INSIDE OUR BORDERS

Smartphone owners keep loads of personal data in their devices in exchange for convenient features.

JUSTIN SULLIVAN/GETTY IMAGES

POCKET PROTECTION

Your mobile device knows almost everything about you. Can it be used against you?

By Matt Alderton

WEIGHING LESS THAN 5 ounces, Apple's iPhone 7 knows whom you call and who calls you. It knows the content of your text messages and emails. It knows where you're going and where you've been. It knows your banking passwords, the names of your friends and the date of your next doctor's appointment. And, if you've ever taken an explicit selfie, it even knows what you look like naked.

"Your cellphone is the most intimate thing in your life," said security expert Bruce Schneier, author of *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. "It knows who you sleep with, when you get up and when you go to sleep. It's the first thing you check in the morning and the last thing you check at night. ... You don't lie to your (cellphone);

it knows more about you than your significant other does."

Of course, cellphone owners enjoy a wealth of 21st-century services in exchange for their data. Travelers who tap an address receive turn-by-turn directions to their hotel. Those who upload vacation photos can quickly share them on social media. And customers who add their credit card information can use their phones to pay for coffee. For most Americans, the question isn't whether their phones should know the things they know. Rather, it's how they should share them and with whom.

"It's very difficult for most consumers to control what happens to their data," said Marc Rotenberg, president and executive director of the Electronic Privacy Information Center, a public interest research center that advocates for digital privacy and civil liberties. "For that reason, we need companies and governments to establish safeguards."

PRIVACY VS. PUBLIC SAFETY

The national conversation about safeguards began in earnest in 2013, when former CIA employee and government contractor Edward Snowden disclosed documents that proved secret mass surveillance of Americans' internet and cellphone communications by the National Security Agency. It reached a fever pitch, however, on Dec. 2, 2015, when husband-and-wife terrorists Syed Rizwan Farook and Tashfeen Malik opened fire on Farook's colleagues at a holiday party in San Bernardino, Calif., killing 14 people and injuring 22 before both were killed in a shootout with police.

Afterward, the FBI recovered Farook's work-issued iPhone, which was locked with a four-digit password and programmed to erase its contents after 10 failed password attempts. Unable to unlock the phone, it asked a federal court to compel Apple to assist its investigation by creating a "backdoor" into Farook's phone. Apple refused.

"The government suggests this tool could only be used once, on one phone. But that's simply not true," said Apple CEO Tim Cook said in a statement. "In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable."

Apple's feud with the FBI ended abruptly in March when the agency announced it had successfully commissioned a private company to crack Farook's phone without triggering a security feature that would have erased all the data. The questions it raised, however, remain — not the least of which is: Which is more important, privacy or public safety?

Privacy advocates point out the personal and social consequences of unsecured mobile data. "(If you have an Android phone) Google knows where you sleep, eat and work. It knows where you go to the doctor, whether you're seeing a therapist, if you're having an affair, where you worship and where your kids go to school," said Nate Cardozo, senior staff attorney at the Electronic Frontier Foundation, a nonprofit that works to defend digital civil liberties. "Even if you don't care that Google knows that, or the government, you might care if your ex, your employer or your insurance company knows it."

MANDEL NGAN/AFP/GETTY IMAGES

JOE RAEDLE/GETTY IMAGES

Edward Snowden, shown on banner above, revealed secret surveillance by the government in 2013, and police sought to access the cellphone of an accused terrorist who killed 14 people at holiday party in San Bernardino, Calif., in December 2015.

The consequences aren't just personal; they're also political, according to Cardozo, who said privacy violations can have a chilling effect on First Amendment rights such as freedom of speech and freedom of assembly. "Privacy is how social movements get built," he said." Gay rights, civil rights, women's rights — agents of social change were dependent on privacy when they created each of these social movements. ... Without privacy, democracy breaks down."

So does creativity, according to Georgetown University Law Center professor Paul Ohm, who cited a 2013 survey by the PEN American Center, a literary and human rights organization. The research found that many American writers censor themselves in emails, on social media and in their writing because of concerns about government surveillance.

"We, as a society, should worry if the people we rely on to imagine our future and reflect on our past no longer feel unencumbered," Ohm said. "It's hard to quantify that kind of harm, but if we're all suddenly looking over our shoulder, it seems likely that we're heading toward a society that is less creative and less vital."

