The Anonymity Experiment

Aaron Goodman

During a week of attempting to cloak every aspect of daily life, our correspondent found that in an information age, leaving no trace is nearly impossible

In 2006, David Holtzman decided to do an experiment. Holtzman, a security consultant and former intelligence analyst, was working on a book about privacy, and he wanted to see how much he could find out about himself from sources available to any tenacious stalker. So he did background checks. He pulled his credit file. He looked at Amazon.com transactions and his credit-card and telephone bills. He got his DNA analyzed and kept a log of all the people he called and e-mailed, along with the Web sites he visited. When he put the information together, he was able to discover so much about himself—from detailed financial information to the fact that he was circumcised—that his publisher, concerned about his privacy, didn't let him include it all in the book.

I'm no intelligence analyst, but stories like Holtzman's freak me out. So do statistics like this one: Last year, 127 million sensitive electronic and paper records (those containing Social Security numbers and the like) were hacked or lost—a nearly 650 percent increase in data breaches from the previous year. Also last year, news broke that hackers had stolen somewhere between 45 million and 94 million credit- and

debit-card numbers from the databases of the retail company TJX, in one of the biggest data breaches in history.

Last November, the British government admitted losing computer discs containing personal data for 25 million people, which is almost half the country's population. Meanwhile, some privacy advocates worry that the looming merger between Google and the Internet ad company DoubleClick presages an era in which corporations regularly eavesdrop on our e-mail and phone calls so they can personalize ads with creepy precision. Facebook's ill-fated Beacon feature, which notifies users when their friends buy things from Facebook affiliates, shows that in the information age, even our shopping habits are fit for public broadcast. Facebook made Beacon an opt-in service after outraged users demanded it do so, but the company didn't drop it completely.

Then we have Donald Kerr, the principal deputy director of National Intelligence, who proclaimed in a speech last October that "protecting anonymity isn't a fight that can be won." Privacy-minded people have long warned of a world in which an individual's every action leaves a trace, in which corporations and governments can peer at will into your life with a few keystrokes on a computer. Now one of the people in charge of information-gathering for the U.S. government says, essentially, that such a world has arrived.

So when this magazine suggested I try my own privacy experiment, I eagerly agreed. We decided that I would spend a week trying to be as anonymous as possible while still living a normal life. I would attempt what many believe is now impossible: to hide in plain sight.

A Gallup poll of approximately 1,000 Americans taken in February 1999 found that 70 percent of them believed that the Constitution "guarantees citizens the right to privacy." Wrong. The Constitution doesn't even contain the word. And in a fully wired world, that's an unnerving fact.

A number of amendments protect privacy implicitly, as do certain state and federal laws, the most significant of which is the Privacy Act of 1974, which prohibits disclosure of some federal records that contain information about individuals (1). Unfortunately, the law is full of exceptions. As Beth Givens, founder and director of the nonprofit Privacy Rights Clearinghouse, put it, the Privacy Act has "so many limitations that it can barely be called a privacy act with a straight face."

Notes:

1. California, where I live, leads the nation in privacy protection. If I'd conducted my experiment elsewhere in the U.S., it would have been even more difficult

In the U.S., privacy law is sectoral, which means that we don't have broad, generally applicable laws to protect our personal information. We've got federal laws that safeguard very specific types of data, like student records, credit reports and DVD rentals. But those have loopholes too **(2)**.

In addition, technological advances are quickly rendering many of these laws useless. What good is strong protection for cable records when a technology like TiVo comes along that is not, technically, a "cable service provider" **(3)**? Or a statute about postal mail in a world where most communication now takes place online? "We're way behind the curve," says Richard Purcell, CEO of the Corporate Privacy Group and former chief privacy officer for Microsoft. "Technology is way ahead of our ability as a society to think about the consequences."

Navigating this technological and legal maze wouldn't be easy; I needed professional help, a privacy guru who could guide me through my week. That man was Chris Jay Hoofnagle, a privacy expert and lawyer who used to run the West Coast office of the Electronic Privacy Information Center (EPIC), a public-interest research center in Washington, D.C., that focuses on privacy and civil-liberties issues.

Hoofnagle had tried his own version of the same thing, partly for fun and partly because of fears of retribution from private investigators he had irritated in his previous job at EPIC. "When moving to San Francisco two years ago, I deliberately gave my new address to no business or government entity," he told me. "As a result, no one really knows where I live." His bills are in aliases, and despite setbacks—like having his power turned off because the company didn't know where to send the statement—he's been successful at concealing his home address.

Now that he's a senior fellow at the University of California at Berkeley's Boalt Hall School of Law, Hoofnagle doesn't keep his office location a secret, so on a sunny afternoon, I set off to meet him there.

Tall and friendly, Hoofnagle has an enthusiastic way of talking about privacy violations that could best be described as "cheerful outrage." He laid out my basic tasks: Pay for everything in cash. Don't use my regular cellphone, landline or e-mail account. Use an anonymizing service to mask my Web surfing. Stay away from government buildings and airports (too many surveillance cameras), and wear a hat and sunglasses to foil cameras I can't avoid. Don't use automatic toll lanes.

Get a confetti-cut paper shredder for sensitive documents and junk mail. Sign up for the national do-not-call registry (ignoring, if you can, the irony of revealing your phone number and e-mail address to prevent people from contacting you), and opt out of prescreened credit offers. Don't buy a plane ticket, rent a car, get married, have a baby, purchase land, start a business, go to a casino, use a supermarket loyalty card, or buy nasal decongestant **(4)**. By the time I left Hoofnagle's office, a week was beginning to sound like a very long time.

