azcentral.com

Email this article **Click to send**
Print this article Choose File Print or Ctrl P or Apple P
Most popular pages **Today** | **This Week**

Watching your every move

Staff reports
May. 13, 2006 01:15 AM

So the National Security Agency has been collecting details on the dialing habits of tens of millions of Americans. The spy agency says it was trying to keep us safe when it embarked on a secret mission to monitor our calling patterns after the Sept. 11, 2001, terrorist attacks.

Fair enough, you say.

But factor in dozens of other types of monitoring done in the name of keeping us safe, making our lives easier and boosting efficiency and you might wonder whether you have any privacy, beyond what your clothing affords.

"We're moving in the direction of having the government turn us into a society that's under constant surveillance," said Alessandra Soler Meetze, executive director of the American Civil Liberties Union of Arizona. Consider:

• Cameras eye you while you drive, bank, shop, eat and sometimes even when you stray into your neighbor's yard.

• Your boss could be monitoring your computer-usage habits, maybe reading your private e-mails. Even the bathroom may not be safe from snoopers.

• Stores keep track of your shopping habits, sometimes sharing the fact that you prefer Crest over Colgate with marketers.

• Applying for a mortgage lays open the full details of your financial, employment and residential history.

The amount of information collected on Americans, much of it readily available and accessible on the Internet, is disturbing, experts say. The databases are ripe for misuse and misinterpretation and are a gold mine for criminals. And the data-gathering grows almost daily.

"We don't have enough privacy laws in place," Soler Meetze said. "So businesses kind of have to step up to do the right thing and make sure this material doesn't get into the wrong hands."

Online gold mine

In the time it takes to read this story, someone could research your entire life.

From where you were born to whom you married, how much you paid for your home to the names of your neighbors, the information is available online.

All it takes is a computer and a few minutes. And it's all perfectly legal.

The kind of background searches that took trained investigators months to conduct a scant 20 years ago now can be achieved in minutes by the teenager next door.

For free, Internet search sites such as Google can help you scroll through phone books across the country in seconds. You can look up someone's Internet address, link to his e-mail, even find a physical address.

For a fee, sometimes as little as a quarter, you can get a fairly accurate financial profile of someone, determine whether he or she has ever sued or been sued and whether they are penny pinchers or mortgaged to the hilt.

Companies such as Lexis Nexis have online subscription services that are used by police, insurance companies, doctors, real estate agents, lenders and even reporters.

They have compiled thousands of pieces of public information from sources as diverse as local courthouses to Departments of Motor Vehicles.

In most cases, locating people and getting a picture of how they live requires only a last name and a vague notion of where they once lived.

For instance, a basic computer search through some Internet sites will allow you to look at possible addresses, Social Security numbers and phone numbers for any given last name. The cost: two bits.

Cameras everywhere

If it's not bad enough that someone you've never met could research your entire life, how about knowing that someone you've never met could be watching you?

If you speed on certain streets or one stretch of Loop 101, traffic cameras will snap your photo. Even if you're not speeding, state Department of Transportation cameras often pick you up when you're driving to work.

Surveillance cameras eye you at the ATM, the mall, casinos, in certain parking lots.

Is this good or bad?

Maybe a little of both, said Rosemarie Urbanski, executive vice president of the Drake Group, an Arizona private investigation firm that specializes in countersurveillance.

What with terrorism threats, concerns about personal safety and the fact that police can't be everywhere, cameras are proliferating, she said.

She favors using electronic eyes to make public areas safer. But she acknowledged that in the interest of law and order, privacy is decreasing.

"It's a Catch-22," she said. "In order to get more security, you're giving up some of your personal freedoms."

Some people would like to push the envelope even further.

Former Phoenix Police Chief Harold Hurtt, who now heads the Houston Police Department, suggested recently that crime-fighting in Houston could be enhanced with surveillance cameras in apartment complexes, on downtown streets and in private homes.

"I know a lot of people are concerned about 'Big Brother,' " Hurtt told reporters at a briefing in Houston, "but my response to that is if you are not doing anything wrong, why should you worry about it?"

You should worry, Soler Meetze said, because your privacy rights are being eroded.

People need to know just how intrusive such cameras are. For instance, in addition to recording video images, are they recording the sounds of private conversations? Are they so powerful that they show what people are reading?

"We need to make sure before we install these cameras that we have in place privacy protections," she said.

Private business owners who put up cameras should also act responsibly. For instance, she said, they should not eavesdrop on private conversations and should destroy the videotapes when they no longer serve a business purpose.

People willingly disclose more personal information when they get a home loan than almost any other time.

Loan documents start with a borrower's Social Security number and then go on to ask for credit-card numbers, tax records, past addresses, maiden name and names of relatives.

It would be easy for the NSA, or others, to use that information to compile profiles of people, including details of other previous residences and their spending habits.

"Many people buying a home just hand over their Social Security number. They don't think about everyone who sees it and can track down almost all of their other personal information with it," said Jay Butler, director of the Arizona Real Estate Center at Arizona State University's Polytechnic.

He said lenders don't necessarily need all the information they ask for, either.

Electronic files breached

Banks, brokerages, mutual-fund companies and other financial outfits have plenty of incentive to safeguard sensitive customer records. Regulators require careful supervision of data. But in addition, sound business practices make safety a viable strategy.

That doesn't mean, though, that records are completely safe. Electronic files have been breached.

Over the years, various federal privacy acts have forced financial firms to take security more seriously.

"It's more important to safeguard the information because banks are obligated by law to collect more information from customers (to comply with the Patriot Act)," said Michael Beird, senior director of retail banking at Cornerstone Advisors, a Scottsdale consulting firm.

As online financial commerce explodes, banks and investment firms also have had

to increase their vigilance while allaying consumer fears.

It is rare for banks to distribute customer records to third parties, Beird said, but this doesn't mean all of your financial records are off-limits. Credit reports are routinely accessed by actual and prospective lenders.

Credit-card firms obtain consumer credit reports to find suitable prospects to pitch pre-approved card offers. When you voluntarily apply for car loans, mortgages and so on, your credit scores and the credit reports on which they're based come into play.

Privacy at work

If you work for someone else, check your expectations for privacy at the office door.

"Any piece of property that is owned by your employers, and not by you, they would have the right to access it," said Amy Jantz, a manager for WorldatWork, a Scottsdale-based professional human-resources firm.

That extends from such everyday equipment as phones and computers to more personal items, such as lockers.

As long as employers put their staff members on notice about their privacy policy, they're basically protected against claims that they have violated a worker's privacy, said Jon Pettibone, a labor and employment-law attorney with Quarles & Brady.

There are a few obvious exceptions, which Pettibone describes as falling within the "reasonable-person standard." These include expecting privacy in the company washroom, although even there, a notice to employees about, say, surveillance would pre-empt privacy complaints, he said.

Jantz said most workers probably don't know that they accepted their employer's privacy policies when they hired on.

Cradle to grave

"You might not realize it at the time because you were signing a kazillion forms," Jantz said.

We are watched from cradle to grave.

Enormous national database cabinets store information on people who use shopping-club cards, memberships and credit cards.

They, those invisible marketers, know whether we're buying infant Tylenol, six-packs of Heineken or a pregnancy test. That information is sometimes sold to telemarketers who find and court us.

We also may gift our informational DNA to people we'll never meet by:

• Filling out questionnaires and sweepstakes for a discount or free gift.

• Sending e-mails and logging onto Web sites. (Each computer has an Internet Protocol address, similar to a telephone number, which allows your Internet service

provider to store information about your activity.)

• Using our cellphones, some of which have Global Positioning System chips that allow our whereabouts to be tracked if, for example, we call 911.

• Calling 800, 866, 888 or 900 numbers. When calling, these numbers can be recorded by a system called Automatic Number Identification and then sold to marketers for mail and phone solicitations.

Data to the NSA

Some consumer advocates say businesses are too easily turning over the private data of their customers to not only other businesses but also to such entities as the NSA.

"We as Americans are giving out a lot of personal information every day," said Mark Cooper, director of research at Washington, D.C.-based Consumer Federation of America. "Who is guarding it? We should have been asking these questions long before now."

Reporters Robert Anglen, Sonja Haller, Charles Kelly, Mary Jo Pitzl, Catherine Reagor and Russ Wiles contributed to this article.

Email this article **Click to send**
Print this article Choose File Print or Ctrl P or Apple P
Most popular pages **Today** | **This Week**