MSNBC.com

Privacy under attack, but does anybody care?

It's vanishing, but there's no consensus on what it is or what should be done

By Bob Sullivan
Technology correspondent
MSNBC

Updated: 4:14 p m ET Oct 17. 2006

Someday a stranger will read your e-mail, rummage through your instant messages without your permission or scan the Web sites you've visited — maybe even find out that you read this story.

You might be spied in a lingerie store by a secret camera or traced using a computer chip in your car, your clothes or your skin.

Perhaps someone will casually glance through your credit card purchases or cell phone bills, or a political consultant might select you for special attention based on personal data purchased from a vendor.

In fact, it's likely some of these things have already happened to you.

Who would watch you without your permission? It might be a spouse, a girlfriend, a marketing company, a boss, a cop or a criminal. Whoever it is, they will see you in a way you never intended to be seen — the 21st century equivalent of being caught naked.

Psychologists tell us boundaries are healthy, that it's important to reveal yourself to friends, family and lovers in stages, at appropriate times. But few boundaries remain. The digital bread crumbs you leave everywhere make it easy for strangers to reconstruct who you are, where you are and what you like. In some cases, a simple Google search can reveal what you think. Like it or not, increasingly we live in a world where you simply cannot keep a secret.

The key question is: Does that matter?

For many Americans, the answer apparently is "no."

When pollsters ask Americans about privacy, most say they are concerned about losing it. An MSNBC.com survey, which will be covered in detail on Tuesday, found an overwhelming pessimism about privacy, with 60 percent of respondents saying they feel their privacy is "slipping away, and that bothers me."

People do and don't care

But people say one thing and do another.

Only a tiny fraction of Americans – 7 percent, according to a recent survey by The Ponemon Institute – change any behaviors in an effort to preserve their privacy. Few people turn down a discount at toll booths to avoid using the EZ-Pass system that can track automobile movements.

And few turn down supermarket loyalty cards. Carnegie Mellon privacy economist Alessandro Acquisti has run a series of tests that reveal people will surrender personal information like Social Security numbers just to get their hands on a measly 50-cents-off coupon.

But woe to the organization that loses a laptop computer containing personal information.

When the Veterans Administration lost a laptop with 26.5 million Social Security numbers on it, the agency felt the lash of righteous indignation from the public and lawmakers alike. So, too, did ChoicePoint, LexisNexis, Bank of America, and other firms that reported in the preceding months that millions of identities had been placed at risk by the loss or theft of personal data

So privacy does matter – at least sometimes. But it's like health: When you have it, you don't notice it. Only when it's gone do you wish you'd done more to protect it.

But protect what? Privacy is an elusive concept. One person's privacy is another person's suppression of free speech and another person's attack on free enterprise and marketing – distinctions we will explore in detail on Wednesday, when comparing privacy in Europe and the United States.

Still, privacy is much more than an academic free speech debate. The word does not appear in the U.S. Constitution, yet the topic spawns endless constitutional arguments. And it is a wide-ranging subject, as much about terrorism as it is about junk mail. Consider the recent headlines that have dealt with just a few of its many aspects:

- Hewlett Packard executives hiring private investigators to spy on employees and journalists.
- Rep. Mark Foley sending innuendo-laden instant messages – a reminder that digital communication lasts forever and that anonymous sources can be unmasked by clever bloggers from just a few electronic clues.
- The federal government allegedly compiling a database of telephone numbers dialed by Americans, and eavesdropping on U.S. callers dialing international calls without obtaining court orders.

Privacy will remain in the headlines in the months to come, as states implement the federal government's Real ID Act, which will effectively create a national identification program by requiring new high-tech standards for driver's licenses and ID cards. We'll examine the implications of this new technological pressure point on privacy on Thursday.

What is privacy?

Most Americans struggle when asked to define privacy. More than 6,500 MSNBC readers tried to do it in our survey. The nearest thing to consensus was this sentiment, appropriately offered by an anonymous reader: "Privacy is to be left alone."