Notes:

2. One oft-cited loophole is in the Driver's Privacy Protection Act of 1994. It was created after a series of crimes linked to Department of Motor Vehicles records, the most notorious of which occurred in 1989: An obsessed fan hired a private investigator to get actress Rebecca Schaeffer's home address from her DMV record and then tracked her down and killed her. Now DMV employees aren't allowed to release personal information. The only problem is that the law has 14 exemptions, including one that allows the release of information to licensed private investigators if they say they're using it for purposes listed in the other 13 exemptions.

3. TiVo actually has a strict privacy policy—but it's the company's own doing. Legally, it's allowed to sell a minute-by-minute record of users' viewing habits.

4. Pseudoephedrine can be used to make methamphetamine, and thanks to a federal law passed in 2006, your name goes into a log when you buy products that contain it.

Automatic Teller: • Banks sell lists of information that you'd think would be kept private—transaction histories, bank balances, where you've sent payments—and can continue to do so even if your account is closed. Aaron Goodman

After withdrawing seven days' worth of cash, I officially began my experiment by attempting to buy an anonymous cellphone. This was a crucial step. My cellphone company keeps records of every call I make and receive. What's more, my phone itself can give away my location. Since 1999, the Federal Communications Commission has required that all new cellphones in the U.S. use some form of locating technology that makes it possible to find them within 1,000 feet 95 percent of

the time; the technology works as long as your phone is on, even if it isn't being used. This is to help 911 responders locate you, but the applications are expanding. Advertisers hope to use cellphone GPS to send text-message coupons to lure you into stores as you pass by, and services such as Loopt and Buddy Beacon allow you to see a map of where your friends are, in real time, using either their cellphone signals or GPS (5). I left an outgoing message explaining that I wasn't going to be using my normal cellphone for a week and then turned it off.

Wearing a baseball cap and sunglasses, I walked into an AT&T store and immediately noticed several black half-globes suspended from the ceiling: surveillance cameras. I needed to keep my head down. When I tried to pay for my new phone, the cashier swiped its bar code, looked up at me with her fingers poised above her keyboard, and asked me for identification. "I don't have any on me," I lied.

She seemed mildly annoyed and asked for my name and address.

"I'm sorry," I said, "but I don't really want my information in the system."

"We need your information."

"Why?"

"For billing purposes."

"But it's a prepaid card. You don't need to bill me."

This, apparently, was irrelevant. "We need to put your information into the system," she said again. "Otherwise you can't buy the phone."

I didn't buy the phone. Instead I walked across the street to a generic cellphone store where a young clerk with pink hair and black-framed glasses was sitting behind the cash register, text messaging. "So do you want me to, like, just put in some random name?" she asked.

Before I knew it, she'd christened me Mike Smith, born October 18, 2007 (6). As she charged minutes to my phone, I overheard a young man next to me tell a different clerk that he wanted to activate a cellphone that was registered under his mother's name. "That's no problem at all," said the clerk. "We just need her Social Security number." Unfazed, the man called his mom. He was dictating the number to the clerk as Mike Smith walked out the door.

Notes:

5. These services are voluntary, but they vividly illustrate the privacy-killing potential of cellphone GPS.

6. She'd asked for my birth date to use as an activation code, but it turned out she really just needed any eight-digit series of numbers

My new phone was anonymous, but I still needed to be careful. If I didn't want it to be traceable back to me, I had to disguise my outgoing calls and minimize the number of calls that I received; records of both could be used to identify me. I changed the phone's settings so that its number wouldn't show up when I placed calls (7) and bought a prepaid calling card to use on top of my cellphone. That way, if anyone were to pull a record of my outgoing calls, they would just see the calling-card number.

If masking your cellphone number is difficult, hiding your online activity is nearly impossible. Anytime you access the Internet, your Internet service provider (ISP) knows you're online, and it might soon keep track of more. In 2005, the European Parliament passed legislation requiring phone and Internet providers to retain records of calls and online activity for between six months and two years. In 2006, then–U.S. attorney general Alberto Gonzales and FBI director Robert Mueller met privately with America's major ISPs to request that they, too, hold on to these records for two years. Search engines already keep records of queries, a practice that's become enough of a concern among users that in December, Ask.com launched AskEraser, a service that deletes your searches within hours. When you send an unencrypted e-mail, it can be intercepted and read and may be stored indefinitely on a server, even if you've deleted it. And Web sites routinely retain such information as how you got there, how long you lingered on each page, and your scrolling, clicks and mouse-overs.

Masking on the Web: If masking your cellphone number is difficult, hiding your online activity is nearly impossible. Aaron Goodman

But I'm getting ahead of myself. My first challenge was to figure out how to connect to the Internet. I subscribed to Anonymizer, a service that uses a technique called secure-shell tunneling to create a virtual link between your computer and Anonymizer's proxy servers (that is, the servers that act as middlemen between your computer and the sites you're visiting). That meant my ISP wouldn't know what Web sites I was visiting, and the sites I visited wouldn't know it was me.

Anonymizer has two potential weaknesses, though. First, Anonymizer itself knows what sites you're visiting, although the company claims not to retain this information. And then there's the conspiracy theory. "There are reports that the government has sneakily had people volunteer to run Anonymizer server nodes who are actually "quislings"—traitors—Holtzman told me. "I don't know if it's true," he said. "But if it were my job to spy on people, I'd be doing it."

