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

----------x

In the Matter of the Application of

JAMES LOGUE,

Petitioner,

-against-

NEW YORK CITY POLICE DEPARTMENT,

Respondent.

----------x

Index No. 153965/2016
I.A.S. Part 13
(Mendez, J.)

AFFIDAVIT OF CHRISTOPHER SOGHOIAN

COUNTY OF NEW YORK)
ss :
STATE OF NEW YORK)

CHRISTOPHER SOGHOIAN, being duly sworn, deposes and says:

1. I make this affidavit in support of Petitioner's reply in the above-captioned Article 78 proceeding. The statements I make herein are based on my personal knowledge, except where stated as on information and belief.

2. I am employed as the principal technologist with the American Civil Liberties Union's Speech, Privacy, and Technology Project. I am also currently 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.

3. 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

statements and claims related to cybersecurity, it is unclear if he has any technical expertise necessary to support such claims.

8. Assistant Chief Donohue does not describe the specific nature of the "multimedia records," but based on his assertions about those records, and based on my knowledge of police surveillance practices, I assume that the "multimedia records" are comprised of still photographs, video recordings, and/or audio recordings created from either handheld devices carried or worn by the undercover officers the NYPD assigned to surveil the protests or from stationary devices installed within Grand Central Terminal.

9. Assistant Chief Donohue first claims that copies of these responsive photographs and video and/or audio recordings, if disclosed, will reveal the "optical technology" (type of surveillance equipment i.e., cameras) the NYPD used when surveilling the protests at Grand Central Terminal. (Donohue Aff., ¶¶ 23, 27). It is true that some digital cameras embed information into the digital images they produce, including, for example, the make and model of the camera, date, time and as well as geo-location information revealing where the photo was taken. However, it is also the case that widely available free tools exist which can scrub this "EXIF" data from images. Just as it is routine in Freedom of Information cases for government agencies to use widely available tools to redact sensitive information (such as the names of government employees) from documents, so too can the NYPD use EXIF scrubbing tools to remove identifying metadata from the multimedia records which might reveal specific information about the make and model of surveillance technology they use.

10. If the surveillance equipment used by the NYPD outputs images and/or records in proprietary file formats for which metadata scrubbing tools do not exist, or which otherwise might reveal information about the equipment itself, the NYPD has the capacity to convert those

files into standard formats which can be scrubbed of identifying metadata, and as a result, will not reveal the type of cameras or other surveillance equipment used.

11. Even if the NYPD's disclosure of the responsive images and recordings were to reveal information about the surveillance equipment, knowing the model of surveillance cameras that the NYPD owns would not result in the types of cybersecurity harms that Assistant Chief John Donohue describe in his affidavit.

12. Assistant Chief Donohue states that disclosing the requested "multimedia" records could permit an enterprising person to learn the kinds of wireless optical surveillance technology the NYPD uses, then argues, without citing any supporting evidence, that with that knowledge, "would-be hackers would have a much easier time understanding and exploiting and attacking NYPD's wireless communications and transmission network." (Donohue Aff., ¶¶ 27-28).

13. He further adds that "Such an attack would jeopardize NYPD's ability to secure its network and surveillance cameras." (Donohue Aff., ¶ 29)

14. Contrary to Assistant Chief Donohue claims, there is no legitimate cybersecurity justification to keeping secret the multimedia records requested of the NYPD.

15. As an illustrative example, public disclosure that the Mayor has an iPhone or the NYPD Commissioner uses a Macbook laptop will not enable an enterprising criminal or a foreign government to successfully hack the Mayor or Commissioner's communications. The Mayor and Police Commissioner's communications are undoubtedly protected by several layers of advanced cybersecurity technologies, including encryption.

16. Likewise, the wireless and fiber optic communications networks used by the NYPD should be secured against hackers with several layers of cybersecurity technologies,

including, at a bare minimum, encryption and access control, just as enterprise and residential wireless networks are routinely encrypted and protected with passwords.

17. Responsible organizations protect their information technology ("IT") infrastructure with industry-standard data security technologies, none of which depend on keeping basic information such as the make and model of devices used a secret. It is simply not credible to argue that the security of the NYPD's video surveillance systems or the NYPD's city-wide wireless and fiber optic communications networks depends on keeping information identifying the "kinds of optical technology NYPD uses to conduct surveillance" hidden from the public. (Donohue Aff., ¶ 27) Moreover, given Assistant Chief Donohue's recitation of the personal safety risks to police officers that are recognized by the NYPD, and the precautions he avers the NYPD takes to protect its officers' safety (Donohue Aff., ¶¶ 5-12), it is inconceivable that the NYPD's IT infrastructure is so vulnerable and poorly secured that merely revealing kinds of optical technology used would allow hackers to gain unauthorized access to those networks and systems.

18. For all the foregoing reasons, the arguments advanced by Assistant Chief John Donohue for why the NYPD's photographs, video and/or audio recordings responsive to Petitioner's request should not be released are incorrect, and this Court should not credit them.

Christopher A Soghoian

CHRISTOPHER SOGHOIAN

Sworn to before me on this
26 day of October, 2016

Notary Public State: Newyork
County: Newyork

EXHIBIT A

Christopher Soghoian, P.h.D.

Privacy and Security Researcher

PO Box 2266
Washington, DC 20013
☎ +1 (617) 308 6368
✉ chris@soghoian.net
www.dubfire.net

Experience

2012–current **Principal Technologist**, *American Civil Liberties Union*, Washington DC.