The phrase echoes a famous line penned in 1890 by soon-to-be Supreme Court Justice William Brandeis, the father of the American privacy movement and author of "The Right to Privacy." At the time, however, Brandeis' concern was tabloid journalism rather than Internet cookies, surveillance cameras, no-fly lists and Amazon book suggestions.

As privacy threats multiply, defending this right to be left alone becomes more challenging. How do you know when you are left alone enough? How do you say when it's been taken? How do you measure what's lost? What is the real cost to a person whose Social Security number is in a data-storage device left in the back seat of a taxi?

Perhaps a more important question, Acquisti says, is how do consumers measure the consequences of their privacy choices?

In a standard business transaction, consumers trade money for goods or services. The costs and the benefits are clear. But add privacy to the transaction, and there is really no way to perform a cost-benefit analysis.

If a company offers $1 off a gallon of milk in exchange for a name, address, and phone number, how is the privacy equation calculated? The benefit of surrendering the data is clear, but what is the cost? It might be nothing. It might be an increase in junk mail. It might be identity theft if a hacker steals the data. Or it might end up being the turning point in a divorce case. Did you buy milk for your lactose-intolerant child? Perhaps you're an unfit mother or father.

Unassessable costs

"People can't make intelligent (privacy) choices," Acquisti said. "People realize there could be future costs, but they decide not to focus on those costs.

The simple act of surrendering a telephone number to a store clerk may seem innocuous — so much so that many consumers do it with no questions asked. Yet that one action can set in motion a cascade of silent events, as that data point is acquired, analyzed, categorized, stored and sold over and over again. Future attacks on your privacy may come from anywhere, from anyone with money to purchase that phone number you surrendered.

If you doubt the multiplier effect, consider your e-mail inbox. If it's loaded with spam, it's undoubtedly because at some point in time you unknowingly surrendered your e-mail to the wrong Web site.

Do you think your telephone number or address are handled differently? A cottage industry of small companies with names you've probably never heard of — like Acxiom or Merlin — buy and sell your personal information the way other commodities like corn or cattle futures are bartered.

You may think your cell phone is unlisted, but if you've ever ordered a pizza, it might not be. Merlin is one of many commercial data brokers that advertises sale of unlisted phone numbers compiled from various sources -- including pizza delivery companies.

These unintended, unpredictable consequences that flow from simple actions make privacy issues difficult to grasp, and grapple with.

Privacy's nebulous nature is never more evident than when Congress attempts to legislate solutions to various perceived problems.

Marc Rotenberg, who runs the Electronic Privacy Information Center and is called to testify whenever the House or Senate debates privacy legislation, is often cast as a liberal attacking free markets and free marketing and standing opposite data collection capitalists like ChoicePoint or the security experts at the Department of Homeland Security. He once whimsically referred to privacy advocates like himself as a "data huggers."

Yet the "right to be left alone" is a decidedly conservative -- even Libertarian -- principle. Many Americans would argue their right to be left alone while holding a gun on their doorstep.

In a larger sense, privacy also is often cast as a tale of "Big Brother" -- the government is watching you or a big corporation is watching you. But privacy issues don't necessarily involve large faceless institutions: A spouse takes a casual glance at her husband's Blackberry, a co-worker looks at e-mail over your shoulder or a friend glances at a cell phone text message from the next seat on the bus.

'Nothing to hide'

While very little of this is news to anyone – people are now well aware there are video cameras and Internet cookies everywhere – there is abundant evidence that people live their lives ignorant of the monitoring, assuming a mythical level of privacy. People write e-mails and type instant messages they never expect anyone to see. Just ask Mark Foley or even Bill Gates, whose e-mails

were a cornerstone of the Justice Department's antitrust case against Microsoft.

It took barely a day for a blogger to track down the identity of the congressional page at the center of the Foley controversy. The blogger didn't just find the page's name and e-mail address; he found a series of photographs of the page that had been left online.

Nor do college students heed warnings that their MySpace pages laden with fraternity party photos might one day cost them a job. The roster of people who can't be Googled shrinks every day.

And polls and studies have repeatedly shown that Americans are indifferent to privacy concerns.

