NYCLU
NEW YORK CIVIL LIBERTIES UNION

MEMORANDUM: WARRANT REQUIREMENT FOR THE USE OF STINGRAYS IN NEW YORK AUGUST 2015

INTRODUCTION

The NYCLU prepared this legal analysis in response to recent revelations that law enforcement agencies in New York have acquired Stingrays—a powerful surveillance device that spies on nearby cell phones—without adopting policies that require warrants prior to their use. As detailed below, New York State has a broad eavesdropping law that not only protects against interception of conversations but also protects against non-consensual access to various forms of signal and data. The state eavesdropping law and constitutional precedent together make clear that law enforcement agencies should be obtaining a warrant prior to using Stingrays—and specifically, for most uses, an Article 700 eavesdropping warrant.

While the NYCLU urges the legislature and the courts to provide further clarification of these requirements in the near future, agencies that own these devices have an independent duty to follow the existing legal framework and respect the privacy of New Yorkers. They should review their practices immediately and adopt a warrant requirement into their policies.

FACTUAL BACKGROUND[1]

Cell site simulators, also known as IMSI catchers or "Stingrays,"[2] are powerful surveillance devices with military origins. Stingrays impersonate cell phone towers and, by sending signals to nearby cell phones, trick them into revealing their telephone numbers (mobile identification number), the unique numbers assigned to the phones by the manufacturer (electronic serial number), and cell phone location information—and in some configurations, also numbers dialed, contents of text messages, and contents of calls. By transporting this brief-case sized device in an aircraft or vehicle or by hand, law enforcement can locate any person who carries a cell phone, whether inside a home, a place of worship, a doctor's office, or any other place, and track the person's movements in real time. Given that 90% of American adults now own a cell phone,[3] Stingrays pose an unprecedented threat to Americans' right to be free of unwarranted government surveillance.

---

[1] This factual background on Stingrays draws from the following sources: Department of Justice, Electronic Surveillance Manual: Procedures and Case Law Forms (June 2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf; *NYCLU v. Erie County Sheriff's Office*, 47 Misc. 3d 1201(A) (Supreme Court, Erie County Mar. 17, 2015); Stephanie K. Pell & Christopher Soghoian, *A Lot More Than A Pen Register, And Less Than A Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J. L. & Tech. 134 (2013-4).

[2] "Stingray" is the name of the leading model of cell site simulators manufactured by the Florida-based Harris Corporation. It is often used in public discourse, and is used in this memorandum, to refer to all models of cell site simulators. Other models of cell site simulators available include Kingfish, Triggerfish, Hailstorm, and Harpoon.

[3] Pew Research Center, Mobile Technology Fact Sheet, *available at* http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.

LEGAL ANALYSIS

I. STATE STATUTORY LAW IMPOSES AN EAVESDROPPING WARRANT REQUIREMENT ON MOST USES OF STINGRAYS.

State law regulates most uses of Stingrays through the interaction of the Penal Law's eavesdropping provision and the Criminal Procedure Law's regulation of eavesdropping warrants. This is because New York's criminal prohibition on eavesdropping is broader than its federal counterpart. It regulates access to electronic communications beyond the interception of conversations. And it applies to law enforcement as it does to civilians, unless law enforcement has obtained an eavesdropping warrant or a pen register order. Because the definition of a pen register order is narrow and limited, however, most eavesdropping under state law—including most uses of Stingrays—requires an eavesdropping warrant.

A. Most Uses of Stingrays Fall Squarely Under the Penal Law's Limitation on Interception or Access to Electronic Communication.

New York's eavesdropping law criminalizes "unlawfully . . . intercepting or accessing . . . an electronic communication." Penal Law § 250.05. Under this provision, access to an electronic communication is unlawful unless done pursuant to an eavesdropping warrant under CPL Article 700 or a pen register order under CPL Article 705. *See* Penal Law § 250.00(8) (defining "unlawfully" as "not specifically authorized" by an Article 700 warrant or Article 705 order).

Significantly, unlike federal law, this provision of New York eavesdropping law regulates access to both contents of communications and non-content information—meaning that it regulates uses of Stingrays even when it is not being used to eavesdrop on phone conversations or messages. "Intercepting or accessing of an electronic communication" is defined as including "the intentional acquiring, receiving, collecting, . . . of an electronic communication, without the consent of the sender or intended receiver thereof." Penal Law § 250.00(6). "Electronic communication," in turn, is defined as "any transfer of signs, signals, . . . data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system," with four exceptions. Penal Law § 250.00(5).