Of course, it's not just abstract art and ideas that are at risk when privacy is threatened. It's also concrete assets — like your identity. "When someone gets access to your personal information, it's not just because they're nosy; it's because they want to use that information," said Rotenberg. He pointed out that while the FBI has approximately 600 locked cellphones it wants to access for investigations, identity thieves potentially have access to 3 million phones that were stolen in the United States last year alone. Securing information from fraudsters, therefore, is perhaps even more important than securing it from government, he argued. "These stolen cellphones are leading to more crime, and that's a problem we shouldn't

CONTINUED »

600

APPROXIMATE NUMBER OF LOCKED CELLPHONES THE FBI WANTS TO ACCESS FOR CRIMINAL INVESTIGATIONS

3

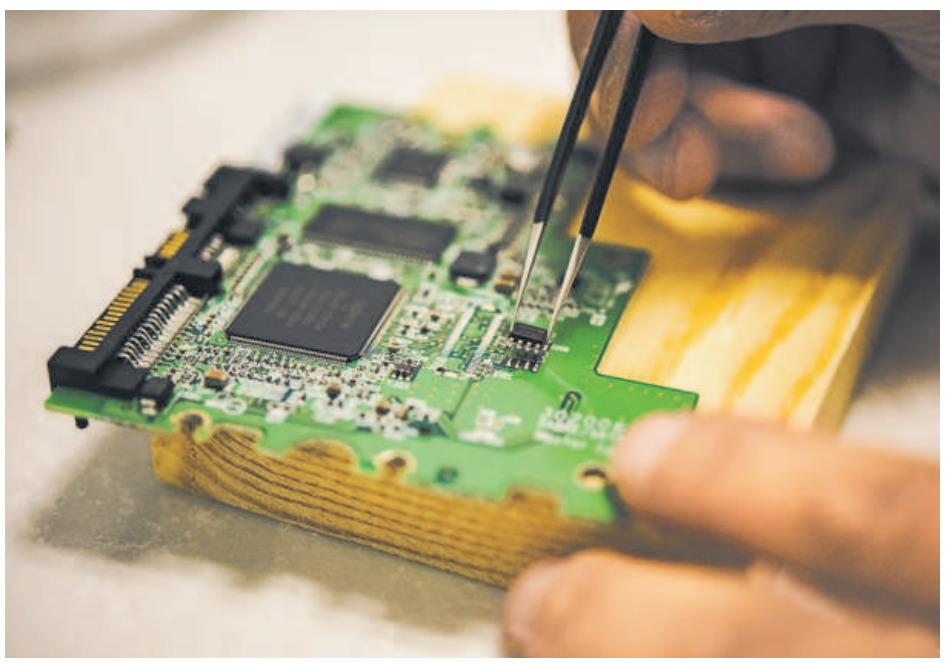
MILLION

NUMBER OF PHONES STOLEN IN THE U.S. IN 2015 THAT IDENTITY THIEVES COULD HACK

INSIDE OUR BORDERS

At the U.S. Immigration and Customs Enforcement's Cyber Crime Center in Fairfax, Va., specialists inspect confiscated digital equipment looking for evidence in criminal cases.

PHOTOS BY JOSH DENMARK/U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT



underestimate."

Which leads to the issue of public safety. While cellphones can enable crime, they can also be used to stop it, according to security experts, who point out the difference between Snowden's case, which involved secret surveillance, and the San Bernardino one, which involved legal forensics.

"(Forensic technology) is not an on-the-wire listening technology," explained Jeremy Nazarian, global chief marketing officer at Israeli mobile data forensics firm Cellebrite, which is rumored to be the company that helped the FBI unlock Farook's iPhone, although representatives wouldn't comment on the case. "It's a technology that can be used to obtain evidence from a mobile device only once that device is in custody as evidence."

Used lawfully — with probable cause and a warrant, for example — both surveillance and forensics can advance public safety by extracting information from cellphones that can help solve crimes, convict criminals and even exonerate innocent suspects.

"Public safety is clearly enhanced by virtue of an investigation being solved faster," Nazarian noted.

