NEW YORK STATE ELECTRONIC COMMUNICATIONS PRIVACY ACT

DIMITRI ANTONIO VALLEJO

JANUARY 30, 2020

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

@ the Urban Justice Center:
40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (646) 602-5600

NEW YORK STATE ECPA

Background

In 1968, Congress ushered in the modern wiretap age with the adoption of the Omnibus Crime Control and Safe Streets Act ("'68 Crime Bill"), creating a special warrant type for real-time collection of audio or video.[1] Almost 20 years later, Congress responded to the growth of digital communication with new—and often laxer—limits on collecting other types of communications, such as email, data transfers from computers, faxes, pagers and the metadata associated with phone conversations. Several decades later, these protections are woefully inadequate, as technological advancement continues to accelerate, but our laws remain decades out of date

The '68 Crime Bill mandated that law enforcement satisfy a series of requirements beyond what is required for a regular warrant before engaging in any real-time collection of audio or video, such as telephone calls and in-person conversations; the additional requirements are referred to as a "super warrant." The '68 Crime Bill, nevertheless, failed to account for the proliferation of nonaudio electronic communications, such as email, data transfers from computers, faxes, pagers and the metadata associated with phone conversations. Congress responded in 1986 with the Electronic Communications Privacy Act (ECPA) and Stored Communications Act, which created the 2703(d) Order ("d-Order")—a loophole around warrants that authorized law enforcement to compel the disclosure of private records simply by attesting that the information sought reasonably relates to an ongoing criminal investigation.[2]

The federal ECPA, similar to the '68 Crime Bill, fails to adequately protect Americans' reasonable expectation of privacy in novel forms of communication from intrusion by law enforcement. The Constitution generally ensures that searches and seizures by the government require a court-ordered warrant that "must be based on reliable information showing probable cause to search…[and] must state specifically the place to be searched and the items to be seized." The introduction of the super warrant in the '68 Crime Bill heightened warrant requirements in specific scenarios where law enforcement sought real-time collection of audio or video; law enforcement must show in those cases that the information sought not only relates to a series of horrible crimes, but also that the information is the only available means of obtaining the evidence necessary for proceeding with prosecution. Any request for a super warrant must also come from a senior supervisor, not regular officers or line attorneys, and the special warrants only last a designated period of time; after that period elapses, law enforcement must notify the subject of their wiretap. When the ECPA entered into force, however, archived electronic communications were removed from the category of private information governed

[1] Omnibus Crime Control and Safe Streets Act of 1968 [Public Law 90–351; 82 Stat. 197].
[2] Electronic Communications Privacy Act of 1986 [Public Law 99-508; 100 Stat. 1848].

by warrant requirements. Instead of ensuring law enforcement has probable cause for searching specific records, the d-Order authorizes the government to obtain electronic communications from third parties simply by claiming that such information is reasonably related to an ongoing criminal investigation.[3] As a result, the ECPA in the current era grants federal agents relatively easy access to huge troves of private civilian data, including: emails older than six months, messages transmitted via social media, any data stored on cloud services such as Dropbox, and even Facebook and Instagram photos.

Federal Case Law

Ever since the groundbreaking Supreme Court ruling in *Katz v. United States*, courts have generally employed the reasonable expectation of privacy test when assessing whether the Fourth Amendment applies.[4] This test considers two questions: 1) is there a subjective privacy interest; and 2) would society recognize that interest as reasonable? When both of these conditions are true, Fourth-Amendment rights and protections are applicable.[5] The existence of the d-Order forces the assumption that an individual's privacy interest in personal electronic data arbitrarily expires 180 days after its creation, authorizing law enforcement to ignore the Fourth Amendment and the reasonable expectation of privacy test. These are the legal loopholes that states such as California are trying to close by passing their own privacy acts.

State Legislation

At least one state has responded to the lack of federal protections with enhanced state warrant requirements. In 2015, the California legislature enacted a law that extended warrant requirements to cover civilian metadata and digital communications, including personal emails, texts, and remotely stored documents.[6] Regrettably, New York has failed to take similar action. The Constitution of New York State mirrors the Fourth Amendment, but also adds an additional clause specifically governing the "interception of telephone and telegraph communications," requiring that law enforcement must indicate "that there is reasonable ground to believe that evidence of crime may be thus obtained."[7] Therefore, ongoing wiretaps necessitate a warrant or court order. Nevertheless, this clause does not invoke the probable cause standard and, as a result, does little to protect against d-Order encroachments.

