Society | DOI:10.1145/3416078 Keith Kirkpatrick

Who Has Access to Your Smartphone Data?

ISPs, app developers, and even the government may know more about you than you think.

IMAGE BY KOSHIRO K/SHUTTERSTOCK.COM

In a world that is defined by the generation and collection of data by technology and communications companies, personal information—including where people go, with whom they associate, what they purchase, and what they read, listen to, and even eat—it is quite a simple task to create a detailed profile of an individual based solely on the data captured in his or her phone.

The right to access and use the cache of personal information stored in each person's smartphone has become a major question about balancing personal privacy rights against governments' desire to monitor and retrieve data about its citizens' activities for law enforcement, public safety, and health issues. While much of the attention over the past several years has focused on demands from law enforcement to access this data to aid in criminal investigations, the COVID-19 pandemic of 2020 has refocused the debate on the government's right to access location data during health or other public safety emergencies.

Within the U.S., the primary communications privacy law that regulates the disclosure of and access to electronic data held by communication services providers, including wireless carriers, Internet Service Providers (ISPs), social media platforms, and search companies, among others, is the Electronic Communications Privacy Act of 1986 (ECPA) which, along with the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act OF 2001, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. As the Act explicitly states, "Some information can be obtained from providers with a subpoena; other information requires a special court order; and still other information requires a search warrant."

Andrew Crocker, senior staff attorney on the Electronic Frontier Foundation's civil liberties team, says the ECPA generally "requires the government to use legal process to get data about users," rather than simply allowing them to request and receive information from service providers.

Similarly, the Fourth Amendment of the U.S. Constitution requires law enforcement agencies to demonstrate probable cause when seeking historical location data from an individual's phone. This requirement was affirmed via a 2018 Supreme Court decision, in which Chief Justice John Roberts, writing on behalf of the majority, held that police are required to obtain a warrant in ordinary investigations, but could access such information without a warrant in an emergency, such as during a bomb threat, kidnapping, or other exigent circumstance where time is of the essence. However, law enforcement agencies do need to obtain a warrant after the imminent threat has passed, to demonstrate the inquiry was made in good faith.

"It would of course be more efficient to allow law enforcement officials to decide who to surveil on their own, without oversight by a court, but that would risk invasive surveillance at the whim of the government," says Crocker. "If there is a true emergency that makes getting a warrant impractical, such as an imminent threat to someone's life, the Fourth Amendment and these laws allow for a brief warrantless search, often requiring the government to come back to a court after the fact."

Former law enforcement officials agree, noting that there will always be some tension between the desire to protect personal privacy and the clear value of information that can be used to solve crimes or keep the public safe.

"It's definitely a challenge, and it's a balance between personal freedom and the ability of law enforcement to do their job, especially during the emergency circumstances that are putting others in harm's way," says Dan-

iel Linskey, managing director of the Security Risk Management practice of New York-based risk solutions provider Kroll, and head of the company's Boston office. Linksey, a former superintendent-in-chief of the Boston Police Dept., notes that in addition to the requirement to get a warrant to obtain information, the business models of Google and other collectors of personal data generally are focused on protecting privacy, rather than making it easy for law enforcement to access such data.

"I think there's a business decision to not share information with law enforcement unless absolutely necessary," Linskey says. "And even when necessary, the resources are not in place to make that a quick or timely process. The number of requests for information has overwhelmed Google, Yahoo, and any of those data providers to keep up with it and to provide information in a timely manner."

Law enforcement agencies have realized the value of obtaining information for use in criminal investigations, as the contents of email, location data, and private SMS messages often can provide the evidence needed to show intent, direct criminal activity, or illustrate that a suspect was in or near a specific location.

Also, the practice of obtaining subpoenas or warrants to obtain personal data from cellphones can be abused, according to George W. Price, a Boston-based attorney with Casner & Edwards LLP who is a former police officer, a former senior special agent with of the U.S. Drug Enforcement Administration (DEA), and a former special assistant district attorney for Middlesex County, MA. "I can find out more about someone through 24 hours of their phone and data use than probably anything else; it's really, really valuable," Price says.

