Concerned About Your Digital Privacy? You Should Be

Your privacy is a cloud of data scattered on servers that are beyond your control. Your Digital profile is regularly bought and sold without your permission. The government can track you by GPS without a warrant. Sure, it's all part of life in the digital age. But it's okay to be annoyed about the extent of it. And it's definitely okay to fight back.

February 22, 2011 6:30 AM

Threat Level I: Irritating

Victims: Anyone who uses technology
Damage: A Slow but manageable leak of personal information, behavior and geographic location

Public Cameras
Legally, public spaces are fair game for taking photographs. But these days the sheer number and sophistication of public cameras is creating an environment of constant surveillance—especially in cities. A 2006 survey by the New York Civil Liberties Union (NYCLU) found more than 4000 cameras in Lower Manhattan alone. "Since then, the number has grown exponentially," NYCLU spokeswoman Jennifer Carnig says. "There are now too many to count." Add to that Google's roving Street View cars, which routinely capture images of houses and pedestrians (sometimes in compromising states), and a growing number of license-plate-reading cameras installed at tollbooths, in police cars and at intersections, which law enforcement uses to run checks on thousands of unsuspecting drivers each day. "We're now seeing proposals in states to allow police to upload, record and build [car-tracking] databases," says Peter Eckersley, a staff technologist at the Electronic Frontier Foundation.

Fight Back *There's really nothing you can do about the proliferation of public cameras, but red-light cameras are another story. Many radar detectors now come loaded with databases of known locations. And if you don't want your house (or anything else personal) on Google Street View, load the offending image and click the Report a Problem link on the bottom left corner. It will bring up removal instructions.*

Location-Based Services
By using a phone's GPS chip to broadcast your location—and by making it easy to find friends who have done the same—"geosocial" networking services such as Foursquare, Facebook Places and Gowalla are transforming the way people interact in the real world. And while a log of your movements is gold to marketers, broadcasting this information can potentially have more dangerous consequences. Security researchers have shown that it's possible to hijack info from geosocial services that was meant to be shared only with friends, and many users don't bother with privacy controls at all. "It amazes me that people post their phone number and location," says Kevin Haley, director of Symantec Security Response. "You're giving access to yourself to anyone in the world."

Social-media expert Carri Bugbee was at a restaurant with friends when two strangers called to threaten her after pulling Bugbee's location from the geosocial networking service Foursquare. "They were trying to scare me," she says, "and it worked." Fortunately, the harassment lasted just one night.

Fight Back *Use location-based services to post where you've been, not where you are. "The present tense makes you vulnerable," says Efstratios Gavas, a computer scientist at the Polytechnic Institute of New York University. Set the privacy settings in Facebook Places to block other people from posting your location. And be wary of linking your Foursquare account to Facebook or Twitter—that will reveal your location to the world.*

SuperCookies
Web cookies aren't all bad—they allow online merchants to store items in virtual shopping carts, and keep you logged in to Web-based e-mail services—but they can also be used by marketers to log your online activity. "Some cookies can track you across multiple sites," says Samy Kamkar, a Los Angeles–based programmer. The conventional best practice has always been to turn off third-party cookies in your browser's privacy settings—this keeps outside advertisers from tracking you, yet still allows websites to work properly. Lately, however, a new privacy threat has gained attention. Cookies are also stored by Adobe's ubiquitous Flash software, which has its own separate privacy settings. The scary part: Blocking cookies in most browsers has no effect on Flash cookies, and savvy marketers have exploited this loophole to open up a whole new avenue of tracking, even using Flash cookies to reinstall deleted

browser cookies. In an effort to draw attention to the issue, Kamkar has created an "evercookie" that constantly repopulates itself, even across browsers, every time you try to delete it. "I think people need to understand every possible location that cookies can be stored," Kamkar says, "then understand how to prevent them."

Fight Back *To control Flash cookies, right-click on any Web-based Flash content (such as a YouTube video), and select Global Settings to bring up the Adobe Settings Manager. To clear the cookies, go to the Website Storage Settings panel.*

Social-Network Data Mining

While social networking sites are designed to help users share information with friends and family, it can be just as easy for unwelcome visitors to eavesdrop. Facebook has come under fire for allowing third-party app developers to collect and sell information about users. Last year, a company called Rapleaf was exposed for using Facebook data to create and sell profiles on individual users. But the concerns are hardly limited to one service. A 2009 survey of 45 social networking sites by the University of Cambridge found that privacy policies were routinely difficult to understand, and there were no industry standards for privacy protection. (Google and Facebook have since revised their policies to address this concern.) Yet experts we spoke with say that these sites pay lip service to privacy but routinely compromise the data of their users through neglect or for profit. "Google, Facebook, Myspace and others have gone beyond connecting people—they're exposing them," says Babak Pasdar of the security firm Bat Blue.