---

[3] The d-Order derives constitutional legitimacy from the 'Third-party doctrine' established by the Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 743-4 (1979): "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."

[4] *Katz v. United States*, 389 U.S. 347, 349 (1967).

[5] *Katz*, 389 U.S. at 361. Justice John Marshall Harlan: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."

[6] Kim Zetter et al., California Now Has the Nation's Best Digital Privacy Law WIRED (2019), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/ (last visited Nov 25, 2019).

[7] N.Y. State Constitution Art. I § 12.

New York's shortcomings are further exacerbated by court interpretations of its existing privacy laws, particularly its eavesdropping statute, which protects electronic communication from interception or access by law enforcement without an issued warrant.[8] While the statute's plain language seems to go further than the ECPA in requiring a warrant for "the intentional acquiring, receiving, collecting, overhearing, or recording of an electronic communication, without the consent of the sender or intended receiver thereof,"[9] recent court interpretations limit these regulations exclusively to communications "in transit" and do not cover information stored on a device.[10] In its 2016 *People v. Thompson ruling*, for instance, the New York Supreme Court held that stored emails were not protected by the eavesdropping statute because the law "is designed to cover communications in transit."[11] The next year, in *People v. Gordon*, the New York Supreme Court addressed a particularly-invasive form of in transit monitoring. It held that the use of a cell site simulator (or "stringray" device)[12] necessitates a warrant under New York's eavesdropping statute because it involves real-time and precise location tracking that reveals sensitive details tantamount to intimacies discoverable through eavesdropping or visual surveillance.[13] Nevertheless, New York continues to lack protections for the stored digital data that represents the overwhelming majority of contemporary privacy concerns.

The trajectory of federal case law is only slightly more optimistic for privacy reformers. In its 2014 *Riley v. California ruling*, the U.S. Supreme Court held unanimously that law enforcement needs a search warrant to access the contents of a cell phone;[14] this created a special rule for electronic storage devices outside the traditional 'search incident to arrest' doctrine[15] that allowed police officers to search any item on a person at the time of their arrest. The government argued that cell phones are identical to items such as cigarette packets during an arrest; therefore, as an officer may search a cigarette packet because it may contain contraband that could pose a threat to the officer, so should an arrest authorize

---

[8] N.Y. CRIM. PROC. LAW § 700.05(3) (McKinney 2013) (defining "intercepted communication" as including, "(a) a telephonic or telegraphic communication which was intentionally overheard or recorded by a person other than the sender or receiver thereof, without the consent of the sender or receiver, by means of any instrument, device or equipment, or (b) a conversation or discussion which was intentionally overheard or recorded, without the consent of at least one party thereto, by a person not present thereat, by means of any instrument, device or equipment; or (c) an electronic communication which was intentionally intercepted or accessed, as that term is defined in section 250.00 of the penal law").

[9] PENAL § 250.00(6).

[10] *Boudakian v. Boudakian*, N.Y. L.J., Dec. 26, 2008 [Sup. Ct. 2008].

[11] *People v. Thompson*, 51 Misc.3d 693 [2016].

[12] Cell site simulators, or stingray devices, sweep up electronic communications by connecting remotely to all mobile devices within range and extracting metadata associated with each phone's incoming and outgoing activities, even going so far as to intercept the content of voice and text communications without the devices owners' knowledge or consent. See "Five disturbing things about the FBI and local police stingray surveillance programs," Privacy SOS (2015), https://privacysos.org/blog/five-disturbing-things-about-the-fbi-and-local-police-stingray-surveillance-programs/ (last visited Nov 25, 2019).

[13] *People v. Gordon*, 58 Misc 3d 544 [Sup Ct 2017]

[14] *Riley v. California*, 573 U.S. ___ (2014).