"At the same time, people's expectations of privacy are different than they were 10 or 15 years ago on data devices. You may have a higher expectation now, because you're basically running your whole life through this digital device, which is not necessarily just used for criminal activity. So, I think we're in new territory, as far as how law enforcement can better access that."

"There are very few legal limits on what governments can do with even the most personal data once they have it."

Most technology companies realize the value of protecting personal information, at least within the U.S., where personal privacy is seen as a pillar of the U.S. Constitution. Says Price, "My sense is that [holders of personal data] are not afraid to push back on law enforcement when they feel like there is not enough evidence, or the warrant doesn't meet the proper standards."

Further, there is very little accurate reporting surrounding the effectiveness of warrants used to get private information from users' data in criminal cases, says Stephen Smith, a former federal magistrate judge in Houston, and now Director of Fourth Amendment & Open Courts at Stanford's Center for Internet and Society.

"If somebody would ask me what kind of legislation is most urgently needed right now, I'd say we need a reporting requirement for all these things, similar to what we have for the wiretaps," Smith says, referring to reports provided by federal and state officials on applications for orders for interception of wire, oral, or electronic communications. "We [would] have a complete picture of what's going on and could see how often these techniques are used for child predators, hostage-taking situations, or other really violent crime, versus how many of these are for identity theft, drug possession cases, or run-of-the-mill cases that don't really require the extraordinary means to get this stuff."

Protections on the collection of personal data are far slimmer in jurisdictions outside the U.S. For example, in the U.K., the police can download cellphone data without a warrant, and news reports indicate that cloud extraction technologies provided by companies such as Petah Tikvah, Israel-based Cellebrite and Alexandria, VA-based Oxygen Forensics can enable law enforcement agencies in the U.K. to continuously track social media accounts, as well as using facial recognition to analyze data extracted from the cloud. U.K. police departments cite three specific powers under which they derive their authority to access this information, including the Police and Criminal Evidence Act 1984 (PACE), the Investigatory Powers Act 2017, or the Regulation of Investigatory Powers Act 2000.

In Japan, the Ministry of Internal Affairs and Communications used to require mobile carriers to obtain the permission of users before sharing any location data with government authorities. However, in June 2015, this requirement was dropped, and news reports indicated some carriers were providing location data to the government, mostly relating to crime investigations. In response, Japanese mobile carrier NTT Docomo announced in May 2016 five smartphone models that would allow authorities to track their locations without users knowing.

Japan has asked owners of both public and private surveillance cameras, as well as wireless carriers, to make user data available to authorities without warrants. This practice, which the Japanese government believes is helpful in solving crimes, as well as tracking domestic abuse cases, is seen as one reason why Japan's crime rate is about a quarter that of the U.S.

The coronavirus outbreak earlier this year has led to even greater sharing of location data between mobile carriers and data collectors. Mobile carriers in Italy, Germany, and Austria shared location tracking info with authorities, while Taiwan, Singapore, and Hong Kong used location monitoring systems to ensure that people who were carrying COVID-19 were staying at home. Further, the Israeli government in March approved emergency measures that allowed its security agencies to track the mobile-phone data of people suspected to be infected with the coronavirus, as well as allowing authorities to enforce quarantines and warn those who may have come into contact with people infected with the virus.

"Realistically, cellphone tracking is already a pretty widespread practice," says Jennifer Fernick, a technology Fellow at the National Security Institute at George Mason University in Virginia, and the head of research and engineering with NCC Group, a global cyber security and risk mitigation firm based in Manchester, U.K. Fernick notes that in order for a cellphone to work, it must be able to connect to various cell towers, and as the phone connects with a tower, location information can be gathered. "So, to some extent that [location] data is already out there, as it is core to how cellphone networks are designed. To defend against that, there's not much you can do, other than put your phone in the fridge, or maybe throw it in the ocean."