There are Anonymizer alternatives (the freeware Tor is probably the best-known), but according to Holtzman, if you want to be sure of anonymity, "you just cannot use your own computer. The only way to do so is if it's brand-new and you never put it online." Unfortunately, I didn't have a brand-new computer, and I needed to use the Internet. I decided to avoid using my own ISP whenever possible. Instead I needed to either piggyback on neighbors' open connections or use public Wi-Fi hotspots (8).

Once I got online, I had other challenges, such as the notorious "cookie," a small text file that Web sites leave on your computer so that you can be identified when you

return. Cookies often make the Internet easier to use; they remember your login name, for example, and some sites now deny access to visitors who refuse cookies. But if you want to remain anonymous online, you've got to toss your cookies. When I looked through my cookie cache, I found them from all sorts of places, including one from a site called Vegan Porn (it's not as naughty as it sounds) and another, from Budget Rent A Car, that wasn't set to expire until 2075.

Lastly, there was the question of e-mail. I set my usual address to forward to a Hotmail account I'd created with fake user information and signed up for a free account through Hushmail, a service that allows you to send encrypted, anonymous e-mail. I figured that if I monitored my messages through Hotmail but responded using only Hushmail, no one would be able to connect the two accounts—or know definitively that the person checking the Hotmail was me. Only later did I discover that even Hushmail has occasionally spilled information to the feds.

Notes:

7. Because of something called "automatic number identification," there's no way to stop your information from showing up when you call toll-free or 900 numbers.

8. Even then, I still wouldn't be entirely anonymous. Every networking device in every computer is assigned a media access control (MAC) address, a unique identifying number picked up by your router when you go online. See this website to learn how to find your MAC address.

I started marking items off Hoofnagle's to-do list. I signed up for the do-not-call registry to avoid telemarketers and sent a letter opting out of all prescreened offers of credit. I called my bank and opted out of its information sharing (9). Then I called my phone company and told them I didn't want them to share my CPNI—customer proprietary network information.

Your CPNI includes records of what services you use, what types of calls you make, when you place them, and a log of the numbers you've called. Before 1996, phone companies were allowed to freely sell this information to third parties for marketing purposes. Today, thanks to legislation limiting what they can do without your permission, CPNI is mainly used to sell you other services offered by your phone company, such as a new long-distance plan.

When my phone company's automated system picked up, a voice announced that my call might be monitored or recorded but that I could ask to be on an unrecorded

line. So I did. “Uh, OK,” the representative said. “But all the lines are recorded automatically. If you don’t want to be recorded, I’m going to have to call you back.”

“How long will that take?” I asked, having already spent 10 minutes on hold.

“We’ll call you as soon as we have a chance,” he said. “Probably within an hour.” In other words, the cost of privacy would be an hour of my time.

I told him that a recorded line was fine and then asked him to stop using my CPNI to market things to me. He agreed. Then he asked if I had a few minutes to talk about my phone service and proceeded to use my CPNI to try to sell me a unified messaging system.

This was getting exhausting. I’d thought a yoga class would be a nice break, but I’d forgotten one thing: The yoga studio I go to has a computer system that keeps track of all its students’ names. I scrawled “CPrice” illegibly on the sign-in sheet and paid in cash. I thought I’d gotten away with my ploy until the end of class when, just after our final “om,” the teacher picked up a piece of paper that the front desk had slipped under the door. “Would whomever signed in as number 19 please stop by the front on the way out?” he asked. “They couldn’t read your signature.”

I doubt the young Buddhists behind the yoga-studio desk are profit-minded enough to sell my personal information, but many other businesses are. Data-broker Web sites sell lists of information you never thought would be for sale—records of 750,000 people who signed up for medical alert services, for example, or a list of 11,418 people, mostly men over the age of 55, who bought a particular herbal sexual-potency product in September or October. Private investigators buy phone records from pizza-delivery places, and a few years ago, data aggregator LexisNexis advertised that it, too, used pizza-delivery records to get hard-to-find phone numbers. If you want to invalidate some of the information on the lists, you could move, but you’d have to carry your own boxes—moving companies sell lists of new addresses to marketers.

More disturbing is the fact that this relatively disparate information is frequently rounded up by other data-aggregator companies such as ChoicePoint and Acxiom. Acxiom’s databases contain records on 96 percent of American households. Its newest customer intelligence database, InfoBase-X, includes 199 million names and can draw on 1,500 “data elements” to help companies market to potential customers, including “Life Event, Buying Activity, Travel, Behavior, Ethnicity, Lifestyle/Interests, Real Property, Automotive and more.”

Notes:

9. Banks sell lists of information that you'd think would be kept private—transaction histories, bank balances, where you've sent payments—and can continue to do so even if your account is closed. But banks are better than they used to be: Until the Gramm-Leach-Bliley Act in 1999, banks could even sell account and credit-card numbers to unaffiliated third parties.

These companies are only minimally regulated, in part because the government itself is one of their largest clients. Contracting data-collection projects to outside companies allows the government to purchase data that would be illegal for it to collect itself. Take, for example, what happened in 2002 when a now-defunct information-mining company and Department of Defense contractor called Torch Concepts got five million itinerary records for JetBlue passengers—records that included names, addresses and phone numbers—for a project whose goal was ostensibly to identify high-risk airline passengers. Torch Concepts then bought demographic data from Acxiom on about 40 percent of the passengers whose records JetBlue had released.