Fight Back *Be wary of what you post on social networking sites. "Don't put your age and household info out there—these are key building blocks of a profile," says Michael Fertik, CEO of ReputationDefender. It's worth the effort to dive deep into the privacy controls of your social networking sites—the default settings are a free-for-all—and delete Facebook apps you don't use anymore.*

Threat Level II: Infuriating

Victims: Frequent fliers, big-business customers, mobile Web surfers
Damage: Deeply personal and potentially financial, yet ultimately repairable

Whole-Body scanners

Now in use in more than 65 U.S. airports, whole-body imagers use either millimeter-wave or backscatter X-ray technology to see weapons that might be hidden beneath clothing. The uproar over these machines peaked last holiday travel season as millions of travelers were exposed to the scanners for the first time. Hundreds of travelers logged complaints with the Transportation Security Administration, and the Electronic Privacy Information Center (EPIC) filed a lawsuit against the Department of Homeland Security to suspend deployment of these scanners in airports. Some privacy advocates claim the machines may even run afoul of child pornography laws.

Fight Back *You have the right to opt out of a body scan, but if you do, be prepared for an "enhanced" pat-down that, to some, may be even more intrusive. Until the law changes, expect a lot of travelers to drive or take the train whenever possible.*

Stolen Databases

According to the Privacy Rights Clearinghouse (PRC), the 2000-plus major data breaches made public since 2005 have exposed more than 500 million customer records to potential cybercriminals. (The total number of affected individuals is difficult to determine, since many people may have been victims of more than one breach.) Customer database breaches can occur for any number of reasons, from a sophisticated attack on a credit card company's server, to a laptop lost by a health insurance employee. In other words: Your privacy may be threatened by somebody else's ineptitude.

During testimony in 2006, former Secretary of Veterans Affairs Jim Nicholson showed a hard drive similar to one that was lost when a VA analyst's laptop was stolen that May. The laptop and drive contained personal data, including social security numbers, for more than 26 million veterans. Luckily, the laptop was recovered before much damage occurred.

Fight Back *These breaches are often out of your control, but you can still minimize the damage. If your data has been compromised, report the incident to a credit rating agency. And if a company wants to use your social security number to identify you, ask them for an alternate ID number—it'll be much less damaging if stolen.*

Cell Phone Hacking

Most security experts agree that the next big wave of cyberthreats will be aimed at mobile phones, which have the double vulnerability of being location-aware and storing plenty of personal data. Security researchers have made a sport of finding potential security holes in Apple's iOS and Google's Android mobile operating systems, and there are already numerous apps that can track a phone's physical location or, as is the case with the M-Spy and IP Webcam apps, remotely turn on an Android phone's microphone or built-in video camera. "With the expanding use of mobile phones, we're only seeing the beginning of the types of privacy breaches possible," says Symantec's Haley.

Fight Back *If you're using Android or a jailbroken iPhone, treat app downloads like e-mail attachments from strangers and limit yourself to apps from developers you trust. If you think your phone may have been compromised, a factory reset (usually found in a smartphone's general or privacy settings) will wipe away any malware.*

Wi-Fi Hijacking

Public Wi-Fi hotspots are often set up with no security precisely so anybody can log on. But this convenience comes at a price: Open networks make it easy for hackers to perform a trick called session hijacking, wherein one user on a network grabs a browser session from another user after he's logged into a supposedly secure site, such as a social network, an online bank or a store. The attacker then has complete access to the victim's account, and can change the password to lock the victim out. Recently, a programmer who goes by the name of Codebutler released a Firefox plug-in called Firesheep, which makes it possible to pull a session hijack with just a single click.

Fight Back *Think twice about what you do when logged on to a public hotspot—a determined hacker can intercept anything you send. And only use networks you trust. Even if one has a legit-sounding name like "AT&T," it could still be a trap. "You may think you're signing up for the coffee shop's Wi-Fi when a hacker has actually set up his own," says Kevin Haley, director of Symantec Security Response.*

Threat Level III: Devastating

Victims: Harassed ex-spouses, government suspects, random targets, future homeowners
Damage: psychological and physical Threats, oppressive Orwellian Intrusion

GPS Car Tracking

Low-cost GPS devices for tracking kids or pets may be marketed for innocent purposes, but they can also be used to sinister effect. Last November, Christina Crosby of Jacksonville, Fla., found one of these devices attached to her car after her estranged husband started randomly showing up at places she went. It is illegal for citizens to secretly track each other via GPS, but the law is not so clear when it comes to the government. And sometimes the law-enforcement GPS dragnet is cast uncomfortably wide. Last summer, the U.S. Court of Appeals for the Ninth Circuit ruled that law-enforcement agencies have the right to attach GPS trackers to your vehicle without a warrant—even in your own driveway.