Because Stingrays intentionally collect signals from a cell phone without the consent of the sender or the intended receiver—at all times the cell phone owner believes that the phone is connecting with a real cell phone tower and not a law enforcement device—their use is regulated under this provision unless a particular use falls under one of the four exceptions. Two of the exceptions are never applicable, as cell phones are not a "tone only paging device," *id.* § 250.00(5)(b), and signals from the cell phones are not "readily accessible to the general public," *id.* § 250.00(5)(d). The other two exceptions may apply depending on the use of Stingrays, although in both of these circumstances other legal protections apply to require law enforcement to obtain a warrant:

- Use of Stingrays to capture "telephonic or telegraphic communication." Acquisition of "telephonic or telegraphic communication" (defined as "any aural transfer" made through

wire, cable, or other like facilities) is exempt from the definition of "electronic communication" because intentional overhearing or recording of such "telephonic or telegraphic communication" without the consent of either party to the communication is regulated separately as "wiretapping." Penal Law § 250.00(5)(a); 250.00(1). Wiretapping is unlawful unless accomplished with an eavesdropping warrant. Penal Law § 250.00(8); § 250.05. Therefore, to the extent law enforcement are using Stingrays to capture "telephonic or telegraphic communication," the wiretapping regulations still require law enforcement to obtain an eavesdropping warrant.

- Use of Stingrays to track movement. The definition of "electronic communication" excludes any signals from a "tracking device consisting of an electronic or mechanical device which permits the tracking of the movement of a person or object." Penal Law § 250.00(5)(c). Some courts have held that when law enforcement tracks the movement of a cell phone, a cell phone can be considered a "tracking device" for the purposes of a federal-law definition similar to that of Penal Law § 250.00(5)(c). *See In re Application of U.S. for an Order Authorizing Use of a Pen Register with Caller Identification Device Cell Site Location Auth. on a Cellular Tel.*, 2009 WL 159187, at *3 (S.D.N.Y. Jan. 13, 2009) (holding that tracking locations of cell phones turns cell phones into a "tracking device" under the federal law equivalent to Penal Law § 250.00(5)(c)). Under this reasoning, the use of Stingrays to track the movement of a cell phone would be exempt from the definition of "intercepting or accessing of electronic communication." Even if Stingrays were exempt as a tracking device, however, *People v. Weaver*, 12 N.Y.3d 433 (2009), as explained in Part II, requires law enforcement to obtain warrants for just such tracking uses.

B. The Penal Law and Criminal Procedure Law Require Law Enforcement to Obtain an Eavesdropping Warrant, Not a Pen Register Order, When Intercepting or Accessing Electronic Communications.

As explained above, law enforcement must obtain a warrant under CPL Article 700 or a pen register order under CPL Article 705 to lawfully intercept or access an electronic communication. *See* Penal Law § 250.00(8). The pen register order under Article 705, however, does not authorize the use of Stingrays. The definitions of "pen register" and "trap and trace device" in CPL § 705.00 describe the primitive devices of the past that attach to landline phone lines and that work in a complementary manner to catch outgoing and incoming phones numbers. *See* CPL § 705.00(1) (describing a pen register as a device that attaches to a telephone line and captures "numbers dialed or otherwise transmitted"); CPL § 705.00(2) (describing trap and trace devices as devices that identify the "originating number"). Stingrays do not fall within the state-law definition of "pen register" and "trap and trace devices" because they do not attach to phone lines and, more importantly, they do not simply capture telephone numbers—they also capture the unique manufacturer number and location information. *See Application of U.S. of Am. for an Order Authorizing Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. 197, 200 (C.D. Cal. 1995) (holding that Stingrays do not fall within the federal definition of "pen register" or "trap and trace device," which at the time mirrored New York State definition). Unlike the federal-law definitions of "pen register" and "trap and trace devices," the state-law definitions have not been amended or broadened in recent years. *Cf. In re Application of the U.S. for an*

Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 749-50 (2012) (describing the amendments to the federal law). That state law has not been amended provides further support to the view that Article 705 should be read narrowly to authorize only the primitive pen register devices contemplated by the legislature previously.

Because judicial authorization to use Stingrays cannot issue under the pen register sections of the CPL, state law mandates that law enforcement using Stingrays to access electronic communications obtain a warrant under CPL Article 700. Penal Law § 250.00(8). Article 700 details a procedure for the issuance of a warrant for interception of or access to "electronic communication," a phrase that is explicitly defined in the CPL to include more than contents of such communication. CPL § 700.05(3). Article 700 also includes a procedure for temporary authorization in emergency situations. CPL § 700.21. These are the appropriate procedures to follow for using devices as powerfully intrusive as Stingrays.