This demographic data included passengers' genders, home-ownership status, occupations, length of time spent at their residence, income level, vehicle information, Social Security numbers and how many kids they had. The company used the information to create detailed profiles of the passengers, including one (with the name stripped off but all other information still intact) that it used as part of a presentation to pitch potential clients.

Transportation was tricky. I'd been wearing my hat and sunglasses so I couldn't be recognized on cameras, but to take buses or the train would be to willingly subject myself to heavy surveillance, and that was against my rules. I couldn't drive my car through toll plazas—they're covered in cameras, and if you have an automatic toll-payment system that uses a pre-paid account, like E-ZPass or, in the Bay Area, FasTrak, you leave behind a record **(10)**.

I'd also learned about EDRs, or event data recorders, small devices installed in most new passenger vehicles that monitor things like speed, steering-wheel angle, acceleration, braking and seatbelt use. EDRs were first developed in the 1970s and began to be installed as part of airbag systems in the 1990s **(11)**. If safety sensors in your car detect a sudden deceleration, they trigger the airbag, and the EDR retains a record of what happened in the seconds preceding and following the collision.

But today, EDRs are part of sophisticated systems that do much more. If you subscribe to GM's OnStar service, for example, and get in a wreck, your car will notify OnStar so a representative can contact you through the speaker system in your car and medics can respond to the scene more quickly.

It's hard to complain about a voluntary service that could save your life, but other features are more intrusive. Starting in 2009, OnStar will be able to remotely deactivate a car's accelerator, forcing it to drive at a top speed of five miles an hour—which is great if your car is stolen but not so good if someone were to hack into OnStar's computers. Plus, systems like these include a two-way microphone and

speakers that the company can activate remotely, which means they can be used for eavesdropping.

The FBI took advantage of this capability a few years ago, when it got court authority to compel a company (which was unnamed in court documents) to turn on the microphone in a suspect's car to monitor conversations. The FBI eventually lost the case on appeal, but only when a court decided that the agency had forced the company to breach its contract with the suspect, because using the car's microphone for surveillance rendered it useless in case of emergency.

Fortunately, my car is old enough that it doesn't have an EDR. If I were to just drive around my neighborhood, I'd only have to worry about traffic and red-light cameras, whose images generally aren't archived unless something noteworthy happens. But I needed to go to San Francisco—the International Association of Privacy Professionals was having a conference. The problem was that attending it would require getting across the Bay Bridge.

Notes

10. Some states have sensors along the road that use toll passes to identify cars as they pass through two points. This information is used to make calculations about traffic speed and feed electronic billboards that provide up-to-the-minute estimated driving times to various locations. This information could also be used, hypothetically, to automatically issue speeding tickets. **Back to text**

11. If you want to see whether your car has an EDR, check your owner's manual—it's usually disclosed in the section about airbags. But EDRs aren't the only thing to be aware of. Car-rental companies have used GPS to tell when customers violated the terms of their contracts by speeding or crossing state lines

At first I thought this might be impossible. Then I remembered Casual Carpool, an informal system in which drivers can use toll-free lanes by picking up passengers throughout the East Bay and dropping them off in San Francisco.

Up to that point, I'd been wearing a cap and sunglasses every time I went outside (12). I liked my camouflage. It made me feel like I could be mistaken for J. Lo. But I thought that for my grand trip into surveillance-camera-dense San Francisco, I should try something different. I decided to wear my visor.

Let me be clear: This was no ordinary face visor. Designed to provide complete sun protection, it was more of a mask, with a wraparound piece of dark plastic that extended from my forehead all the way down to my chin. It made me look like a welder. It also made it difficult to see. But I still managed to find a car, and surprisingly, no one commented on the visor. In fact, they didn't talk to me at all.

You're Being Watched: No one knows exactly how many surveillance cameras are being used in the U.S. right now, but consider that the much-smaller U.K. has three to four million, and has recently approved funding to pay for cameras in the hats of more than 2,000 police officers. Aaron Goodman

At the conference, I switched from visor to hat, which made it easier to blend into the crowd of more than 900 “privacy professionals” (whose existence is a sign that more companies are taking privacy seriously). Here I listened to lectures on two technologies—IPv6 and RFID—that have significant privacy implications. IPv6, which stands for Internet Protocol Version 6 and is an eventual replacement for our current Internet protocol, IPv4, would allow mobile devices to connect to one other directly without any need for a server; it also means that your camera, PDA or just about any other gadget could have a unique identifier that would make it possible to track you in real time.

And then there are RFID (radio-frequency identification) chips, small devices that consist of a microchip and an antenna that use radio waves to identify objects and people (13). About five years ago, these chips (often called tags) were the obsession of conspiracy theorists everywhere. But the time to really worry about RFID may be near. Experts like Holtzman predict that soon the price of the tags will drop enough that they will be attached to almost everything we buy and will become so small as to basically be invisible. “You couldn’t get away with this experiment in a couple years

because of the RFID chips," Holtzman told me later. "You'd literally have to get rid of everything you own and start over, since every artifact you'd bought from a major manufacturer would probably have a chip embedded in it that could identify you as the buyer."

Just before the conference ended, I tracked down Richard Purcell, the former CPO of Microsoft. After dodging security cameras in the hallway, we ducked into an empty ballroom to talk. He was not encouraging. "The thing is, surveillance is a fact of our electronic society," he said. "You are going to be tracked. One has to be thoughtful about that." He's right. No one knows exactly how many surveillance cameras are being used in the U.S. right now, but consider that the much-smaller U.K. has three to four million.

