SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

---------- x

NEW YORK CIVIL LIBERTIES UNION,

Petitioner,

-against-

THE NEW YORK CITY POLICE DEPARTMENT,

Respondent.

---------- x

AFFIDAVIT OF GREGORY ANTONSEN IN SUPPORT OF RESPONDENT'S VERIFIED ANSWER

Index No. 100788/2016
I.A.S. Part 17
(Hagler, J.)

STATE OF NEW YORK)
) SS:
COUNTY OF NEW YORK)

GREGORY ANTONSEN, being duly sworn, deposes and says as follows:

1. I am an Inspector in the New York City Police Department ("NYPD"), and currently serve as Commanding Officer of the Technical Assistance and Response Unit ("TARU"). I have been employed by the Department since 1985, and have held my present position since 2015. I have previously served as Commanding Officer of the Financial Crimes Task Force and Major Case Squad and have commanded an Investigative Unit for over 12 years.

2. In my current capacity as Commanding Officer of TARU, I oversee approximately 100 detectives, supervisors and civilians. TARU provides both covert and overt technical assistance to NYPD investigations conducted by the Detective Bureau, Intelligence Bureau, and Internal Affairs Bureau.

3. I am fully familiar with the facts and circumstances stated herein. This affidavit is based on my personal knowledge, as well as upon information and belief based on information provided by other employees of the NYPD and on records of the NYPD maintained

in the ordinary course of business, which I believe to be true and accurate. I submit this affidavit in support of Respondent's Verified Answer to the Petition.

Summary

4. I am informed that the Petitioner in this case, the NYCLU, has submitted a Freedom of Information Law ("FOIL") request to NYPD seeking records relating to NYPD's use of cell site simulation ("CSS") technology, commonly known as "stingray" devices. Specifically, Petitioner seeks (1) "purchase orders, invoices, contracts, loan agreements, and other similar records regarding the NYPD's acquisition of cell site simulators," and (2) an unredacted version of NYPD's non-disclosure agreement with the Harris Corporation, which shows model names and numbers of cell site simulators (together, hereinafter, "Withheld Records").

5. The purpose of this affidavit is to explain the reasons that disclosing the Withheld Records would cause grave damage to NYPD's counterterrorism and law enforcement operations, and so could endanger the lives or safety of New Yorkers.

6. Additionally, disclosing the Withheld Records would reveal confidential and non-routine criminal investigative techniques, which would hamper NYPD's ability to conduct operations and would permit perpetrators to evade detection. Moreover, disclosure of the Withheld Records would jeopardize the ability of NYPD to secure its information technology assets.

NYPD's Counterterrorism Operations and Use of Technologies

7. From past experience, NYPD is aware that terrorist and criminal organizations, and individuals that contemplate terrorist operations against New York City, are likely to scrutinize NYPD's counterterrorism operations, its responses to criminal activity, and its documents, so as to discern information concerning NYPD's capabilities, techniques,

strategies, and operational tactics, all of which could assist them in planning and successfully executing their crimes, while evading detection and capture.

8. NYPD uses a variety of technologies in protecting the City from crime and from terrorist attacks. Some of these technologies are highly specialized and are essential in preventing, or thwarting, terrorist attacks.

9. However, the success of operations using such specialized technologies depends on NYPD's ability to carefully guard information relating to the specifications of these technologies so that would-be criminals could not develop or utilize strategize that defeat or overcome their capabilities. Such a principle applies here.

10. A great vulnerability the NYPD counterterrorism program faces is the release of information that would reveal, or tend to reveal, the extent, scope, and limitations of NYPD's operations, as such information would allow terrorists to more easily develop and execute their plans.

11. NYPD's counterterrorism programs have become models for other municipalities worldwide. Because of this, our relationships with other federal, state, local, or foreign law enforcement and intelligence organizations would be damaged if we were unable to protect documents that should not be released because they detail non-routine criminal investigative techniques used by NYPD and which are also be employed by other organizations such as the FBI and Department of Homeland Security.

CSS Technology

12. CSS technology is perhaps the most reliable method available to law enforcement to locate individuals in real time who are participating in the commission of a crime.

13. As most individuals, including criminals and terrorists, rely on cellular technology for communications and information, and thus keep cellular phones on their person, locating an individual's phone using CSS technology is often tantamount to locating the individual.

14. At a minimum, the technology may permit law enforcement to identify locations where the individual had recently been present, thus allowing law enforcement officials to canvas an area and interview witnesses.

15. In a terrorist or hostage situation, such technology is absolutely invaluable and can make the difference between locating a suspect in a matter of hours or days, and locating a suspect in a matter of minutes, thus preventing the commission of worse acts of terror.

16. As already disclosed publicly, NYPD uses CSS technology in two circumstances: First, NYPD may be granted a court order pursuant to federal and state statutes and based on a probable cause finding which authorizes the use of a pen register, trap and trace, and the cell site simulator, and which also authorizes the seizure of cell site and other relevant information from a target cell phone or device.

17. Second, NYPD may use CSS technology when an exigent circumstance requires the use of the technology, such as the kidnapping of a child or to interrupt an imminent terror attack. In fact, locating the cell phone often leads to the apprehension of a criminal suspect.

18. For example, earlier this year, NYPD was notified that a young girl was being held against her will in New York City, although she was able to make very brief calls on her cell phone. Using the girl's cell phone number, NYPD was able to deploy CSS technology in an attempt to locate the phone. NYPD located the phone and, upon further investigation, it was

discovered that the girl had been forced into prostitution by her captors for some weeks. Fortunately, because of the use of the CSS, NYPD was able to rescue the girl on the same day it was notified that she had been abducted.

19. Similarly, just this month, an elderly woman with diminished mental capacity had been missing for over twenty hours. She was in dire need of medical attention because she had a chronic heart condition for which she required medication. Fortunately, she had kept her cell phone on her person. NYPD deployed a CSS and was able to locate the elderly woman. She was rushed to the hospital, where she received medical attention. Had NYPD not been able to use the CSS, she might not have survived until she was located.

20. For another example, several years ago, a man was kidnapped at gunpoint in Brooklyn. The next day, the kidnappers contacted the man's family by phone and made a ransom demand. The man's family notified the police, who immediately began tracing calls to and from the kidnappers' cell phone. The police were able to locate the general vicinity of the cell phone, and deployed CSS technology to find the phone's specific location. Within an hour of using the CSS, the police located the kidnappers' phone, which was in a car. In the trunk of the car was the kidnapping victim, who was bound, gagged, and unconscious, having been severely beaten. He was taken to the hospital, where he survived, despite having suffered a fractured skull. Without the use of the CSS technology, the police may not have been able to locate him in time to save his life.

21. These are just three of hundreds of stories about how NYPD's use of CSS technology has saved lives and led to the apprehension of perpetrators of serious crimes. Were NYPD required to reveal the specifications of this technology, such examples of success might not be possible.

22. CSS technology is also in use by numerous law enforcement agencies around the country, including the FBI and federal Department of Homeland Security. Upon information and belief, certain branches of the U.S. armed forces employ CSS technology to locate insurgents and terrorists abroad. CSS technology is thus a crucial device in preventing terrorist attacks and in stopping crimes.

The Withheld Records Should Not be Released Publicly

23. As discussed in greater detail below, the disclosure of the Withheld Records would reveal the precise specifications of CSS technology in NYPD's possession, including each specific technology's general capabilities. When combined with other publicly available information, the Withheld Records would reveal the precise capabilities, limitations, and likely uses of the CSS devices in NYPD's possession.

24. Based on information that has already been released publicly, various types and models of equipment exist for purchase by law enforcement agencies from Harris Corporation such as the Stingray, Stingray II, Triggerfish, Gossamer, Harpoon, Amberjack, Kingfish and software such as FishHawk and Porpoise. Each product has a different function or capability.

25. For example, some of the above listed models are hand-carried, while some are designed to mount in vehicles. One is an antenna to broaden the search range of the CSS. Some software boosts a device's capabilities to include eavesdropping. Other software allows law enforcement to intercept text messages. Certain models are only able to locate phones associated with certain phone carriers.

26. The different models were introduced to law enforcement in different years. In addition, the different items and models cost different amounts.

27. While the law prohibits dissemination of brochures describing the technology in more detail, the Petitioner has nonetheless posted such prohibited information on its website. See http://www.nyclu.org/files/AmberJack_ProductDescription.pdf (last visited August 16, 2016). Other information describing the equipment is also available on the internet.

28. Because many of the specifications of the technology are now publicly available, disclosing NYPD contracts and purchase orders with the Harris Corporation, which contain the models, costs, and years of purchase, would reveal the exact capabilities, and conversely the limitations, of NYPD equipment.

29. Telegraphing the NYPD's capabilities and limitations would provide crucial information to criminals and terrorists. Such information would allow them to circumvent one of NYPD's most essential technological capabilities and methods in the event of an emergency.

30. For example, if it is disclosed that NYPD has a particular model of stingray, terrorists or criminals might chose phone carriers that are not detected by that particular CSS model.

31. As with any specialized technology, it would be harmful if such information were made public, and it would greatly hamper law enforcement efforts to manage a non-routine technology. However, even if the model names or technical specifications were redacted from the Withheld Records, the remaining records would still allow the public to determine the number of any CSS technologies purchased, and would permit the public to infer technical specifications based on the cost, timing or frequency of the contracts or purchase orders, training provisions, servicing provisions, and necessary software or hardware updates, all of which are included in the Withheld Records.

32. Public knowledge of this kind of information would undermine any deterrent effect achieved through the lack of disclosure of more specific information.

33. In areas outside of New York City, law enforcement agencies have observed an increase in the number of "countermeasures" taken by criminals to defeat CSS technology. While some of these countermeasures require a high level of technical sophistication (and are primarily in use on the U.S./Mexico border), other more accessible methods are also available and are employed by criminals seeking to evade detection. Although it is prudent not to discuss the details of such countermeasures in a publicly filed affidavit, suffice it to say that NYPD is concerned that such countermeasures could be used in New York City, and could cause great difficulty should NYPD need to use its CSS technology during an emergency situation.

34. The CSS technologies are also critical and essential information technology assets. As such, all CSS technologies require periodic software updates. Public disclosure of the specifications of the CSS technologies in NYPD's possession from the Withheld Records would make the software vulnerable to hacking and would jeopardize NYPD's ability to keep the technologies secure. Of great concern is that a highly sophisticated hacker could use the knowledge of NYPD's CSS technologies to invade the CSS software undetected, thus creating a situation in which law enforcement personnel are lured into a situation based on a misleading cell-phone location and are then trapped and ambushed.

35. Moreover, knowledge of the number of CSS devices in use would permit terrorists to determine locations at which the CSS technologies are likely to be used, and, by using this information, to design an attack to overwhelm the Department's available resources, for example by choosing to create so many simultaneous hostage situations around the City that NYPD is not able to locate each set of hostages using its CSS technology.

36. Any such attack would, of course, endanger public safety. Moreover, because the CSS technologies can be used to assist in locating terrorists who are participating in an ongoing attack, if the Department's available CSS resources were deliberately overwhelmed, such an attack would likely lengthen the amount of time terrorists were at large, potentially causing more casualties.

37. Finally, disclosure of the Withheld Records could impair NYPD's relationships with other law enforcement agencies with which we partner. These agencies may use similar devices and implicitly rely on NYPD to keep the kinds of information contained in the Withheld Records confidential. Disclosure of the Withheld Records could also impair NYPD's relationships with the corporations who manufacture and supply these devices to NYPD, thus preventing NYPD from gaining access to this crucial technology in the future. Indeed, upon information and belief, the Harris Corporation has stopped selling CSS technology to municipalities because it no longer trusts municipalities to keep its proprietary information confidential.

38. Accordingly, it is apparent to me based on my expertise in criminal investigations that disclosure of the Withheld Records would reveal non-routine law enforcement techniques, would hamper NYPD's criminal investigations and intelligence operations, would jeopardize the ability of NYPD to secure its information technology assets, and could endanger the lives and safety of New York's residents and visitors.

[redacted]

Gregory Antonsen

Sworn to before me
this 17 date of August, 2016

[redacted]

Notary Public

EILEEN G. FLAHERTY
Notary Public, State of New York
No. 02FL6075185
Qualified in Kings County
Commission Expires Nov. 8, 2018