Your Cellphone Is Spying on You

How the surveillance state co-opted personal technology

Ronald Bailey

BIG BROTHER has been outsourced. The police can find out where you are, where you've been, even where you're going. All thanks to that handy little human tracking device in your pocket: your cellphone.

There are 331 million cellphone subscriptions—about 20 million more than there are residents—in the United States. Nearly 90 percent of adult Americans carry at least one phone. The phones communicate via a nationwide network of nearly 300,000 cell towers and 600,000 micro sites, which perform the same function as towers. When they are turned on, they ping these nodes once every seven seconds or so, registering their locations, usually within a radius of 150 feet. By 2018 new Federal Communications Commission regulations will require that cellphone location information be even more precise: within 50 feet. Newer cellphones also are equipped with GPS technology, which uses satellites to locate the user more precisely than tower signals can. Cellphone companies retain location data for at least a year. AT&T has information going all the way back to 2008.

Billboard, Travelpix Ltd/Getty

Police have not been shy about taking advantage of these data. According to the American Civil Liberties Union (ACLU), U.S. law enforcement agencies made 1.5 million requests for user data from cellphone companies in 2011. And under current interpretations of the law, you will never find out if they were targeting you.

In fact, police no longer even have to go to the trouble of seeking information from your cell carrier. Law enforcement is more and more deploying International Mobile Subscriber Identity locators that masquerade as cell towers and enable government agents to suck down data from thousands of subscribers as they hunt for an individual's cell signal. This "Stingray" technology can detect and precisely triangulate cellphone signals with an accuracy of up to 6 feet—even inside your house or office where warrants have been traditionally required for a legal police search.

Law enforcement agencies prefer not to talk about cellphone tracking. "Never disclose to the media these techniques—especially cell tower tracking," advises a guide for the Irvine, California, police department unearthed by the ACLU in 2012. The Iowa Fusion Center, one of 72 local law enforcement intelligence agencies established in coordination with the Department of Homeland Security, distributes a training manual that warns, "Do not mention to the public or media the use of cellphone technology or equipment to locate the targeted subject." The ACLU translates: "We would hate for the public to know how easy it is for us to obtain their personal information. It would be inconvenient if they asked for privacy protections."

Ubiquitous cellphones, corporate acquiescence, stealthy new surveillance technologies, and unchecked police intrusiveness combine to produce a situation where the government can pinpoint your whereabouts whenever it wants, without a warrant and without your knowledge. The courts have largely punted on this issue so far. But should carrying convenient communications technology mean that we give up our right to privacy?

Panopticon Rising

Back in the 18th century, architect Samuel Bentham designed a building in which every occupant would be perpetually observable by a hidden inspector located in a central tower. His brother, philosopher Jeremy Bentham, dubbed the building the Panopticon (literally, "all seeing") and argued that widely adopting it could solve most of society's ills. "Morals reformed—health preserved—industry invigorated—instruction diffused—public burthens lightened—Economy seated, as it were, upon a rock—the Gordian knot of the poor-law not cut, but untied—all by a simple idea in Architecture!" Bentham enthused. The occupants of the Panopticon, not knowing if they were in fact being observed, would come to assume constant surveillance and eventually "watch themselves." No actual inspector needed.

More than 200 years later, geographers Jerome Dobson from the University of Kansas and Peter Fisher from the University of Leicester took the concept of the Panopticon to the next level. In a 2003 article in *IEEE Technology and Society Magazine*, the two ominously predicted "geoslavery," defined as "a practice in which one entity, the master, coercively or surreptitiously monitors and exerts control over the physical location of another individual, the slave." In their most lurid scenario, the master would be able to constantly monitor his slave's location and, if he wasn't where he was supposed to be, remotely administer an electric shock to get him back in line. Although no one has offered an electric shock app for cellphones yet, private companies like PhoneSheriff and FlexiSPY offer cellphone software that enables parents and spouses to secretly monitor others' contacts, conversations, and locations. As creepily invasive as private surveillance is, however, it's far worse for our civil liberties that surreptitious tracking by law enforcement has so dramatically increased since 2003. How free would you feel if you thought there was a good chance the cops were monitoring your movements?

"The reason that the Panopticon will slip into the modern world is because it offers so many benefits, as Bentham argued," Dobson tells me. "The downsides will become apparent only after we've been seduced by the benefits."