And more cameras arrive all the time. The New York City Police Department, for instance, aims to install an additional 3,000 public and private security cameras below Canal Street, with video feeds that could broadcast directly to the Department of Homeland Security and the FBI. That's understandable—once the Freedom Tower goes up at the World Trade Center site, lower Manhattan will once again be home to one of the most conspicuous terrorist targets in the world. But the surveillance-camera craze has begun to veer into absurdity: The British government recently approved funding to pay for cameras in the hats of more than 2,000 police officers.

Notes:

12. The quality of the images taken by most surveillance cameras—at least the surveillance cameras of today—is unrefined enough that you don't need too much of a disguise. Back to text

13. Starting last year, all new U.S. passports are embedded with RFID chips that contain the person's identifying information and a photo, and research is under way on how to embed the chips in paper currency. RFID tags are already used to "microchip" pets. One company, VeriChip, has implanted 500 people in the U.S. with RFID chips and it has proposed replacing military dog tags by implanting the chips into American soldiers. It sounds far-fetched, but this is a real enough possibility that last October, California governor Arnold Schwarzenegger signed a bill forbidding employers to force employees to have RFID chips implanted under their skin

The problem with Casual Carpool is that it primarily runs into the city, which left me without a way to get home. I decided to take a cab but then noticed a plastic decal that read "Smile, you're on camera!" Whatever. By that point, one more camera was

the least of my worries. Instead, I spent the cab ride mulling the most common counterargument to concerns over lost privacy: So what? If giving up personal information makes it easier for me to shop online, so be it. If total surveillance can prevent terrorist attacks, bring on Big Brother.

Here's the thing, though—We don't know what information is being collected about us, whom it's being shared with, what it's being used for, or where it's being held. As companies and the government collect more and more data on us, some of it will inevitably be incorrect, and the effect of those errors could range from trivial to severe. It's not a big deal to get coupons for products you don't want, but if a mistake in your file or an identity theft caused by a data breach drives down your credit score, you could find yourself knocked into the subprime-mortgage market. And privacy-invading safeguards don't just catch bad guys. Anyone could end up like Senator Ted Kennedy, who was erroneously placed on a do-not-fly list because a terrorist had once used the alias "T. Kennedy."

For now, few systems are in place to help us understand what data is being gathered or correct the inevitable mistakes, and in the absence of laws that define punishments for data breaches—and judges who enforce them—companies can walk away from serious privacy violations with nothing more than a slap on the wrist.

Case in point: When EPIC filed a complaint with the FTC against JetBlue for disclosing passenger information to Torch Concepts, the agency never publicly opened an investigation; in response to a separate suit filed by JetBlue passengers, a federal judge agreed that the company had violated its privacy policies but dismissed the lawsuit because passengers weren't able to prove that anything had happened to them as a result of the profiling, and that JetBlue hadn't "unjustly enriched" itself by sharing the information. And because this kind of news is so often met with no more than a collective shrug, such privacy violations are likely to keep happening.

At the end of my week of paranoia, I met Hoofnagle at the Yerba Buena Center of the Arts in San Francisco so he could grade me on my performance.

His verdict: I did a pretty good job. But his approval seemed less satisfying when I considered all the aspects of my life that made it easier to minimize my digital trail. I don't use pay-per-view or FasTrak. I don't work in an office, which would require an ID card and logging on to and e-mailing from company computers. I don't use Instant Messenger, play online games, visit chatrooms, or sell things on eBay. I've never

been married or arrested, or owned property or a business, so few public records are associated with my name.

Also, spending one week undercover doesn't do anything about information that's already out there—information that, for the most part, I volunteered. Countless Web sites have records on me. UPS, FedEx and the Department of Motor Vehicles know where I live. My bank, credit-card company, gym and phone company all have me in their records, and my information is in alumni databases. Both my college and graduate school have lost laptops containing my Social Security number.

I was reminded of something Holtzman had told me earlier that week. "No matter what you do, you'll never really know if you're successful at keeping private," he said. "There are all sorts of trails you leave that you'll never even know about."

Once Hoofnagle had left, I walked through an exhibit, "Dark Matters," that happened to feature—no kidding—pieces about surveillance. One installation in particular captivated me. Called Listening Post, it was a darkened room with gray walls, empty except for a large lattice hanging from the ceiling made from 231 small screens, each the shape and size of a dollar bill. The screens displayed scrolling blue-green sentence fragments that were being culled, in real time, from Internet chatrooms. Occasionally the program would search for sentences that began with key words—"I am," "I like," "I love"—and the results would roll across the screens. "I love my new cellphone." "I love you and your sexy hair." "I love Quark."

It was strangely calming, standing in this dim room, watching the words and thoughts of strangers reveal themselves to me. I still had my hat on, but for once there were no surveillance cameras, so I sat down on a bench in the room and pulled out my notebook, grateful to finally be the observer rather than the observed. And then, out of the corner of my eye, I saw her: a security guard standing in the room's darkened corner—silent, motionless, watching

COMMENTS

Cell Phones:

Can't buy a cell phone anonymously ----50 years ago, you could have a phone only if Ma Bell came into your house and placed it there. And the phone and its operation were in their control.
Cell phone location tracking ---- Phone tracking always existed. In the past Ma Bell

knew you were using their phone in your kitchen.
Call tracing ---- Not only were calls traced previously, they were individually and personally connect by an operator – an operator who could, at her discretion, listen or record the call.
Cell phones are not secure ---- Party lines were less secure.

