PRIVACY

Increasingly, we use online services such as Gmail and Facebook for our private communications, while we store and back up sensitive personal documents in the "cloud" with Internet storage providers, such as Dropbox and Apple iCloud. Although criminals occasionally breach those services to access individuals' private information for nefarious purposes—from credit card fraud to offensive voyeurism—hackers pose only a modest threat to most Internet users, especially users who take reasonable security precautions online. And when such breaches do cause serious harm, stiff criminal penalties await those hackers who are caught and prosecuted.

Yet there is one adversary against whom existing laws offer limited relief: the government. Technological change has rendered obsolete the legal regime that Congress crafted to protect us against unwarranted government access to the private information we store electronically with third-party providers. From law enforcement to intelligence agencies, many government entities, however noble their intentions, possess powerful legal and technical tools for gaining access to our communications and "metadata" about them (metadata include information such as the date and time of a phone call, or the "to" and "from" addresses of an email, but do not include content-specific information).

As several recent leaks and newly declassified documents have revealed, the breadth of information secretly collected by the U.S. government from its citizens is staggering.

Therefore, Congress should require that all law enforcement and intelligence authorities do the following:

- Obtain a search warrant before compelling a provider to divulge the contents of a U.S. person's private communications or other personal information stored with a third-party provider.
- Obtain a search warrant before tracking the location of a U.S. person's mobile communications device.
- Obtain a court order on the basis of individualized, reasonable suspicion before it can compel a provider to divulge a U.S. person's call detail records under 18 USC § 2703 or Section 215 of the USA PATRIOT Act.

By modernizing existing privacy protections to reflect current technological realities, Congress can reaffirm its commitment to individual liberty in the information age and can ensure that the Internet remains a powerful engine of economic growth. Reforming those laws need not endanger crime victims or national security. Indeed, Congress can strengthen our privacy while preserving most of the tools that law enforcement and intelligence agencies need to do their important jobs.

The Stored Communications Act is the primary federal statute governing law enforcement access to private information stored by, or transmitted through, a third-party communications service (Electronic Communications Privacy Act of 1986, Public Law 99–508, Title II, 100 Stat. 1848 [1986]; codified as amended at 18 USC §§ 2701–10 [2012]). The law, enacted in 1986 as part of the broader Electronic Communications Privacy Act, provides for varying degrees of protection for information stored electronically with third parties. Some of those protections are fairly noncontroversial.

For instance, law enforcement may compel a provider to divulge so-called basic subscriber information, including a subscriber's name and address, with a standard subpoena (18 USC § 2703[c][2]). Yet the same standard applies when law enforcement wishes to access the *contents* of private data stored with a cloud backup provider or folder synchronization service. (The government must generally give a subscriber notice before accessing the contents of his or her records, although the government routinely delays such notice under 18 USC § 2705[a].) Those subpoenas are typically issued by a prosecutor and receive no judicial review whatsoever. On the other hand, the Stored Communications Act requires law enforcement to obtain a warrant issued upon a showing of probable cause before it may compel a provider to divulge the contents of a person's unopened emails stored remotely, provided that such emails are no more than 180 days old (18 USC § 2703[a]).

In 1986, when Congress crafted that law, the distinction between opened and unopened email—and between communications and other information stored electronically online—made sense, given the state of technology at the time. In 2014, however, Americans reasonably assume that their digital "papers and effects" are safe from warrantless government access—an assumption that is often

inaccurate. To remedy that mismatch between perception and reality, and to assure consumers that their data in the cloud are safe from law enforcement fishing expeditions, Congress should pass legislation based on the Email Privacy Act (H.R. 1852 in the 113th Congress), which enjoyed 270 cosponsors in the House—including most Republicans and nearly 100 Democrats. Congress should also require law enforcement to obtain a warrant before tracking the location of an individual's mobile device, except in emergencies that involve imminent threats to life, such as the kidnapping of a child.

Congress should also address the blanket warrantless surveillance of Americans' telephony metadata and other electronic information by the National Security Agency (NSA). That issue is distinct from law enforcement access, as U.S. intelligence agencies operate under a legal regime that parallels—but is largely distinct from—the Electronic Communications Privacy Act framework described above. Instead, the NSA's intelligence collection inside the United States is governed by the Foreign Intelligence Surveillance Act of 1978 (Public Law 95–511, 92 Stat. 1783 [50 USC §§ 1801–11]); and the USA PATRIOT Act of 2001 [Public Law 107–56, 115 Stat. 272]).

Unlike civilian law enforcement agencies, which must seek warrants, orders, and convictions through state and federal courts of general jurisdiction, the NSA and other intelligence agencies are overseen by the Foreign Intelligence Surveillance Court (known as the FISA Court) (50 USC § 1803). That specialized federal court hears only those matters involving national security and intelligence operations. Unlike most hearings held by civilian courts, the FISA Court's hearings are closed to the public, and most documents filed with the court are sealed as a matter of law. Until former NSA contractor Edward Snowden disclosed numerous classified documents to the *Guardian* and *The Washington Post* in 2013, little was publicly known about the substance of the FISA Court's opinions, or the activities it had authorized.

Among those documents was a FISA Court opinion interpreting Section 215 of the USA PATRIOT Act, a controversial provision that authorizes the Federal Bureau of Investigation to secretly seek a court order requiring a person or company to produce any "tangible things" related to an authorized investigation (50 USC § 1861). On the basis of that authority, the FISA Court issued an order that required Verizon's business unit to divulge to the NSA *all domestic telephony metadata* in the company's possession—including mobile phone data. The FISA Court has since renewed the Verizon order on numerous occasions, along with similar orders for information from an unknown number of other telephone companies.

Even if some small percentage of the telephony metadata collected by the NSA pertains to bona fide national security and intelligence-gathering operations, the digital dragnet authorized by the FISA Court cannot be reconciled with the principles codified in the Fourth Amendment to the U.S. Constitution—to outlaw the "general warrants" that British officials had used to search colonists' persons and papers without individualized suspicion. And although the Supreme Court has held that the Fourth Amendment does not implicate the collection of telephone records, Congress retains the ability to protect the American people by imposing limits on government officials that go beyond the bare minimum required by the Constitution.

Since the Snowden disclosures, the Obama administration has placed some limits on how officials may search the NSA's telephony metadata database, providing for judicial review of such queries in most circumstances. Yet those protections sidestep the fundamental problem with domestic surveillance. What matters most is not *how* the data are queried, but that the government forces companies to *divulge* their bulk records in the first place. Although the law should enable intelligence agencies to obtain telephony and other metadata from U.S. companies about individuals reasonably suspected to have direct involvement with a national security threat, such collection should be targeted and precise, not indiscriminate and suspicionless.

Experts: Ryan Radia, Wayne Crews

For Further Reading

Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *Guardian*, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

For a broader discussion of the Stored Communications Act and its various legal protections, see Orin S. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," *George Washington Law Review* 72 (2004): 1208, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860.