost Dignity – This last concern is more difficult to quantify, but we all realize that when private information is made public, we can lose a part of our dignity. What if all of your medical records were made public? What if every essay you ever wrote in school was available online?

Even public figures (like politicians) believe they should have a zone of privacy. Past and current presidents have refused to publish all of their medical records, school records, and other private information. While we may debate whether public figures should reveal all of this information, we would probably all agree that private citizens should not lose a zone of privacy in their lives.

In this article we have talked about how technology allows us to peer into other people's lives. That is why we need to revisit the subject of ethics as it relates to technology that can violate our privacy. We shouldn't use technology to spy on others or to hurt their reputation. Christians should express their concerns about intrusions into their privacy.

This subject also reminds us that we must live our lives above reproach. Philippians 2:14-15 says "Do all things without grumbling or disputing, that you may prove yourselves to be blameless and innocent, children of God above reproach in the midst of a crooked and perverse generation, among

whom you appear as lights in the world." 1 Timothy 3:2 says that an elder must be "above reproach" which is an attribute that should describe all of us. Live a life of integrity and you won't have to be so concerned about what may be made public in age where we are losing our privacy.

Notes

1. Kerby Anderson, "Privacy 2000," Probe Web site, 2000, www.probe.org/privacy-2000/.
2. Kerby Anderson, "Homeland Security and Privacy," Probe Web site, 2003, www.probe.org/homeland-security-and-privacy/.
3. David Holzman, *Privacy Lost: How Technology is Endangering Your Privacy* (San Francisco: Josey-Bass, 2006), 4.
4. Ibid., 5.
5. Ibid., 6.
6. Ibid.
7. Ibid., 10.
8. Ibid., 13.
9. Ibid., 19.
10. Ibid., 23.