Surveillance

Security cameras identify people in public ---- Previously people walked past (and waved to) permanent neighbors every day. People noticed who was new on the street or who was shopping in the bricks-&-mortar store.
Internet ISP tracking ---- 50 to 100 years ago, the telephone operator personally placed everyone's calls and knew every one you IM'd with.

Criminal Activity

Ex-criminals decry publication of their addresses ---- In earlier societies and small towns, moving away from a checkered past was not possible

Anonymity

Address disclosure ---- In earlier times address disclosure also meant disclosure of what kind of underwear you hung upon the clothesline. Everything you did outside of your house was public knowledge.
On-line services track surfing ---- In a small community, everyone knew where you shopped and what you bought. The merchant may have been your neighbor or your school teacher's brother.
Credit reports ---- In earlier societies, your credit worthiness & general reputation were public knowledge.
Records disclosure ---- Marriages and legal contracts have been posted in public notices an newspapers since before the revolution.

A few quick things. First, it's possible to spoof your MAC address, and thus switch it to a random MAC address each time you . SMAC would be the most obvious tool for this purpose.

IPv6 is actually intended to be user-switchable, so that's a rather overstated issue, especially since it's so similar to MAC address systems in that regard.

RFID chips can be broken rather easily; the most simple methods would be through the use of a large electromagnetic pulse (attach a capacitor such as those found in disposable cameras to coiled wire) or simply microwaving the device. I expect such things to be rather common.

As for my primary comment : if you think you're paranoid now, wait until you start actually looking deeper down the rabbit hole. Think about what a single, exposed and compromised router close to you could send to a lucky hacker. Think about upcoming technologies that give glimpses into someone's life by simply being in the wrong place at the wrong time when someone else had a camera.

Big camera systems have shown themselves to be nearly worthless on a city-scale, as you might be able to watch an entire gang unload bullets on a helpless bystander yet lose track of them completely fifteen steps away. This data becomes even more meaningless when you have to sift through thousands of cameras for data that may well not be there. Now, when several thousand concerned citizens individually and simultaneously decide to cameraphone the creepy guy with the hat and glasses, you've got more of a problem.

And that's not even getting into near-future technology or paranoid conspiracy theory like tracking dollar bills by serial number or thermal tracking, or certain new technologies like the upcoming quantum computing trend (assume four years before government- and experimental-available 30+ qubit quantum computers become available and reliable, assume twenty years before such things are common place; each one will result in the complete destruction of many encryption techniques).

What's worse, though, is that many of the things you've done only made wide-area searches for suspicious activity *easier*. An adult wearing sunglasses and a baseball cap strikes me as a bit odd. Seeing sudden streams of purely encrypted text coming from a residential house? Seeing out-of-place access from a house when it normally gets nothing? Hell, even updating your virus scanner or firewall tells ClamWin or Kaspersky your general location and operating system.

The simple and ugly truth is that there isn't, and never was, and basic human right to privacy. It doesn't take a government or a nasty person (but I repeat myself) to violate any created right; it takes your actions, and most of your actions will cause it to be violated. That's as true in the 1800s, when the old fart at the counter

remembered every item you purchased since you were five years old, as today when it's replaced by a computer. It's more present now, but only because we rely on transactions like it so much more.

The more you rely on them, the harder and more expensive and more stringent any laws or contractual agreements to protect your privacy will need to be.

I say this as a network technician, whose local security is set to "0 privacy".

Interesting article. I had a few comments/quibbles/whatever.

As for going online anonymously, did you consider an Internet café? Most I've been to will let you pay with cash and won't need any information to create an account that couldn't be faked. Maybe that wouldn't have worked for you — I don't know if there's one near where you live, I don't know how much you use a computer or what else you use it for besides writing, and so on — and in any event, Internet cafés probably have surveillance cameras. Still, finding one of those was my first thought.

As for the Do Not Call registry, why did you need that? With everything you did, it sounds like you wouldn't have generated any new information in telemarketers' databases. And getting calls based on information gathered before the start of your experiment doesn't seem like it would violate the spirit of things.

And as for the camera in the hats of British police officers, that actually sounds like a good idea to me. At least, at first glance. Everything the camera is capturing, there's a police officer watching it anyway, but the camera DOES create a record of everything the officer says and does. The watchmen are already watching you; the camera is also watching the watchmen. (In theory. Assuming everything is recorded and saved, and the officer can't easily turn the camera off or obscure it, or if it is turned off any evidence gathered then is considered suspect, and so on.)

I get the basic point, that it would have made your experiment much harder if those police were around here. But unlike most of the surveillance state changes, I would be cautiously optimistic about something like a camera on all policemen.

It isn’t that funny, Since this experment was in californa I was supprised I did not see anything about the fact that you have to have a "card" to get the discount at any of the Major Grocery stores out here which is just another way of tracking every single thing you buy at every store. So did you buy food that week?

I must congratulate you, for going through the motions of "disappearing" or "falling off the grid" as it were... doing so gives the author good insight into the mind of someone that relies on this anonymity as a way of life.

cybishop brings up a good point, insofar as the "head mounted cameras could be used both ways" for police, but a hat can be easily removed, misplaced, crushed, forgotten, or otherwise be unused by said officer. placing it in a more... necessary peice of equipment would make more sense. something like a kevlar vest equipped with an audio/video array would make the best logical sense.

there remains some criticism about this article, on my end. to start off in a dense urban area like San Fransisco, where too many people see each other on a daily basis, isn't my idea of the best way to do this for two reasons:
1) They already know you live in said area.
2) Too many cameras have already filmed you.

start off by renting a hotel room under a pseudonym, in a small-ish town, something local, scenic, maybe even tourist friendly. pay by cash. watch nothing on tv, and wear said disguise as often as possible. you don't want them remembering the real you, only the John R. Smith that rode into town a few days ago and left without so much of a word.

buy a car from someone, an old beater preferably, as a "gift" for a relative.

move yourself into another destination, keeping up the disguise and/or moniker as long as humanly possible. pay your new landlord in cash. get a job somewhere where you aren't required to use your social insurance number, or use banking information. if you "need" to have a bank account, make one, but when your pay arrives, on that day, remove your money from said bank account. from the teller in the store, and not from the ATMs (they have cameras)

The cellphone segment is a good one, using pre-paid airtime can get lost in the "traffic" or all other pre-paid users. Avoid calls to call centers as they are recording all conversations "for training and feedback purposes"

It is possible to live a life of complete anonymity, but it's hard work. it requires diligence and steadfastness that, in this day and age, is hard for most people to grasp.

Taking different routes to places (mapquest loves me) is also essential, to avoid being followed/tracked. you can find city maps at your local municipal office and they don't usually put up too much of a fuss if you're looking to make some photocopies.

The essential is to understand how you can be tracked. support local and independent merchants, as they will be some of the last ones to implement RFID chips. Walmart's openly stated a few years ago that they were included in over 65% of their products. There is no record of it or linkable admittance to it, obviously, but we've all known it.

The step that most people who want to undertake this kind of experiment are remiss to take is the complete and total uprooting of their lives as they know it.

To truly cloak every aspect of daily life, one must begin an alternate life, adhere to it, and put away the past life. sever all connections with the people you knew, and start making new friends who know you under your alias.

This message was posted from someone on a laptop using a commercial and freely available WiFi connection, and said laptop will be formatted, it's MAC address changed, and logging for the router's been disabled, it's logs cleaned. (this company needs to stop hiring teenagers for their computer techs...)

I've fallen "off the grid" in my country for well over 9 years now, and I've enjoyed a careful freedom that none of the other people I knew then have now.

Going through AT&T was a mistake. Using a smaller Prepaid carier would be better. I've used Virgin Mobile off and on for several years. All you have to do is buy a phone ("disposable phone") and register online. You can use any address and any name. You can even get a different area code by using the right address, so if anybody was looking for you they would be looking in the wrong area. This will work with many other cariers too.

Logless VPN services give you true anonymous.

_____

Anonymous VPN

Are we really talking about ourselves...or "pointers" to ourselves. For example, suppose you have a database with my chronological age: 47. The real crises is the point at which you start making extrapolations about me. It's not a problem that you know the date on which I was born...the problem (and it's always been with us) is

what you do with that data. What type of credit or insurance do you give me. What do you think of my political beliefs.

The real identity crises in the last 30 years has been the growth of the relational database. This type of database assumes homogeneity across all tables. A person is a person who can be linked to any number of equivalent tables and a conclusion (or segregation) can be drawn.

Take my own case. I had one year of very bad financial problems caused by divorce, the Tech Bust and other factors. However, before and after I have maintained a well paying job, steady employment, stable address, money in the bank. The relational database does not have the capacity to take into account catastrophic events because it just averages it all in.

It doesn't account for rapid changes in opinion or personality. Suppose I convert from being a Democrat to a Republican. "On average" I am still a Democrat, even though my current opinions would be 180 degrees from a Democrat.

The real problem is not the pervasiveness of the technology, but the complete archiac nature and brittleness of it. Object oriented databases may allow for heterogeneous data collection, as would XML documents. Then there is of course our self-written stories on Facebook and Twitter. Imagine if someday, Savings and Loan officers go to our blogs and read about us and our past and make credit decisions based on our own words! Our data capture techniques should be as individualistic as we are.

As far as privacy, I say "feh". I want people to know who I am. I want them to get as much as my story as possible when evaluating me. Let it all hang out...let everyone in the neighborhood (just like back in the 60s) know who each other is and what they like to do. Don't hide it, flaunt it!

There hasn't been any hope of privacy or anonymity since at least 1965, that I can confirm. Belief in such things is foolishness. Unlike the author, I did work in military intelligence way back in the 1960s. I had a clearance several levels above Top Secret. In fact, I was cleared to read anything that came through our facility. One day while on burn detail (where they burn all the classified waste paper in the king of all paper shredder-incinerators) I came across a book about the size of a large city phone book. It was stamped with all sorts of "Eyes Only" "Limited Distribution" kind of stuff so naturally that me and my buddies wanted to read it.

It turned out that it was a collection of political profiles of US citizens. It was apparently being maintained by branches of the US military and there must have been a number of these books around, because I was in a foreign country at the time where there was limited use for such a book.

I looked it over and determined that it was as illegal as hell. The military just isn't supposed to be collecting that sort of info on US citizens. But there it was.

I thought it over -- whether I should turn it in or not. I decided that, if I did, I would still be in jail and no one else would be punished. As far as stopping it, that was simply hopeless. Even if it had been exposed, there were simply too many protections built into the system to allow anyone to get any punishment for it.

