NY Electronic Communications Privacy Act (NY ECPA)

Policy Brief ::: Last Updated June 6, 2017

tl;dr:

New York's existing privacy laws require law enforcement to obtain a warrant before searching physical files, desktop computer hard drives, and postal mail. But law enforcement does not currently require a warrant when accessing private data stored in email, text messages, social media, or other online repositories. In light of increased use of mobile devices and cloud computing, both the New York Assembly and Senate have introduced nearly identical bills extending warrant requirements to electronic communication information. The bill contains exceptions for the recovery of lost or stolen devices and access to data in emergencies involving danger of death or serious physical injury.

Both an Assembly bill and Senate bill are pending. The bill will likely have a harder time in the Senate than the Assembly.

Impact on Members / Suggested Next Steps

If passed, the NY ECPA would substantially reduce the number of law enforcement requests for user data because, with the exception of emergency requests, every request would now require a warrant.[1] Any company that collects user data would be impacted by the new, more circumscribed warrant process, which includes a procedure for challenging the constitutionality of warrants and orders from law enforcement.

The Senate bill is fairly active at the moment. Any members who are willing to offer support for the bill should contact Tech:NYC.

The Assembly and Senate Privacy Bills

On January 13, 2017, a coalition of 19 Assembly members introduced A1895 (now A.1895a), the New York State Electronic Communications Privacy Act (NY ECPA). The bill would add a new article (§695) to the criminal procedure statute.

[1] Although a number of technology companies already have a corporate policy requiring a court order for access to user data (e.g., Twitter, Google), many companies do not.

- It would require that law enforcement obtain a warrant in order to compel the production of electronic communication information, including mobile device and cloud data, from a service provider or third party.[2]
- In the case of emergencies (danger of death or serious injury), law enforcement could access information without a warrant so long as they file with an appropriate court order authorizing such access within three days following such access.
- Warrant recipients (such as service providers) could petition the issuing court to quash or modify the warrant, or request the destruction of information obtained via such warrant, on the basis that the warrant violates the U.S. Constitution, the New York State Constitution, or is otherwise contrary to federal or state law.
- Law enforcement agencies would be required, once per year, to supply the attorney general's office with aggregate reporting data on information obtained under this new process.
- The bill would also authorize the Attorney General of New York to bring civil actions to compel law enforcement to comply.

On May 10, 2017, Senator Tony Avella introduced an essentially identical Senate bill (S.6044). Avella's Senate version of the bill would also amend the criminal procedure law by adding new article §695.

Background

- A number of state governments already require a warrant for access to electronic communication content. For example, California updated its statute in late 2015 to require a warrant where law enforcement seeks access to any metadata or digital communications, including emails, texts, or any documents stored in the cloud.[3]
- At the federal level, although Title III requires that federal law enforcement obtain a court order in order to intercept communications in real time, there are exceptions for emergency circumstances.[4] Furthermore, the federal ECPA governing law enforcement access to stored information—which was last revised in 1986—has been widely criticized for being outdated and out of touch with the way that people store and transfer information.[5]
- 74% of Americans say it is "very important" to them that they be in control of who can obtain information about them.[6]
- 91% of adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies.[7]

[2] The bill would also limit the use of so-called "Stingray" devices, which sweep up cell phone data by spoofing cell phone towers, a practice frequently used by law enforcement in states where the practice is still legal (including New York State).
[3] California Now Has the Nation's Best Digital Privacy Law, Wired, October 8, 2015.
[4] Title III of the Omnibus Crime Control and Safe Streets Act of 1968.
[5] See, e.g., 1986 Privacy Law Is Outrun by the Web, New York Times, January 9, 2011. The Electronic Privacy Information Center provides a good overview of the federal statute.
[6] The state of privacy in post-Snowden America, Pew Research Center, September 21, 2016.
[7] The state of privacy in post-Snowden America, Pew Research Center, September 21, 2016.

- In the second half of 2016, Facebook received 26,014 law enforcement requests affecting 41,492 user accounts. Facebook was able to produce the requested data in 83.46% of cases.[8]
- In 2016, 12 percent of Twitter's law enforcement requests in the U.S. were demands from New York law enforcement.[9]
- In 2016, Verizon received 265,035 law enforcement requests for customer data, but only 8 percent with a warrant.[10]

Stingray Devices

- Stingray devices connect to every cell device within range, not just the targeted device. The controversial devices are capable of both (a) recording numbers for a mobile phone's incoming and outgoing calls; and (b) intercepting the content of voice and text communications.[11]
- Several states, including California, Washington, Virginia, Minnesota, and Utah, now mandate that a warrant be issued for use of the Stingray devices. In 2015, the Department of Homeland Security and the Department of Justice also imposed new policies that require a warrant for Stingray use in most cases.
- The federal government has funded most local and state Stingray programs. Stingray use under the federal program is subject to stringent NDAs, meaning that judges and attorneys can't obtain crucial evidence during trial. For example, a Baltimore detective refused to answer questions on stand during a trial because he was bound by an NDA. The FBI has relied on this relative Stingray secrecy, in part, to avoid the kinds of Fourth Amendment challenges we increasingly see (below).[12]
- According to a 2016 congressional report, the Department of Homeland Security (DHS) operates at least 124 Stingray devices. Since 2015, DHS policy has required search warrants before deploying Stingray devices.
- The ACLU and EFF have been helping to bring legal challenges, such as in a case this spring in the D.C. Court of Appeals. Two courts have held that the Fourth Amendment requires the government to get a warrant before using a Stingray device: The Maryland Court of Special Appeals in 2016 and a federal court in Manhattan in a DEA case in July 2016.[13]
- We're starting to see reports that Immigration and Customs Enforcement (ICE) is using Stingray devices to locate undocumented immigrants.

---

[8] Facebook government requests report.

[9] Twitter transparency report.

[10] Verizon transparency report.

[11] According to documents obtained by the ACLU. Stingrays devices also go by names like cell-site simulator, triggerfish, IMSI-catcher, Wolfpack, Gossamer, and swamp box. They are about the size of a large suitcase.

[12] Five Disturbing Things About the FBI and Local Police Stingray Surveillance Programs, PrivacySOS, April 14, 2015. It's possible that data collected via use of federally-funded Stingray devices is aggregated and stored in federal law enforcement databases, meaning that millions of Americans are being surveilled and tracked.

[13] *United States v. Raymond Lambis*, SDNY, 2016.

FURTHER READING

- Public Perceptions of Privacy and Security in Post-Snowden Era, Pew Research Center, November 2014
- The state of privacy in post-Snowden America, Pew Research Center, September 2016
- The NYCLU NY ECPA page, including their one-pager
- The ACLU on Stingray devices
- Congressional report on Stingray devices from December 2016
- Feds are using Stingray cell-trackers to find undocumented immigrants, The Verge