- Led a multi-year campaign to research and expose law enforcement agencies' use of StingRays, a cell phone tracking technology. This campaign resulted in widespread public awareness of the technology, an end to the government's official policy of secrecy, the establishment of a warrant standard by DOJ and DHS, and the passage by multiple states of Stingray-specific privacy laws.
- Led a multi-year campaign to discover and expose the use of hacking by the FBI. While researching the agency's early use of malware, I discovered that in a 2007 surveillance operation, FBI agents impersonated the Associated Press. My disclosure of the FBI's use of these tactics resulted in a significant public debate regarding the impersonation of the media by the government, investigations by the Department of Justice Inspector General and Congress, and the establishment of new, stricter impersonation policies by the FBI.
- Developed a proactive advocacy strategy related to government cybersecurity. This highly successful campaign resulted in a number of Inspectors General enabling "HTTPS" encryption for their online whistle-blower hotlines, as well as the FBI and Director of National Intelligence enabling "STARTTLS" encryption on their email servers.
- Worked with reporters at national news organizations to place major surveillance and cybersecurity related stories, many of which appeared on their front pages.
- Assisted with litigation strategy and research on surveillance, privacy and national security related cases.

2012–current **Visiting Fellow**, *Information Society Project, Yale Law School*, New Haven, CT.

- Organized two academic conferences focused on US law enforcement use of new surveillance technologies. The first, in 2013, on the use of Stingrays and cell phone location surveillance, and the second, in 2014, on government hacking. These events, which were the first of their kind, featured legal scholars, technology experts, investigative reporters, federal judges and Congressional staff.

2009–2010 **Technologist**, *U.S. Federal Trade Commission*, Washington DC.

- Advised staff attorneys conducting investigations in the area of behavioral advertising and Internet privacy.
- Initiated numerous new investigations, assisted with the collection of evidence and analysis of data, participated in information-gathering discussions with companies under investigation, and provided technical assistance to staff drafting access letters, subpoenas, complaints and consent agreements.
- Investigated companies included Facebook, Twitter, Netflix, and MySpace.

2008–2009 **Student Fellow**, *Berkman Center For Internet & Society, Harvard University, Boston, MA*.

Summer 2007 **Intern**, *DoCoMo Communications Laboratories Europe*, Munich, Germany.

Summer 2006 **Intern**, *Application Security Group, Google*, Mountain View, CA.

Summer 2005 **Intern**, *Security Technology Group, Apple Computer*, Cupertino, CA.

Summer 2004 **Intern**, *IBM Research*, Zurich, Switzerland.

Education

2006–2012 **Ph.D. Informatics**, *Indiana University*, Bloomington, IN.
The Spies We Trust: Third Party Service Providers & Law Enforcement Surveillance.

2003–2005 **M.S. Security Informatics**, *The Johns Hopkins University*, Baltimore, MD.

1999–2002 **B.S. Computer Science**, *James Madison University*, Harrisonburg, VA.

Significant Accomplishments

- Testified as an expert witness in *United States v. Michaud*, the first case where the FBI's bulk hacking of thousands of Tor users was challenged on constitutional grounds. Have subsequently testified as a *pro-bono* technical expert for the defense in several other FBI hacking cases.
- Spoke at multiple training events for federal judges, at the invitation of the Federal Judicial Center, focused on government use of surveillance technology.
- Testified before the German Parliament, the European Parliament, and several state legislative committees about government surveillance.
- Developed a browser add-on that let users opt-out of behavioral advertising by 80+ companies. The tool was downloaded 750,000 times before I sold it to a privacy-focused start-up.
- Cited by 9th Circuit Court of Appeals and the New Jersey and Massachusetts Supreme Courts.
- Cited in *State v. Andrews*, the first appellate decision to require a warrant for StingRay tracking.

Scholarships and Awards

- Profiled by the Economist, Wired, IEEE Spectrum, Le Monde and Folha De S. Paulo.
- Politico 50, "a top thinker, doer and visionary transforming American politics," 2015.
- Tech Titan, Washingtonian Magazine, 2013, 2015.
- TED Senior Fellow (2015), TED Global Fellow (2013).
- TR35 (Top 35 Innovators Under 35), MIT Technology Review, 2012.
- Open Society Fellow, Open Society Foundations, 2011–2012.
- Privacy Champion Award, Electronic Privacy Information Center, 2012.
- Humane Studies Fellowship, Institute For Humane Studies, 2008 and 2009.

Selected Academic Publications

Stephanie K. Pell and Christopher Soghoian. Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy. *Harvard Journal of Law and Technology*, 28(1), 2014.

Stephanie K. Pell and 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. *Yale Journal of Law & Technology*, 16(1), 2013.

Stephanie K. Pell and Christopher Soghoian. Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact. *Berkeley Technology Law Journal*, 27(1), 2012.

Christopher Soghoian and Sid Stamm. Certified Lies: Detecting and Defeating Government Interception Attacks against SSL (Short Paper). In *Financial Cryptography and Data Security - 15th International Conference*, 2011.

Christopher Soghoian. An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government. *Minnesota Journal of Law, Science & Technology*, 12(1), 2011.

Christopher Soghoian. Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era. *Journal on Telecommunications and High Technology Law*, 8(2), 2010.

Christopher Soghoian. Caveat Venditor: Technologically Protected Subsidized Goods and the Customers Who Hack Them. *Northwestern Journal of Technology and Intellectual Property*, 6(1), 2007.