Now couple that with something else interesting. Does anyone remember the Pueblo incident of 1968 when the North Koreans captured a US spy ship? Got any idea what the spy ship was doing? One of the things it was doing was listening to ordinary telephone conversations carried over ordinary landlines -- from international waters. That was 1968, before the advent of sophisticated electronics like hand calculators.

If I want to know anything about you, I can know it. I can record your private activities within your home with tools that are cheap enough for an average citizen to buy, and that would leave absolutely no trace that I had been watching you. If I can do that on an ordinary person's budget, then what do you think the government could do, any time they wanted to?

The bottom line is this: The only reason you have any privacy at all is because your life is too boring for anyone to bother looking. That's the truth. Accept your bare-nakedness and get over it.

The step that most people who want to undertake this kind of experiment are remiss to take is the complete and total uprooting of their lives as they know it.

To truly cloak every aspect of daily life, one must begin an alternate life, adhere to it, and put away the past life. sever all connections with the people you knew, and start making new friends who know you under your alias.

Good idea of the commercial! but I think plus a pair of glasses is even more perfect www.firmoo.com/

Anonymity in cyberspace is really an illusion

By Fang Zhi Yuan

When Minister for Community, Youth and Sports Dr Vivian Balakrishnan said in a speech recently that “anonymity is an illusion in cyberspace”, some netizens dismissed his words as an empty threat and even challenged him to trace them. Some tried to court trouble by hurling invectives at him in internet forums on purpose to prove him wrong.

Recent incidents have convinced me that anonymity in cyberspace is really an illusion. The government does have the technical and financial means to track every single one of us down if it is determined to do so. The only reason why it is refraining from taking such drastic actions is that the price to pay for is too high.

In 2007, three bloggers were prosecuted under the Sedition Act for the articles they posted on their personal blogs which are deemed to be offensive to a minority race in Singapore. One of them, if I remembered correctly hosted his blog on a blogspot.com. He was tracked down in the matters of days.

That is why this site has repeatedly shunned from discussing racial and religious issues because we know the government is especially anal about them. And this is also the reason why comments from all our readers are still put under moderation for us to filter out these taboo subjects.

Though wayangparty.com has acquired a reputation as one of the most liberal blogs around, we do practise a limited form of self-censorship. As far as possible, we try not to censor or moderate comments posted here.

There is no anonymity on government-owned forums like CNA, Hardwarezone and STOMP. Your IP addresses have been locked and it is very easy to trace your identity compared to let’s say, delphiforums which is hosted in the United States. After we broke the news about “PothePanda”, we have been receiving emails from Singaporeans from all walks of life including civil servants about internet policing by the government.

Unfortunately, there is no way we can verify their claims and we can only take what they say with a pinch of salt. Nevertheless, we believe there is some element of truth in them.

The government does know what is going on in the blogs and internet chatrooms. For example, the PAP MPs are aware of the online poll we conducted on Seng Han Thong and his assailant and this was brought up in Parliament.

Journalists read our blog daily to fish for information here. Two hours after we published the leak about the CDC bonuses, a journalist emailed us to inquire more about the case.

You may have noticed that there are a few commentators who criticized our articles all the time with the sole motive of putting us down. Some readers have asked us to censor their comments altogether. We have to allow them to post freely not so much for free speech, but because they are our “guardian angels”.

If the encounter of “PothePanda” is to be believed, a covert ops may be going on for quite some time to identify “radical” bloggers and netizens and to “persuade” them to moderate their stance via an invitation to “limp kopi”.

Nobody will know what is happening because the press doesn't report on it and the monikers simply vanish into thin air. I am sure you are aware of some prominent bloggers and forumers who have been on the "missing in action" list for a long time. Over here at wayangparty, I must admit we have pushed the boundaries to its limits and probably beyond it. Though some of our articles may sound too "dangerous", we have taken extra precaution to ensure there is no way the authorities can find fault with us. It will surely peeve them off, but it will be too tall an order for them to charge us without any solid grounds.

We are taking a calculated risk and I must admit I am quite disturbed by recent developments. A long time socio-political blogger Lucky Tan has taken down his blog till further notice. This was what he wrote: "*I receive a few emails that a number have been followed. Something may be on. I'll be back once the picture is clearer."*
I am not sure if Lucky Tan had received the same emails as we did, but the contents are definitely not reassuring.

Perhaps it is time for wayangparty.com to re-evaluate its editorial stance and policy. We are no longer the wayangparty.com 6 months ago. With a readership approaching TODAY Online's (our alexa.com ranking today is 696, not far from TODAY's 412), it is inevitable that people will start to sit up and take notice of us. It may become a necessity to move eventually into the middle ground not only to survive, but to continue to grow.

When Malaysian blogger Raja Petra Kamarrudin was arrested under the ISA last year, over 2,000 Malaysians turned up in a candle-light march to protest against his arrest. I wonder at times whether any of our readers will bother if we "disappeared" from blogosphere one day.

Public pressure is the only and yet the best form of defence against a dictatorial regime bent on cracking down on dissenting voices in order to preserve and perpetuate its own political hegemony without which we will forever be herded by them like blind sheep.

As of now, I implore every one of you reading this to take extra precaution when posting in the government-owned forums. A seemingly innocuous post on molotov cocktails can get one into trouble. The cloak of anonymity is in reality a delusion and it pays to be on the safe side.

http://www.temasekreview.com/2009/03/25/anonymity-in-cyberspace-is-really-an-illusion/