Stephanie Pell, former counsel to the House Judiciary Committee, and Christopher Soghoian, a senior policy analyst and chief technologist at the ACLU's Speech, Privacy, and Technology Project, argue in the Spring 2012 *Berkeley Technology Law Journal* that "the presence of modern surveillance mechanisms, visible and imperceptible, public and private, promotes the 'Panoptic effect'—a general sense of being omnisciently observed." Pell and Soghoian argue that aware-

U.S. law enforcement agencies made 1.5 million requests for user data from cellphone companies in 2011. And under current interpretations of the law, you will never find out if they were targeting you.

ness of the state's Panoptic "gaze" becomes coercive: We act differently if we believe we are being watched. Individual freedom requires the ability to avoid the judging gaze of others, especially agents of the state. "As modern location surveillance techniques increase in precision and their pervasive distribution throughout society becomes known," write Pell and Soghoian, "people become increasingly aware of, and potentially influenced by, a palpable sense of the omniscient gaze similar to that produced by the design of Bentham's" Panopticon.

Somebody's Watching

"Awareness that the Government may be watching chills associational and expressive freedoms," wrote U.S. Supreme Court Justice Sonia Sotomayor in *U.S. v. Jones*, a 2012 case dealing with warrantless GPS tracking. Sotomayor added that such unfettered tracking "may alter the relationship between citizen and government in a way that is inimical to democratic society." Dobson asks: "What happens if you create a society in which nobody can do anything wrong, never step out of line or go off the path? Would that be the same self-motivated society we have today?" Watched citizens are tantamount to prison inmates; they just roam a larger cage.

"Privacy is rarely lost in one fell swoop," writes George Washington University law professor Daniel Solove in a May 2011 *Chronicle of Higher Education* essay. "It is usually eroded over time, little bits dissolving almost imperceptibly until we finally begin to notice how much is gone." Solove suggests that privacy will be lost slowly at first, as many people shrug when the government begins to monitor incoming and outgoing phone numbers. After all, they're just phone numbers. Each increase in government spying—recording selected phone calls, installing video cameras in public spaces, surveilling via satellite, tracking bank transactions, compiling records of Internet searches—is shrugged off as a minor intrusion. "Each step may seem incremental," Solove warns, "but after a while, the government will be watching and knowing everything about us."

Solove points out that awareness of pervasive surveillance not only affects how citizens go about their lives (how they express themselves, with whom they associate); it also skews the balance of power between individual citizens and government bureaucracies. As the size and scope of government grows, bureaucratic mistakes become more common and harder for citizens to correct. Putting limits on government surveillance is therefore a way to prevent the government from doing wrong to its citizens.

Aficionados of the HBO series *The Wire* will remember the great difficulty Baltimore detectives had in obtaining permission to wiretap the public phones and cellphones used by drug gangs. What followed were long, fruitless stakeouts and boring nights and days listening for relevant calls, all in the face of ever-tighter budgets and hostile bosses with higher priorities.

What a difference a decade makes. "Most modern surveillance can be performed with a few clicks of a mouse, a fax, or a phone call to a service provider, all from the comfort and safety of the officer's desk," explains the ACLU's Christopher Soghoian in his 2012 dissertation *The Spies We Trust*. Soghoian adds, "Telecommunications carriers and service providers now play an essential role in facilitating modern surveillance by law enforcement officers. The police merely select the individuals to be monitored, while the actual surveillance is performed by third parties: often the same email providers, search engines and telephone

companies to whom consumers have entrusted their private data. Assisting Big Brother has become a routine part of business." Big Brother and Big Business must part.

As journalist Garret Keizer says in his 2012 book *Privacy*, "There are many good reasons to stand up for privacy, some having to do with building a good society, others having to do with living a tolerable life."

By the Numbers

Modern digital technologies are making it simple and very cheap for agents of the state to find out where you are and where you have been, and even to predict where you're going. In July, Rep. Edward Markey (D-Mass.) reported that wireless carriers responded to 1.3 million demands from law enforcement agencies for subscriber information in 2011, including location data, calling records, and text messages. Subsequent reporting bumped that number up to 1.5 million requests. Soghoian notes: "More than half of these requests were subpoenas, and were therefore likely issued without judicial review." The amount of data is probably much greater than that number suggests, since a single request might involve a "dump" of all subscribers who connected to a particular tower during a specified period of time. In 2010 Sprint admitted that the company had over the years complied with 8 million requests from law enforcement agencies for customers' GPS information.

Between 1968 and 2011, by comparison, American law enforcement agencies obtained a total of just 46,988 wiretap orders, including 2,732 in 2011. During that period, Soghoian notes, federal and state courts rejected requests for wiretaps only 34 times. In 2011, 97 percent of wiretaps were for portable devices. *The Wire* also gets this right: The war on drugs was used to justify 95 percent of federal and 81 percent of state wiretap orders.

Most of the requests for electronic communications and data transmitted by the cellphones, personal computers, and other digital devices remain forever secret. In a May 2012 *Harvard Law and Policy Review* article, U.S. Magistrate Judge Stephen Smith asks, "What is the most secret court docket in America?" Many people might think of the court created by the Foreign Intelligence Surveillance Act (FISA), which deals with requests for warrants to monitor suspected spies and terrorists. Since 1979 the FISA court has considered 28,000 secret warrant applications and renewals, turning down just five. By comparison, Smith calculates, in 2006 alone federal magistrate judges issued more than 30,000 secret search orders under the Electronic Communications Privacy Act (ECPA), which specifies minimal legal standards from government surveillance of cellphone and Internet communications.