II. THE STATE AND FEDERAL CONSTITUTIONS IMPOSE A WARRANT REQUIREMENT ON ALL USES OF STINGRAYS.

Even without the protections of state statutory law, the use of a device as invasive of privacy as Stingrays presumptively requires a warrant under the state and federal Constitutions. First, Stingrays can penetrate walls and locate cell phones within buildings where the police would not be able to achieve visual surveillance without a warrant. Thus the warrantless use of Stingrays violates the well-established constitutional right to privacy inside homes and other private spaces. *See United States v. Karo*, 468 U.S. 705, 715 (1984) (holding that it was unreasonable for the government to warrantlessly employ a beeper to determine whether a particular article was located inside a home at a particular point in time); *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (holding that use of thermal imaging to detect information on the interior of the home constituted a search).

Second, when Stingrays are used to track a person's location, whether in a public or private place, *People v. Weaver*, 12 N.Y.3d 433 (2009), mandates that law enforcement obtain a warrant. In *Weaver*, the Court of Appeals held that the state constitution requires law enforcement to obtain a warrant as a presumptive matter before using a GPS device to track a person's vehicular location over a 65-day period. *Id.* at 447. Such location monitoring, the Court recognized, reveals trips of "indisputably private nature" such as "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, [and] the gay bar." *Id.* at 441-42. Stingrays infringe on the privacy concern recognized in *Weaver* when used to track a person's movement with precision in a similar way as *Weaver*.

Third, the warrantless use of Stingrays, regardless of the manner or location of use, is an unconstitutional search of cell phones—their phone numbers and the electronic serial numbers, and in some configurations, numbers dialed, contents of text messages, and contents of calls.[4]

[4] To the extent Stingrays are intercepting the content of calls, text messages, or web pages visited, additional constitutional reasons require law enforcement to obtain a warrant. *See Katz v. United States*, 389 U.S. 347, 352-53 (1967) (holding that user of public telephones had reasonable expectation of privacy in conversations); *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (finding reasonable expectation of privacy in content of emails).

The Supreme Court has made clear that physically intruding on personal property for surveillance purposes is a search under the Fourth Amendment. *See United States v. Jones*, 132 S. Ct. 945, 949 (2012). Stingrays perform a search under *Jones* because they use signals to physically intrude into cell phones and compel them to disclose their contents. Moreover, this forced disclosure allows the law enforcement to search the contents of cell phones—a search that presumptively requires a warrant under *Riley v. California*, 134 S. Ct. 2473, 2485 (2014).[5]

Finally, recent reports indicate that Stingrays interfere with cell phone service and downgrade mobile devices from 3G and 4G connectivity to 2G.[6] Prolonged interference of cell phone service without a warrant may constitute an unreasonable seizure—an interference with a person's possessory interests in the cell phone and its service. *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (defining "seizure" for constitutional purposes as a "meaningful interference with an individual's possessory interests in that property").

For all these reasons, federal and state Constitutions require at minimum that law enforcement obtain a warrant before using Stingrays. As described above, Article 700 of the state law already sets forth the appropriate warrant procedure for the use of Stingrays in most circumstances.

CONCLUSION

Law enforcement agencies violate New Yorkers' right to privacy, as protected by constitutional and statutory law, when they use Stingrays without obtaining a warrant. Agencies should immediately adopt a Stingray use policy that requires that their officers obtain a warrant at minimum—and, in appropriate circumstances depending on use, an Article 700 eavesdropping warrant.

[5] The so-called third-party doctrine, under which it has been deemed that society has no reasonable expectation of privacy in phone dialing records that are maintained by the telephone company, does not apply here as law enforcement is obtaining information not from the telephone company but directly from the cell phone user. *Cf. Smith v. Maryland*, 442 U.S. 735, 741 (1979) (holding that there was no intrusion in a constitutionally protected area in part because the pen register was installed on telephone company property). Even if law enforcement need not apply for a warrant to obtain telephone dialing records from the telephone company, it certainly needs a warrant to enter a home or to seize and search through a phone to obtain the same records.

[6] *See* Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders*, Wired, Mar. 1, 2015, *available at* http://www.wired.com/2015/03/feds-admit-stingrays-can-disrupt-cell-service-bystanders/.