

and Its Impact on National Security and Consumer Privacy, 28 Harv. J. of Law & Technology 1 (2014).

- 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. of Law & Tech. 134 (2013).

3. My academic scholarship on Stingrays has also been cited by a number of federal and state courts.¹ Most recently, it was cited by the first appellate court to decide whether use of Stingrays requires a warrant. *See State v Andrews*, 227 Md App 350 [Md Ct Spec App Mar 30, 2016]. The court held that it does.

4. Similarly, my academic research on cellular phone location tracking by law enforcement has been cited by federal and state courts.²

5. I organized the first ever academic panel discussion about law enforcement use of Stingrays at Yale Law School in 2013. I have also lectured about Stingrays at several training events for federal judges, organized by the federal judicial center.

6. I completed a Ph.D. in Informatics at the School of Informatics, at Indiana University in 2012, and was, until 2012, a fellow at the Center for Applied Cybersecurity Research at Indiana University. I also hold a Masters in Security Informatics from the Johns Hopkins University and a Bachelor of Science in Computer Science from the James Madison University.

¹ In addition to *State v Andrews*, see also, e.g., *In re Application of the of America for an Order Relating to Telephones Used by Suppressed*, 2015 WL 6871290 [ND Ill Nov 9, 2015, No 15 M 0021]; *In re Cell Tower Records Under 18 U.S.C. § 2703(D)*, 90 F Supp 3d 673 [SD Tex 2015].

² See *United States v Pineda-Moreno*, 617 F3d 1120 [9th Cir 2010] [Kozinski, J., dissental]; *State v Earls*, 214 NJ 564 [2013]; *Commonwealth v Augustine*, 467 Mass 230 [2014].

7. I am currently employed as the principal technologist with the American Civil Liberties Union's Speech, Privacy, and Technology Project and am also a Visiting Fellow at Yale Law School's Information Society Project. I have previously worked in technical roles at the Federal Trade Commission, Google, Apple, and IBM. Attached as Exhibit A is a true and correct copy of my current resume.

8. I have personally filed a number of public records requests relating to the government's use of Stingrays. Attached as Exhibit B is a true and correct copy of the documents that I received from the U.S. Immigration and Customs Enforcement ("ICE") in 2012 in response to a Freedom of Information Act request.

Petitioner's FOIL Request

9. In preparing this affidavit, I reviewed the following materials:

- Petitioner's Freedom of Information Law Request, dated April 13, 2015;
- Affidavit of Gregory Antonsen, dated August 17, 2016;
- Affidavit of William Eric Chapman, dated August 17, 2016.

10. I understand that through Requests 1 and 3, which are at issue in this Petition, the petitioner seeks records that indicate the models of Stingrays owned by the NYPD, the dates of purchase, and the prices paid. Model names of Stingrays are names such as StingRay, StingRay II, Hailstorm, and KingFish.

11. A Stingray is a cellular surveillance device that impersonates a cellular network base station (commonly known as a "cell tower") operated by one or more wireless carriers. The Stingray tricks all nearby phones and other mobile devices that subscribe to those impersonated wireless carriers into revealing private, identifying information to the Stingray, which permits the

user of the Stingray to identify all nearby mobile devices and to track the location of particular phones.

12. Just knowing that the NYPD owns and uses Stingrays is like knowing that NYPD officers are issued guns. Some models of Stingrays and their optional software add-ons have different capabilities from other models, just like a handgun has different features and capabilities than an assault rifle. For example, a “StingRay system with FishHawk GSM Intercept S/W upgrade,” which the federal Drug Enforcement Administration purchased in 2007, can be used to intercept voice communications.³ As another example, the FOIA response that I have attached to this Affidavit showed that ICE owns an “Airborne Flight Kit” that allows the StingRay II to be mounted in an airplane, helicopter or drone, and, as a result, be flown over cities (*see* exhibit B at 2012FOIA5235 000010).