Beyond simply using carrier data to track cellphone users, multinational technology companies, including Google, Unacast, Tectonix, X-Mode, and Facebook, among others, are now making available user location data that is captured via apps on users' smartphones, to track social-distancing efforts. While the data is anonymized—and users that have turned on location tracking have, by default, consented to this information being captured by accepting the terms and conditions of the apps they use—there is a fear that this information may be stored forever by authorities, and used in unrelated matters.

Fred Cate, vice president for research at Indiana University and founding director of the university's Center for Applied Cybersecurity Research, points to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and to the laws most U.S. states have "that give states enormous authority when addressing public health issues.

"I don't doubt for a moment that states have the authority to use this data, which in every case I am aware of they are getting from a third party, in any event. To my mind, the bigger challenge isn't whether they can get it, but what can they do with it once they have it?"

Cate says that while the Fourth Amendment clearly lays out the proper procedures for obtaining data (generally requiring the government to show it has a legitimate reason for needing the data), once the government has it, there are no laws covering how long the government may keep the data, or how it may be used in unrelated situations.

"There are very few legal limits on what governments can do with even the most personal data once they get it," Cate says, noting that in cases involving public safety, security, or health issues, "I suspect almost everyone would approve of the use. But what if, once the government has the data, they then use it for unrelated purposes?"

Cate notes financial information collected during a criminal investigation on money laundering, for example, could be turned over to the Internal Revenue Service if instances of non-related tax evasion activity were found, even in the absence of a criminal charge or conviction. Indeed, given the dearth of regulation, Cate says, there are no usage or time limits to what the U.S. government can do with that data.

"Some agencies have policies," Cates says. The U.S. Federal Bureau of Investigation (FBI), for example, "used to delete information about you when you turned 70 or 75, but that changed after 9/11. However, that was just an internal policy, and there was no legal force to that. In other words, there's no time limit on that data." C

Further Reading

The Fourth Amendment to the U.S. Constitution: https://constitutioncenter.org/interactive-constitution/amendment/amendment-iv

Google's Process for Handling Requests for User Information: https://bit.ly/3ahEKQh

How the U.S. Government is Tracking People via their Cell Phones, *The Wall Street Journal*, Feb. 10, 2020, https://www.youtube.com/watch?v=SXAShotdFZo

U.K. Police and Criminal Evidence Act 1984 http://www.legislation.gov.uk/ukpga/1984/60/contents

U.K. Investigatory Powers Act 2017 http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

U.K. Regulation of Investigatory Powers Act 2000 http://www.legislation.gov.uk/ukpga/2000/23/contents

Keith Kirkpatrick is principal of 4K Research & Consulting, LLC , based in New York, USA.

ACM Member News

CYBERSECURITY AT OAK RIDGE NATIONAL LABORATORY

"My father brought home a computer when I was in high school, and I taught myself to program on one of the early TRS-80s," says Deborah Frincke, associate laboratory director for the National Security Sciences Directorate at the U.S. Department of Energy's Oak Ridge National Laboratory (ORNL).

Frincke's early computing experience helped her to discover her passion. She went on to earn her undergraduate, master's, and doctoral degrees in computer science, all from the University of California, Davis.

After obtaining her Ph.D., Frincke joined academia as a professor of computer science at the University of Idaho. After that, she moved to the Pacific Northwest National Laboratory, where she rose to chief scientist for cybersecurity before leaving for the National Security Agency (NSA).

At the NSA, Frincke served in various roles, most recently as research director. She was also the agency's Science Advisor, which meant she needed to understand and advise on a diverse range of fields including mathematics, computer science, cybersecurity, quantum and high-performance computing, engineering, and various physical sciences.

Throughout her career, Frincke has focused on cybersecurity, especially collaborative approaches to defensive aspects of cybersecurity, to better protect systems and identify vulnerabilities.

At ORNL, Frincke is assembling a national security science directorate, which requires inventorying current cybersecurity initiatives at the facility, then determining how to strengthen them, and set the overall strategic direction.

"One of the things that excites me about this job is increasing my scope beyond those fields I led at NSA," Frincke says.

—John Delaney