DIGITAL CITIZENS ALLIANCE REPORT

GARTH BRUEN: PROTECTING YOUR PRIVACY WEEK

A DIGITAL CITIZENS ALLIANCE SPECIAL REPORT FOR "CHOOSE PRIVACY WEEK"

PROTECTING YOUR PRIVACY WEEK

The Romanian dictator Nicolae Ceausescu was noted for one of the most expansive surveillance regimes in history,[1] with huge swaths of the civilian population employed to spy on the rest, networks of recording devices in public places, pervasive wiretaps, and extensive files on the general population. In the end, this did not prevent Ceausescu from being overthrown and executed in 1989.

In general, mass government surveillance is a failure. The less a government trusts its people, the more likely it is that government will collapse under the strain of having to watch over everyone's shoulder. When discussions of privacy arise, it is often this image of the all-seeing government eye that comes to mind, instilling fear in citizens. But as a practical matter, it simply does not work. Because the government has the authority to seize our property, our freedom, and ultimately, our lives, the idea of the government targeting its own citizens is disconcerting. For the most part, however, this is not where our privacy is under attack.

So where are the threats to privacy coming from? From private companies who collect more information and more effectively use that information in ways the government could never dream of. And there is a third threat: Private individuals such as "hackers" or data thieves use the information collected by governments and private companies for purely illicit purposes to wreck individual lives. Your access and information is not just a weapon against you, but against others.[2] When the government collects my data, I am not so much concerned about what they will use it for; rather I am terrified that they will lose it.

Choose Privacy Week, beginning May 1, is the right time to consider some

[1] http://nyti.ms/13A2lwL

[2] http://tcrn.ch/16SGbgC

of these issues and how to best protect the information you consider most personal.

The discussion of privacy takes many forms, and before it can be tackled, we must set our own limits and expectations. No one can ultimately guarantee a right to privacy; it is up to the individual to manage it. For this same reason, I am reluctant to give out information when I make purchases. The blatant, and almost daily, mismanagement of personal data by public and private entities should shock the public more than wiretaps.

In matters of commerce, we all exchange a piece of our privacy as part of the transaction; just be sure you do not give too much in the deal. When we use credit cards, we are in part financing the ease and access of purchasing by handing over our purchasing behavior to a variety of potential users for more marketing. Consider that companies have always tried to get more information about you; it is good business to do so. The practice is not new, but the tools with which companies gather information are much more effective than ever before. This allows companies to hone in on customers, turning business opportunities into customers. Some people will welcome getting coupons for products needed at a particular moment in life—for example, just before or after the arrival of a child. However, companies have designed algorithms that can detect your new arrival almost before you can—leading to potentially awkward moments for people who aren't ready to share their news with family and friends.

Social media has turned the privacy argument on its head. Most privacy violations in this sphere are self-inflicted. Individuals vomit volumes of intimacies online now. Concepts of social responsibility and self-control have not caught up with the pace of technology. The idea that everyone on the planet can potentially immediately see nude images of yourself taken by your own mobile phone is something humans have simply never had to

contend with ever in the history of civilization until more or less last year. Nothing is new under the sun except the unprecedented level and speed of distribution. Cars and firearms come with training and tests; handheld, personally humiliating media does not. We owe it to our children to impress upon them the responsibility that comes with access to mass communication. This is voluntary privacy abandonment through technology; it is actually easy to control. The non-voluntary data capture is harder to deal with.

Ever wonder why so many things on the Internet are free? They're not. Any website offering something free is getting something in return—your information. Your information is worth infinitely more than whatever they are giving away. If that ringtone, game, or picture is worth your information, then go ahead. Too much spam in your free email? Guess who is responsible. Sure, they have powerful spam filtering…to keep out the competition.

But the consumer has more control over the situation. The variety of services available creates choice; many do not track or sell your email or purchases. You also have the right to ask what your information is used for and to whom it is sold. Pay attention to the news and how it relates to your personal life in terms of which companies openly hand over your personal data. Read your credit card and phone bills in detail. Check your credit record regularly and ask your medical professionals how they protect your information. The individual has a responsibility to protect his or her personal information because no one else will do it for you.

Beyond these methods, changing technology has given the individual the power to "spy back." The rapid availability of public documents, government meeting transcripts, and even live-streamed policy discussion has created opportunities for transparency never before imagined. Public disclosure is now at a level that is even difficult to consume.

And remember that some of the most frequent victims of identity theft are children because they have clean credit records that will likely not be reviewed by their parents until it is too late. Protect their information like it is your own.

With all of this, it is difficult to know where to start; here are ten quick tips:

1. What are you comfortable with people knowing about you? Use this as your yardstick for what you put online or into any public space. Does everyone on the Internet need to know which smoothie bar you are going to?

2. Use cash. Any transaction under ten thousand dollars can be anonymous with cash.

3. Ask why. When someone requests your private data, ask him or her why; ask to see documented policy. For example, RadioShack and other retailers will often request Social Security Numbers (SSN) for Trac or Go phones claiming the manufacturers require them, but when you buy these phones directly from the manufacturer they don't ask for an SSN.

4. Never give any information to people who call you. Obtain a contact number yourself and call back.

5. Even data fragments are dangerous. ATM receipts, printed emails, old utility bills, boarding passes, and a number of seemingly innocuous pieces of paper all contain little parts of your life someone can construct an intimate picture from. Keep and properly dispose of even minor personal documents, anything with your name or account numbers.

6. Use private browsing. Many Internet browsers now have private browsing settings, which do not store tracking information or give out stored data.

This may prevent certain websites from displaying properly, but it can be turned off or on as needed.

7. Don’t talk to strangers. This is advice we give to kids, and it should be obeyed in adulthood. This does not mean we cannot interact with new people, it just means verify who you are talking to and avoid handing over personal details unnecessarily. If you are on a business trip, some friendly stranger who approaches you in the hotel bar could be the competition or just a common thief regardless of their claim to be “attending the conference.”

8. Limit exposure. No one realistically needs ten credit cards or dozens of online accounts. Many purchases can be made online now without creating a new account even if the website wants you to.

9. Lock up and back up your mobile device. Use the desktop software that came with your phone to regularly move data off of it. This will help avoid putting your whole life on the device and prevent a heart attack when your phone is lost. Password-protect it and lock it in your desk when you are not using it.

10. Unplug. Disconnect every once in a while and go truly “wireless.” It can be liberating. Every moment you are not online or on the phone is a moment without free access to your information.

If you want your information to remain private, you have to act in a way that preserves it as much as possible. The novel *1984* is frequently referenced as a cliché of privacy invasion, but anyone who has read the book knows it was ultimately control of the protagonist’s mind that signaled the loss of his humanity. Freedom is not free; it takes courage for any individual to stand up to any invasive tide, and it is in the individual’s discretion how much he or she is willing to exchange in the transaction. You can choose privacy; learn more at **http://chooseprivacyweek.org**.

digitalcitizens alliance

www.digitalcitizensalliance.org