Affidavits of Gregory Antonsen and William Chapman

13. In their Affidavits, Inspector Gregory Antonsen of the NYPD Technical Assistance and Response Unit and William Chapman, a program manager and information technology specialist with the FBI, list a number of reasons that they believe that information about the NYPD’s acquisition and use of Stingrays should not be made public. Although Inspector Antonsen and Mr. Chapman state a number of specific technical opinions, they do not provide any evidence that they have sufficient technical expertise necessary to make such claims.

14. The public disclosure of models of Stingray products that the NYPD owns, the dates of purchase and the prices paid is in the public interest because it would advance a much-

³ Available at <https://www.fbo.gov/index?s=opportunity&mode=form&id=9aa2169a324ae7a1a747c2ca8f540cb3&tab=core&tabmode=list&=>. A true and correct copy of this web page printed on August 30, 2016, is attached to this affidavit as Exhibit C.

needed debate on how much the NYPD is spending on what types of surveillance capabilities. Similar debates are taking place in communities around the country. Disclosure of this information, however, would not result in the types of harms that Inspector Antonsen and Mr. Chapman describe in their affidavits.

Inspector Antonsen's Opinions

15. Inspector Antonsen claims that disclosing the model name of a Stingray may allow “terrorists or criminals” to “cho[ose] phone carriers that are not detected by that particular CSS model.” (Antonsen aff ¶ 30.) But as I explain below it is not the mere model name, like Hailstorm, KingFish, or StingRay, which reveals the wireless carriers that can be impersonated.

16. There are a few cellular technologies widely used by so called 2G and 3G cellular networks. These technologies include GSM and UMTS, which are used by AT&T and T-Mobile, while CDMA and CDMA2000 are used by Verizon and Sprint. The Harris Stingray-family products are capable of communicating with phones that use these different cellular technologies, providing that the relevant add-ons are purchased from Harris.⁴

17. For example, the invoices that the U.S. Immigration and Customs Enforcement produced to me in response to my FOIA request reveal that the agency purchased “Harpoon IDEN 800 MHz,” “CDMA Controller Software,” and “GSM Controller Software” (ex. B at 2012 FOIA5235 0035-0036). The phrases “CDMA,” “GSM,” and “iDEN” in these line items indicate what networks the Stingrays are capable of impersonating because of these add-ons.

⁴ Another cellular technology, iDEN, was used in the past by Sprint for its “push to talk” service, but the company turned off its iDEN network in 2013. *See* Neal Gomba, *It's Dead, Jim! Sprint iDEN Has Finally Been Shut Down*, Extreme Tech, July 1, 2013, <http://www.extremetech.com/electronics/160033-its-dead-jim-sprint-iden-has-finally-been-shut-down>. A true and correct copy of this article printed from the website on August 30, 2016, is attached as Exhibit D to this affidavit.

18. Although it is hard to imagine that the NYPD has not purchased the add-ons necessary to conduct surveillance on all U.S. cellular networks, I understand that the petitioner has agreed to redact information about particular add-ons that would reveal the cellular networks that they work with (i.e., the phrases “CDMA,” “GSM,” etc.).

19. Inspector Antonsen also states that people have been taking unspecified “countermeasures” to defeat Stingrays (Antonsen aff ¶ 33). It is true that cybersecurity researchers and defense contractors have developed technical countermeasures capable of detecting, and in some cases, thwarting tracking and other surveillance by Stingrays. It was the public availability of detailed technical information about Stingrays, such as through patent filings and in academic research (*see* exhibits G-J), not the disclosure of invoices and government contracts, that aided this development.

20. The most effective countermeasure, which can be used by anyone at no-cost is to simply turn off a phone or put it into airplane mode. This will thwart tracking by any model of Stingray. Knowing the models of Stingrays that the NYPD uses does not make this countermeasure more or less effective. It is 100% effective regardless of which models of Stingrays the NYPD uses.

21. Inspector Antonsen also claims, without citing any evidence, that revealing the model names will make the NYPD’s Stingrays more vulnerable to hacking (Antonsen aff ¶ 34). This is akin to the NYPD refusing to reveal whether the agency has issued new iPhones to police officials because public disclosure of the fact that police officers are using iPhones will leave them vulnerable to hacking.

22. Contrary to Inspector Antonsen's claims, there is no legitimate cybersecurity justification to keeping secret the names of the particular Harris products used by the NYPD. It would be a serious problem if the costly surveillance devices purchased by the NYPD without public competitive bidding are so woefully insecure that the only thing protecting them from hackers is the secrecy surrounding their model names. The Harris Corporation, which in addition to manufacturing Stingrays has been awarded public contracts for securing the President's communications and supplying secure radios used by the U.S. Army,⁵ is clearly capable of designing secure products for its government customers that does not rely on keeping secret the mere existence of the devices for their security.

23. Inspector Antonsen suggests that revealing which devices have and have not received critical security patches could expose those devices to compromise by hackers (Antonsen aff ¶ 34). First, none of the many Harris invoices or purchase records from other state, local and federal agencies that I have reviewed have ever revealed which specific software updates an agency has or hasn't installed, just as records revealing that an agency had purchased iPhones for officers would not reveal which particular iOS security updates the agency had or hadn't installed on those devices. Second, it is my understanding that the petitioner has agreed to redact particular software version numbers from the records it is seeking if the NYPD's records reflect this information.

⁵ Contracts, U.S. Dept. of Defense, Aug. 20, 2014, <http://www.defense.gov/News/Contracts/Contract-View/Article/606003>. A true and correct copy of this document printed from the website on August 30, 2016, is attached as Exhibit E to this affidavit. *See also* Harris Corp. Awarded \$1.7B Army Contract, Orlando Business Journal, June 23, 2016, <http://www.bizjournals.com/orlando/news/2016/06/23/harris-corp-awarded-1-7b-army-contract.html>.

24. Inspector Antonsen further states that revealing the number of Stingrays in use would “permit terrorists to determine locations at which [the Stingrays] are likely to be used” (Antonsen aff ¶ 35). But there are approximately a half dozen federal agencies that use Stingrays, including the Federal Bureau of Investigations, the U.S. Marshals, the Secret Service, the Drug Enforcement Administration, the Immigration and Customs Enforcement and the Internal Revenue Service.⁶ When used, these devices impersonate legitimate cellular networks, so even if a sophisticated party were able to detect that a Stingray is in use in a particular part of New York City there is no way for them to identify it as a NYPD Stingray, or a device used by any other federal, state or local government agency. As a result, even if the number of Stingrays owned by the NYPD is known, there is no way to know that just because a Stingray is being used in one location another Stingray that belongs to the NYPD or another agency is not being used elsewhere.

25. Inspector Antonsen also claims that knowing the number of Stingrays owned by the NYPD may enable an extremely well-resourced criminal group to orchestrate a greater number of simultaneous hostage situations than the number of Stingrays available to the NYPD (Antonsen aff ¶ 35). Even assuming that such a sophisticated criminal group made the unlikely decision to rely on its knowledge of the number of Stingrays in the NYPD’s possession to use cell phones in executing such a hypothetical event, knowing that number will not help them as it is almost certainly the case that one, if not multiple, federal law enforcement agencies would step in and assist the NYPD with their own cellular surveillance technology. Moreover, this hypothetical is no different from saying that at some point some criminal group may be able to

⁶ See <https://www.aclu.org/map/stingray-tracking-devices-whos-got-them>.

overwhelm the number of police cars that the NYPD owns or the number of police officers on the force.

Mr. Chapman's Opinions

26. Mr. Chapman of the FBI expresses concern over unnamed adversaries being able to “construct and successfully operate their own [Stingrays] against Federal, state, and local law enforcement, other Government entities, and the military, thus impeding effective functioning of the Government, law enforcement, and the military, all of which would endanger public safety and national security.” (Chapman aff ¶ 22 Category 1(a).)

27. First, merely revealing the model names of particular Harris products the NYPD has purchased—information that is printed on Harris’s price list of products marketed to federal agencies that has been published by the General Services Administration and included in invoices released by numerous other local, state and federal agencies, including the FBI⁷—will not result in the disclosure of any new technical information about how the Harris products function under the hood.

28. Second, if the FBI is concerned that foreign governments, criminals and hackers can make or manufacture their own Stingray-type devices, that ship sailed long ago. Dozens of surveillance companies from countries around the world now manufacture and openly advertise Stingrays for sale. (*See Pell & Soghoian*, 28 Harv. J. of Law & Technology at 41-42.) Even the Harris Corporation’s products are openly sold to foreign buyers. For example, a few years ago, I

⁷ Carl Prine, *FBI Closely Guards Details of Spy Gear Technology*, Trib Live, Feb. 16, 2014, <http://triblive.com/news/alleghey/5548583-74/fbi-technology-projects> [“Harris alone secured 68 FBI contracts worth at least \$23.7 million. Purchases included Harris devices such as the StingRay, Amberjack, Kingfish and Gossamer trackers, plus spare parts and classroom instruction”]. A true and correct copy of this article printed from the website on August 30, 2016, is attached as Exhibit F to this affidavit.

downloaded a Harris Corporation product catalogue, written in Portuguese, from the website of a Brazilian surveillance technology reseller that included significant amounts of technical information about the specifications of different Harris products.

29. Like the FBI, I too am worried about the threat posed by foreign governments, criminals and hackers illegally using Stingrays in the United States. Indeed, in 2012, I organized a demonstration of a home-made Stingray for Congressional staffers in an attempt to alert Congress to the risk that Members of Congress faced from foreign governments attempting to spy on their calls.

30. However, shielding from public disclosure the names of the models of Stingrays that the NYPD has purchased will not stop foreign intelligence services from spying on the phone calls of U.S. politicians, nor will it somehow make it harder for hackers or hobbyists to build their own Stingrays. Indeed, graduate students have written lengthy theses about Stingray technology,⁸ and several Stingray manufacturers, including Harris, have submitted detailed, public patent applications that describe their interception technology.⁹ No matter how much the NYPD and FBI would prefer that information about their cellular surveillance technology remain a secret, the cat has been out of the bag for more than a decade. (*See generally* Pell & Soghoian, 28 Harv. J. of Law & Technology at 40-54.)

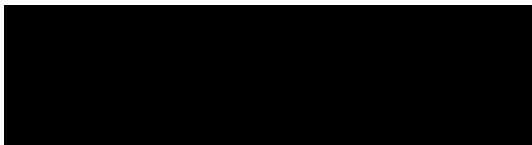
⁸ See eg Daehyun Strobel, IMSI Catcher 13 (July 13, 2007) (unpublished seminar paper, Ruhr-Universitat Bochum), available http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf. A true and correct copy of this article printed from the website on August 30, 2016, is attached as Exhibit G to this affidavit.

⁹ Patent applications filed by the Harris Corporation are publicly available on the U.S. Patent and Trademark Office website at www.uspto.gov/. True and correct copies of these patent applications number 7,592,956, number 5,719,584, and number 5,687,196 are attached as Exhibits H, I, J to this affidavit, respectively.

31. Technically sophisticated people can now build and operate their own Stingrays. This will remain the case whether or not the names of the Stingray products purchased by the NYPD are made public.

32. Mr. Chapman also expresses concerns that disclosing model names of Stingrays “would reveal the specific resources available to the police department (as well as those not available to it).” (Chapman aff ¶ 22 Category 2 (a).) In this regard, Stingrays are not unique. Knowing whether the NYPD owns a particular model of Stingray would reveal the resources of the NYPD in the same way that revealing that it owns a particular model of a drone, body camera or police car would reveal the resources available to the NYPD.

33. Mr. Chapman also raises the possibility of the development of “heat maps.” It is not clear what Mr. Chapman means by a heat map, but to the extent it means a map of locations in New York City where Stingrays are most frequently used, the disclosure of model names, numbers of Stingrays, and their price would not aid in the development of such a map because they do not reveal when, where, or how frequently the NYPD uses its Stingrays.



Christopher Soghoian

Dated: August 31, 2016
New York, NY

Sworn to before me this
31st Day of August, 2016



NOTARY PUBLIC