[15] *United States v. Robinson*, 414 U.S. 218, 235 (1973): "In the case of a lawful custodial arrest the full search of a person is not only an exception to the warrant requirement of the 4th Amendment, but is also a reasonable search under that Amendment."

them to search the contents of a cell phone.[16] The Supreme Court unanimously rejected the government's argument and, in an opinion by Chief Justice John Roberts, established that cell phones contain such large volumes of sensitive information that they need additional Fourth-Amendment protections. Roberts compared warrantless searches of cell phones—which could reveal highly personal details about hopes, dreams, and intimate associations—to the general warrants used by British colonial authorities and decried by American revolutionaries. In 2018, in *Carpenter v. United States*, the Supreme Court ruled that collection of cell site location information (CSLI) for more than seven days required a warrant because "when the Government tracks the location of a cell phone it achieves near perfect surveillance as if it had attached an ankle monitor to the phone's user."[17] Although these recent cases held that Fourth-Amendment protections certainly extend to stored electronic communications in some cases, they do not specifically describe the line that, once crossed, violates constitutional protections. Therefore, while federal case law has confirmed the existence of privacy rights in electronic information, contemporary jurisprudence is insufficient for clearly delineating the particular data and contexts that invoke such constitutional privileges.

Given courts' narrow interpretations of New York privacy law, the act of acquiring stored electronic communications in the state largely mirrors the standard of the federal ECPA. Law enforcement, therefore, does not require a warrant to access any information stored in email, text messages, social media, or other data stored in the cloud. Even worse, because the ECPA authorizes law enforcement to compel data from third-parties by employing a d-Order, many innocent New Yorkers may find themselves caught up in sweeping requests by law enforcement without ever even receiving notice. In 2011, for example, after hundreds of peaceful Occupy Wall Street protesters were arrested for marching on the Brooklyn Bridge, the New York district attorney's office issued a d-Order to Twitter for nearly four months of user account data associated with one of the protesters. The d-Order included demands for tweet text, subscriber information, and IP addresses that would reveal their locations, simply because they engaged in non-violent civil disobedience.[18] The demand was deeply chilling to protesters, including those engaging lawful demonstrations protected by the First Amendment. These sorts of requests by law enforcement are the results of an ECPA that was crafted to operate in a society without the internet and other modern forms of digital communication. Ultimately, the ECPA is clearly inadequate for ensuring modern digital privacy protection.

The New York State ECPA

New York's best answer to the shortcomings of current privacy regulations is the New York State Electronic Communications Privacy Act (NYECPA), which has been co-sponsored by nine legislators in the New York State Assembly.[19] The NYECPA aims to protect the digital information of all New

[16] *Riley*, 573 U.S. (Opinion of the Court) Slip op. at 6.
[17] *Carpenter v. United States*, 585 U.S. ___ (2018). (Opinion of the Court) Slip op. at 13.
[18] *People v. Harris*, 949 N.Y.S.2d 590 (Crim. Ct. 2012).
[19] A.B. A1895, 241d Leg., Reg. Sess. (N.Y. 2017), https://www.nysenate.gov/legislation/bills/2017/A1895.

Yorkers by extending warrant requirements to cover all mediums of modern electronic communication, including:

> …the contents, sender, recipients, or format of an electronic communication; the precise or approximate location of the sender or recipients of an electronic communication at any time during such communication; the time or date such communication was created, sent, or received and information pertaining to an individual or device involved in the communication including but not limited to an internet protocol address.[20]

The NYECPA would also institute a near-complete ban on the use of stingrays and other forms of intrusive real-time metadata collection by law enforcement. Aside from adequately safeguarding every New Yorker's reasonable expectation of privacy, the NYECPA would also benefit all private companies that actively collect or store user data—such as Google, Facebook, Verizon, and Twitter—by significantly reducing the quantity of data requests pursued by law enforcement, as every demand would now require an accompanying warrant. Ultimately, the NYECPA substantially updates New York's privacy regulations by preventing law enforcement from issuing numerous and sweeping unwarranted demands to third parties for electronic communication information.

Conclusion

The last time federal law was updated to protect digital privacy was almost forty years ago, in the pre-internet world of 1986. Many of the legislators responsible for drafting and passing the ECPA had never held a wireless phone, let alone a pocket-sized smart device. Updated privacy protections are decades overdue, with existing federal laws insufficient for ensuring Americans' privacy rights. The NYECPA provides New Yorkers with working digital privacy safeguards that cover modern forms of communication—smart phones, social media, cloud storage, location data, and any other electronic information with a personal privacy interest.

[20] Id.

Surveillance Technology
Oversight Project, Inc.
40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT