



Technology's watchful conveniences

—by Ellen Nakashima

The tracking begins shortly after we wake up. All through the day, from walking out of our houses to go to work, to e-mailing friends and shopping and working, the watchful eye of technology records our movements and preferences. Welcome to the 21st century.

Like many Americans, Kitty Bernard, a 56-year-old real estate agent, uses modern gadgets to make life easier, and along the way she creates a data trail that others can access and preserve, sometimes permanently. Every Internet search resides on a computer somewhere. Comings and goings are monitored by security cameras. Phone calls are logged by telecommunications companies.

This explosion in data collection has been embraced by many Americans as a trade-off for convenience and discounts. But it also has raised questions about personal privacy at a time when the government is increasingly tapping into these reservoirs of telling details to fight crime and terrorism.

The new Congress began to examine the uses and abuses of data gathering for security and commerce early in 2007. A look at Bernard's activity one recent day helps to illustrate what they're likely to find: that ordinary Americans leave a trail of digital data that are being gathered, stored, and analyzed, and that these people seldom realize it.

6:15 a.m.

Bernard, who is married and has a grandson, pads into the lobby of her Reston condo complex on the way to the

building's gym, and almost no one else is about. But a security camera records her. If the government or a divorce lawyer wants the tapes, they can subpoena them.

7:17 a.m.

Bernard returns to her condo after her workout, nestles into a bedroom love seat and fires up her laptop to check e-mail. She opens a few, deletes 38 more—junk mail from Weight Watchers, a personal trainer, a firm that sells art posters. The U.S. government claims that even before she's opened them, it should have the right to read them if it needs to. The technology exists to do that.

Bernard is not only trackable, but she is a tracker. She says it helps her be a better real estate agent. Through a Web-based notification service, she can see what homes her clients are interested in as well as copies of e-mails sent to new clients who register on her Web site, KittyBernard.com. "I can e-mail them and say, 'I see you've been on my Web site.'"

8:30 a.m.

She takes a cellphone call from her daughter. After a brief chat, she hangs up. But her cellphone is still sending its ID signals to the nearest cellular towers, giving her phone company her approximate location. Approximate, but precise enough that the FBI has used such information to locate suspects, and marketers are contemplating using it for targeted cellphone advertising pitches by text message.



8:35 a.m.

Bernard pulls into an Exxon Mobil gas station. She holds a small wand called a Speedpass to a sensor at the gas pump. The gadget uses radio frequency identification (RFID) waves to charge her Exxon Mobil account directly. No cash. No card swipe.

RFID chips are being placed in credit cards, passports and items on store shelves. Some people have even had chips injected into their bodies so emergency room doctors can have instant access to their medical records. The chips can track, conduct transactions, and, in some cases, be hacked. They transmit information to private databases.

Civil libertarians fear that one day soon this will mean a retailer could recognize Bernard as soon as she walks in the door, even before she identifies herself, or that data brokers could track how many times she entered a bar, even if she paid cash.

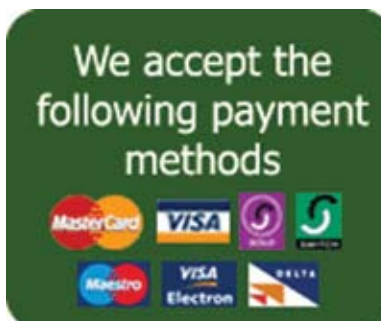
By default, Exxon Mobil has the right to share her name and other information it collects on her with "consumer reporting agencies, banks, insurance companies, retailers, publishers and direct marketers"—unless Bernard "opts out." But she has never done so. Such information is often buried in the privacy policies sent in the mail or posted on retail Web sites that Bernard never bothers to read. "I don't know anyone who's read them," she says.

8:40 a.m.

Bernard enters her Coldwell Banker office building and is recorded by a hidden security camera.

10:25 a.m.

She logs on to Top Producer, Web-based software for real estate agents, which allows Bernard to retrieve notes



on her clients wherever she has access to the Internet. She can look up clients' birthdays and home-buying anniversaries, lending a personal touch to her service.

The trend toward Web-based computing means that reams of data Bernard and others used to keep in notebooks are now stored on servers owned by private companies, where the data are potentially vulnerable to hackers and potentially accessible to government authorities.

11:05 a.m.

She dials Domino's for pizza. Domino's tracks her name, phone number, address, and size and type of pizza ordered. Unless a store decides otherwise, the data are held forever.



That way, Domino's can provide more personalized service—"Hi, Ms. Bernard, would you like your regular—mushroom and sausage?"

Domino's, which hopes to have a national database of customers soon, says it does not share or sell customer information. But companies that specialize in providing unlisted and cellphone numbers, among other records, often buy phone numbers from pizza delivery services, according to Merlin Information Services, a data broker.

12:30 p.m.

Bernard gets back in her car, a 2003 Mercedes-Benz with navigation and roadside emergency service. She turns the key in the ignition, activating a Global Positioning System device that uses satellites to pinpoint her location and is constantly sending out signals.

GPS technology allows her to map out a route and find streets and landmarks, restaurants, and hotels. She can use a CD, which displays on a dashboard screen, or push a button and connect to a roadside assistance call center run by the Texas telematics firm ATX to guide her if she's lost or call her a tow truck.

GPS generates a record of her travels, though ATX says it does not keep such location records now. The company stores emergency call records — location, time, nature of call—for billing and other purposes.

12:35 p.m.

Bernard pulls up to a tollbooth on the Dulles Toll Road. A Smart Tag on her front license plate communicates with a sensor and pays her toll. A light flashes green. Over the long run, Bernard has saved hours by using her Smart Tag, with its RFID chip, to zip through tollbooths.

The Virginia Department of Transportation records the date and time she passed, the toll location, the amount paid, and her customer account information. The FBI has used this type of information to help solve murder cases, and private attorneys have used it in divorce cases.

As Bernard passes the tollbooth, two cameras record her—one in front of her car and one in back.

2:10 p.m.

Bernard enters Costco. She wheels her cart to a cashier and uses her Costco membership card, which is linked to an American Express card, to buy bottled drinks and bagged candy. She likes the credit voucher she will get at year's end, worth one percent of her total purchases, thanks to her Costco membership.

Costco likes its database of 50 million shoppers' purchase histories, e-mail addresses, and phone numbers, which it can use to notify consumers of a product recall or do marketing research. Bernard's credit card companies know her income and her shopping habits. They can share her information with affiliates without her permission and need not stop even if she asks them to.

Credit bureaus maintain gigantic databases on consumers such as Bernard fed by tens of thousands of banks, auto lenders, credit card issuers, state welfare agencies, utility companies and court records.

3:25 p.m.

Bernard visits BestBuy.com to look for a CD case. Best Buy receives good ratings from customers on privacy, according to the Ponemon Institute, a privacy research group. But online retailers in general are a prime target for people who call the retailer pretending to be a customer to obtain passwords and other personal information that they then use to access online bank accounts. This practice, known as pretexting, is also done by fly-by-night data brokers who collect and sell phone numbers and other personal data.

4:15 p.m.

Bernard enters Belmont Country Club, a planned community in Loudoun County, to show a client a house. Two cameras record her car entering. Residents can tune their TV sets to the security channel and see who's at the gate. Bernard inserts an electronic key—which looks like a pager—into a black rectangular lockbox, and a real key drops out.

The e-key uses an infrared beam to transmit the date and time, her name and phone number, and her company name to the lockbox. The lockbox, itself





an electronic device, beams to the e-key a number linked to the house address. The information is kept by GE Security, which puts it on a Web site for real estate professionals who want to check the last three months of activity. The firm stores the data for years— just in case an agent needs it to, for instance, help settle a civil dispute.

5 p.m.

Bernard, back in her car, presses a button for a concierge service. She wants to make a dinner reservation. "I'm speaking with Mrs. Bernard?" says Denise, her concierge. "Fan-tastic." The service, run by VIP Desk of Alexandria, can book hotel stays, set up scuba lessons and even find a pet sitter. Today, Denise reserves a table for Bernard and her husband, John Emert, at Legal Sea Foods in Tysons II Galleria mall.

VIP Desk serves millions of customers and keeps large amounts of data that can be customized for its corporate clients, which include credit card companies and travel companies.

5:20 p.m.

Back in her office, Bernard does a Google search on a coffee maker because she can't remember the model's exact name. "Tazzimo," she types. "Tazzamo," then "Tazmo." Finally, she types in "coffee makers" and gets a link to Amazon.com. She clicks on the link. "There it is!

Braun Tassimo," she says.

Google collects billions of search queries a month typed in by users such as Bernard, creating one of the largest databases of online behavioral data in the world. Google uses this data on an aggregate level for research purposes, such as refining its search engine, or to see how many people are clicking on ads so that Google can bill the advertisers. Google targets ads to users based on the search terms they use and can target ads by geography.

6:45 p.m.

Bernard and her husband enter the mall. They are heading to Legal Sea Foods. Security cameras record their passage.

9:00 p.m.

Bernard and Emert return from dinner and shopping, using an RFID key fob to enter the building. A camera again records them.

9:05 p.m.

She logs on to her laptop again, seeing only a few e-mails. After watching a little television with her husband, she'll head to bed about 11 pm—time for a shut-eye.

No one is forcing Bernard to embrace this technology. She loves the time she gains by paying road tolls electronically, the sense of security she feels by having GPS in her car. She

sometimes buys real estate client lists so she can target categories of buyers—seniors or first-time home buyers— "as long as it's not intrusive," she said.

Who's to say what's intrusive at a time when teenagers are baring their souls on Web sites? When people are taking video of routine and shocking events alike and putting them on the Web? When patients' health records are being scanned into giant databases? Much of these data—voice, video, text—are not being analyzed, at least not on a systematic basis. But the government is seeking ways to effectively do so, for law enforcement and security.

These caches of data will only continue to grow, with storage cheap and tens of millions of people like Bernard eager to get in on the digital revolution, sending messages and conducting transactions with an ease futurists once only dreamed of.

In just one day, Bernard paid eight tolls electronically. She used her credit card four times and sent 20 e-mails. She passed before security cameras at least 50 times. "Amazing," she said in a follow-up interview. "It's astounding to think that my whereabouts and activities can be tracked by any number of companies and individuals."

But, she said, she's not inclined to change her ways. Bernard said she already takes measures to guard her privacy. She saves intimate details for phone calls. She's on a do-not-call telemarketing list. She trusts her company to keep her office system hacker-free. For the most part, she trusts that the government will not be interested in her personal life—hoping for security through obscurity. As most of us probably do.



In this article: Security camera (p. 31). On page 32, speed pass (www.exonmobil.com), Ranger vehicle GPS tracking and map (www.ggsmark.com), phone gizmo (<http://roscoctagelane.blogspot>), electronic key (<http://pro.corbis.com>), "plastic money." On page 33, e-mail services, key fob (www.slipperybrick.com), and smart tag (<http://oneduasam.files.wordpress.com>). On page 34, America's most (e-mail) addicted (<http://gigaom.files.wordpress.com>), smart tag (www.coolmarketingthoughts.com).