Then there's the fact that criminals are increasingly using mobile devices. When crimes such as human trafficking, narcotics smuggling and cybercrime are committed using cellphones, it stands to reason that cellphone evidence can play an important role in prosecuting them.

"Illicit activity is increasingly being conducted online. Between 2010 and 2015, (Homeland Security Investigations) has seen almost a five-fold increase of data seized and analyzed," said Dani Bennett, spokeswoman for U.S. Immigration and Customs Enforcement's Homeland Security Investigations, the principal investigative arm of the U.S. Department of Homeland

CONTINUED »

INSIDE OUR BORDERS

ZACH GIBSON/GETTY IMAGES

The U.S. Supreme Court ruled in 2014 that the warrantless search and seizure of a cellphone's contents during an arrest is unconstitutional. The case involved a suspect in San Diego whose mobile device was confiscated and searched by police when he was arrested in 2009.

Security. "The amount of seized data being analyzed coming from mobile devices compared with non-mobile devices is still a small percentage overall, but the trend is heading upwards dramatically."

DIGITAL DEFENSES

According to Sen. Ron Wyden, D-Ore., privacy and public safety are not mutually exclusive. "Our people want ... the best possible security and the strongest possible privacy protections," he said. "We can have both, although increasingly, the policies being proposed don't do much of either.

Wyden is leading the effort to change that as the sponsor of two bills that he hopes will lead the way on digital defense. The first, the Geolocation Privacy and Surveillance Act, or GPS Act, would require government agencies seeking location data from citizens' mobile devices to have probable cause and a warrant, and would prohibit private companies from sharing location data without customers' explicit consent. The second, the Secure Data Act, would prohibit government mandates to build security vulnerabilities or "backdoors" into mobile devices, like the one the FBI requested of Apple. The bill proposed by Sens. Richard Burr, R-N.C., and Dianne Feinstein, D-Calif., would mandate the opposite by requiring tech companies give the government access to plain-text user data. Wyden released a statement saying he would filibuster it if it reaches the Senate floor. As of mid-November, neither proposal has come to a vote.

"Federal law hasn't kept up with technology," Wyden said. "So from a legal standpoint, I think it's safe to say Americans' electronic ... data is up for grabs. I want clear rules that speak to how we'll keep people safe while also protecting their privacy."

The Supreme Court laid the foundation for exactly such rules in 2014, when it decided the landmark Fourth Amendment case *Riley v. California*. The court's unanimous decision held as unconstitutional the warrantless search and seizure of a cellphone's contents during an arrest.

> "It's very difficult for most consumers to control what happens to their data. For that reason, we need companies and governments to establish safeguards."
>
> **— Marc Rotenberg, president and executive director of the Electronic Privacy Information Center**

"Chief Justice (John) Roberts' opinion is a love letter to the smartphone," Ohm said. "It said that ... (constitutional protections) should be stronger for your smartphone than they are for even your bedroom."

As decisive as it was, *Riley* was only the first chapter on cellphone privacy. For instance, courts and lawmakers still must determine who owns cellphone data — the consumers who generate it or the companies that collect it — and for how long companies can retain it.

Industry also must do its part, according to the Electronic Frontier Foundation's Cardozo, who supports end-to-end encryption of cellphone data to protect it both on devices and in the cloud. "We need more corporations to do what companies like Apple and WhatsApp have done, which is encrypt data in transit in ways that no one can access it — not even themselves," he said, citing as an example his phone's ability to estimate the length of his commute home from work. "The way Apple has built its products, it doesn't know where I live or work; my phone does. With an Android phone, that information is processed on Google's servers instead of on the device."

Although few dispute the merits of security, Nazarian said the responsibility for protecting privacy rests with people, not technology. "There's nothing inherent in technology that leads to its misuse," he said. "It's up to our partners in law enforcement to follow the law ... in legally obtaining, accessing and managing evidence."

And up to consumers to be better stewards of their data in the first place, according to Ohm. "In some cases, we're (surrendering our data) in exchange for some really wonderful innovations — like Amazon on the fly and YouTube on the train. But for the average citizen, it's a really bad bargain," he concluded. "I think everybody could stand to think a little bit more about the risks. If they did, we would probably have a lot more laws and protections."