The general defense for such indifference is summed up a single phrase: "I have nothing to hide." If you have nothing to hide, why shouldn't the government be able to peek at your phone records, your wife see your e-mail or a company send you junk mail? It's a powerful argument, one that privacy advocates spend considerable time discussing and strategizing over.

It is hard to deny, however, that people behave different when they're being watched. And it is also impossible to deny that Americans are now being watched more than at any time in history.

That's not necessarily a bad thing. Without an instant message evidence trail, would anyone believe a congressional page accusing Rep. Foley of making online advances? And perhaps cameras really do cut down on crime.

No place to hide

But cameras accidentally catch innocents, too. Virginia Shelton, 46, her daughter, Shirley, 16; and a friend, Jennifer Starkey, 17, were all arrested and charged with murder in 2003 because of an out-of-synch ATM camera. Their pictures were flashed in front of a national audience and they spent three weeks in a Maryland jail before it was discovered that the camera was set to the wrong time.

"Better 10 guilty persons escape than one innocent person suffer" is a phrase made famous by British jurist William Blackstone, whose work is often cited as the base of U.S. common law, and is invoked by the U.S. Supreme Court when it wants to discuss a legal point that predates the Constitution.

It is not clear how the world of high-tech surveillance squares with Blackstone's ratio. What would he say about a government that mines databases of telephone calls for evidence that someone might be about to commit a crime? What would an acceptable error rate be?

Rather than having "nothing to hide," author Robert O'Harrow declared two years ago that Americans have "No Place to Hide" in his book of the same name.

"More than ever before, the details about our lives are no longer our own," O'Harrow wrote. "They belong to the companies that collect them, and the government agencies that buy or demand them in the name of keeping us safe."

That may be a trade-off we are willing, even wise, to make. It would be, O'Harrow said, "crazy not to use tech to keep us safer." The terrorists who flew planes into the World Trade Center were on government watch lists, and their attack was successful only because technology wasn't used efficiently.

Time to talk about it

But there is another point in the discussion about which there is little disagreement: The debate over how much privacy we are willing to give up never occurred. When did consumers consent to

give their entire bill-paying histories to credit bureaus, their address histories to a company like ChoicePoint, or their face, flying habits and telephone records to the federal government? It seems our privacy has been slipping away -- 1s and 0s at a time -- while we were busy doing other things.

Our intent in this week-long series is to invite readers into such a debate.

Some might consider the invitation posthumous, delivered only after our privacy has died. Sun's founder and CEO Scott McNealy famously said in 1999 that people "have no privacy – get over it." But privacy is not a currency. It is much more like health or dignity or well-being; a source of anxiety when weak and a source of quiet satisfaction when strong.

Perhaps it's naïve in these dangerous times to believe you can keep secrets anymore – your travels, your e-mail, your purchasing history is readily available to law enforcement officials and others. But everyone has secrets they don't want everyone else to know, and it's never too late to begin a discussion about how Americans' right to privacy can be protected.

URL: http://www.msnbc.msn.com/id/15221095/

Innocent Safety & Guilty Privacy BY: JUSTICE FRANCIS, CAITLIN JACOBS, HANNAH ZHANG Do you agree? Such person or warranty made by the Group (3) deems appropriate evidencing the most recent date as authorized hereunder. The Class of its peers, or other Individuals under the Company also make such duties of the name AND Licensee in regards to this presentation.Â 2016. Sullivan, Bob. "Privacy under Attack, but Does Anybody Care?" Msnbc.com. N.p., 17 Oct. People do and donâ€™t care But people say one thing and do another. Only a tiny fraction of Americans â€“ 7 percent, according to a recent survey by The Ponemon Institute â€“ change any behaviors in an effort to preserve their privacy. Few people turn down a discount at toll booths to avoid using the EZ-Pass system that can track automobile movements.Â When the Veterans Administration lost a laptop with 26.5 million Social Security numbers on it, the agency felt the lash of righteous indignation from the public and lawmakers alike. So, too, did ChoicePoint, LexisNexis, Bank of America, and other firms that reported in the preceding months that millions of identities had been placed at risk by the loss or theft of personal data. So privacy does matter â€“ at least sometimes.