Last October, Yasir Afifi, a college student and son of an Islamic-American community leader, discovered a GPS tracking device on his car during an oil change. The California resident's friend posted pictures of it on the Internet, and two days later, FBI agents showed up at Afifi's door to reclaim their device. Afifi's lawyer says he has not been charged with any crime.

Fight Back *If you have reason to believe someone is tracking your vehicle, take it to a mechanic for a look-see—most found trackers pop up during routine inspections. The best place to look: under the car, near the rear wheels.*

Internet Trolls

Allison Stokke wasn't looking for Internet fame, but it sure found her. In May 2007, a picture of the high-school pole-vaulter from Newport Beach, Calif., was posted on a track-and-field enthusiast site. While there was nothing unusual about the photo, the image of the pretty athlete inexplicably went viral. Within weeks, she was dealing with unofficial fan pages, fake Facebook profiles and a deluge of lewd messages and phone calls. These days, the Internet can turn almost anybody into an object of mass obsession, often for no real reason. One center of gravity for those obsessions is the anarchic anonymous Internet posting site *4chan.org*. Started in 2003 by a 15-year-old from New York City, it has morphed into a pure expression of Internet id—an endless stream of geek slang, pornographic pictures and juvenile jokes that can motivate its users (known derisively as trolls) to gang up on almost anyone. Targets have ranged from the vaguely political (a hack of Sarah Palin's webmail account) to the weirdly sentimental (a flood of birthday cards sent to a 90-year-old World War II veteran), to the downright vindictive (a barrage of harassment directed at an 11-year-old Florida girl). The site's tech-savvy trolls have been known to find and distribute its victims' personal information, and the attacks are as random as the site itself.

Fight Back *Protecting yourself from Internet trolls is like a farmer attempting to fend off locusts. Because there is usually no central organization behind the behavior, it can be impossible to deal with head on. Worse: Trying to fight* *back could further provoke the perpetrators. If you are the victim of an attack, keep in mind that most reputable sites such as Facebook, Myspace or YouTube respond to take-down requests for any material that is lewd, slanderous or threatening.*

Cyberstalking
In 2004, Alexis Moore's ex-boyfriend hacked into her online accounts, shut off her utilities and cellphone and then emptied her bank account. "It took three long, frustrating years to fix everything," Moore, the founder and president of the victims' support group Survivors in Action, says. As privacy invasions go, stalking is the most personal and intensely frightening. And as technology has improved, stalking perps have become more sophisticated. Keylogging software makes it possible to remotely monitor every word typed on a PC, webcam hijacking software can secretly capture video every time someone moves in front of their computer, and cellphone trackers can transmit the location of victims in real time. "The technology is outpacing law enforcement's capability to keep up," says Michele Archer of Safe Horizon, a domestic violence support center. "For many victims, it's very scary. They tell us they feel like they're being watched all the time."

Fight Back *If you or someone you know is being harassed, contact a local victims' services group, says Michelle Garcia of the National Center for Victims of Crime, which has resources on its website, ncvc.org. Garcia also recommends that victims document everything. "Let all of your calls go to voicemail so that they are recorded," she says. "Also print out instant messages and create a log of the date, time and place of each incident."*

The Aware Home
The hot new Microsoft Kinect is a revolutionary camera-based gaming accessory that recognizes the movements of players' bodies. It also has the potential to become a sophisticated digital marketing tool. Last November, Microsoft executive Dennis Durkin commented to investors that the Kinect could conceivably be used to track the behavior of people watching television. "In the future, [we'll be able to] get better data about how many people are in a room when a [football] game is being played," he said. "How are those people engaged with the game? Are they wearing Seahawks jerseys or are they wearing Giants jerseys?" Likewise, smart-grid technology already in use by some major utilities allows for real-time monitoring of electric meters, with an eye toward eventually embedding intelligence in every appliance in the house, including thermostats, washers, dryers and refrigerators. The aim is to promote efficiency, but the side effect may be to turn your home into a highly precise behavior-monitoring system.

Fight Back *Although none of this stuff is currently being used for a Big Brother agenda, consumers should keep tabs on the evolution of any technology that watches you in your home. Advocacy groups are demanding privacy protections be built into aware devices and smart-grid infrastructure. The data collected by these devices could eventually be used by everyone from nanny-state public officials to criminals cruising for empty homes.*

BY GLENN DERENE AND SETH PORGES

Taken From: Popular Mechanics Online