"To put this figure in context, magistrate judges in one year generated a volume of secret electronic surveillance cases more than thirty times the annual number of FISA cases," Smith writes. "In fact, this volume of ECPA cases is greater than the combined yearly total of all antitrust, employment discrimination, environmental, copyright, patent, trademark, and securities cases filed in federal court." This pervasive secrecy means police surveillance is rarely challenged because 1) law-abiding citizens never learn that they have been targeted, since their service providers are not allowed to tell them; 2) court orders authorizing surveillance are sealed and never made public; and 3) the public and Congress do not have access to systematic data on how often electronic surveillance is used.

The Justice Department argues that obtaining geolocation data does not require a warrant based on probable cause. To obtain "noncontent" information such as email addresses, phone numbers, and locations, the DOJ says, law enforcement agencies need only present an appropriate judge with "specific and articulable facts" indicating that the information requested is "relevant and material to an ongoing criminal investigation." Under the usual standard for a search warrant, police would have to show there was probable cause to believe the information they sought was evidence of a crime. Many local police departments have policies that are looser and more inconsistent than the Justice Department's: Based on information from 230 law enforcement agencies around the country, the ACLU found that nearly all of the police departments acknowledged tracking cellphones, but "only a tiny minority reported consistently obtaining a warrant and demonstrating probable cause to do so."

Warrants Wanted

Last January the Supreme Court provided hope that the rising tide of police surveillance might be stemmed. In *U.S. v. Jones*, it ruled that attaching a GPS tracking device to someone's automobile and tracking him 24 hours a day for a month

In 2010 Sprint admitted that the company had over the years complied with 8 million requests from law enforcement agencies for customers' GPS data.

is unconstitutional in the absence of a warrant. Although that conclusion was unanimous, the Court was divided on the rationale for it. Anthony Scalia, in an opinion joined by four other justices, emphasized the trespass required to attach the tracking device. Samuel Alito and three other justices emphasized the nature and volume of the information collected by the surveillance, which they said violated reasonable expectations of privacy. As Alito noted, the majority's reasoning would not apply to tracking via cellphone towers or GPS signals, which do not require a physical intrusion on the target's property. Hence we do not know yet whether the Court will decide those kinds of surveillance require warrants.

The privacy coalition Digital Due Process argues that "the government should obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cellphone or other mobile communications device." The coalition includes companies such as Google, Microsoft, Apple, Facebook, and Intel, along with advocacy groups such as the ACLU and the Competitive Enterprise Institute.

Requiring a probable-cause warrant is certainly better than merely articulating a reason the police might want to spy on someone. But warrant applications are rarely rejected by magistrates. Optimists would say that's because the police and prosecutors draft them more carefully when faced with a higher standard. Pessimists would point out that prosecutors control all of the information provided to magistrates, who then have little choice but to rubber-stamp the warrants. "A warrant is actually not that high a standard," explains ACLU legislative counsel Christopher Calabrese, "but it is the legal standard for kicking down the door to your house."

The Geolocation Privacy and Surveillance (GPS) Act, introduced last June by Sen. Ron Wyden (D-Ore.) and Rep. Jason Chaffetz (R-Utah), would require law enforcement agencies to obtain warrants for real-time and historical geolocation data. Calabrese says the language in the GPS Act is broad enough to cover location data from car navigation systems such as OnStar and GPS systems such as TomTom as well as cellphones. It would even cover data collected by location-based service providers such as Foursquare and Loopt or self-driving automobiles of the future.

Soghoian and Pell propose additional safeguards. They argue that Congress should require police to erase data when investigations are concluded and inform innocent people whose information is collected as part of an investigation within 90 days of completing it. They say requiring such disclosure would encourage cops to narrow their information demands, since "the cost of notifying 200 people will presumably be greater than that of notifying only 20." Finally, since Congress and the courts cannot monitor and regulate what they cannot see, Soghoian and Pell want Congress to require that all court orders seeking location data be reported within 30 days and tabulated as to type and quantity in an annual report to Congress.

Cultivating and maintaining a society of free and responsible individuals is impossible under the permanent Panoptic gaze of the government. Ubiquitous surveillance becomes indistinguishable from totalitarianism. "The ultimate check on government as a whole is its inability to know everything about those it governs," Keizer writes in *Privacy*. In other words, state ignorance is the citizenry's bliss.

Science Correspondent Ronald Bailey (rbailey@reason.com) is the author of Liberation Biology (Prometheus).