IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

XIAOXING XI, *et al.*,	:	
Plaintiffs,	:	**CIVIL ACTION**
v.	:	**No. 17-cv-2132**
FBI SPECIAL AGENT ANDREW HAUGEN, *et al.*,	:	**JURY TRIAL DEMANDED**
Defendants.	:	

ORDER

AND NOW this _____ day of _____, 2018, upon consideration of the Government's Motion to Dismiss Plaintiffs' Claims Against Official Capacity Defendants Christopher A. Wray, Jefferson B. Sessions, III, and Adm. Michael S. Rogers (ECF 38), and plaintiffs' response to that motion, **IT IS ORDERED** that the motion is **DENIED**.

BY THE COURT:

_____
R. BARCLAY SURRICK, J.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

XIAOXING XI, *et al.*,	:	
Plaintiffs,	:	**CIVIL ACTION**
v.	:	**No. 17-cv-2132**
FBI SPECIAL AGENT ANDREW HAUGEN, *et al.*,	:	**JURY TRIAL DEMANDED**
Defendants.	:	

PLAINTIFFS' RESPONSE IN OPPOSITION TO THE OFFICIAL CAPACITY DEFENDANTS' MOTION TO DISMISS THE COMPLAINT

David Rudovsky
Jonathan H. Feinberg
Susan M. Lin
KAIRYS, RUDOVSKY, MESSING, FEINBERG & LIN LLP
The Cast Iron Building
718 Arch Street, Suite 501 South
Philadelphia, PA 19106
215-925-4400
215-925-5365 (fax)

Patrick Toomey
Ashley Gorski
Jonathan Hafetz
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
212-549-2500
212-549-2654 (fax)

April 9, 2018

Counsel for Plaintiffs

TABLE OF CONTENTS

Introduction 1

I. Summary of plaintiffs' surveillance claims 3

A. The searches and surveillance of plaintiffs' communications, personal computers, and cell phones 3

B. The types of surveillance at issue 5

1. Criminal and FISA searches requiring a showing of probable cause 5

2. Warrantless surveillance under Section 702 and Executive Order 12333 5

II. Legal standards 9

III. The government's ongoing retention and searching of plaintiffs' personal data and communications establishes their standing to seek injunctive and declaratory relief. 11

A. The government's ongoing retention and searching of plaintiffs' personal data and communications is an injury-in-fact. 11

B. Plaintiffs' injuries will be redressed by the injunctive and declaratory relief they seek. 15

IV. Plaintiffs have plausibly alleged the violation of their Fourth Amendment rights. 17

A. Plaintiffs have plausibly alleged that they were subjected to criminal searches and FISA searches based on false affidavits. 17

B. Professor Xi has plausibly alleged the warrantless surveillance of his communications. 19

C. The surveillance of Professor Xi's communications violated the Fourth Amendment's warrant requirement. 23

1. Warrantless searches are per se unreasonable. 25

2. The foreign-intelligence exception does not apply to the warrantless surveillance of Professor Xi. 25

3. The government's warrantless surveillance of foreigners does not excuse its failure to obtain a warrant before exploiting the communications of Americans like Professor Xi. 29

D. The warrantless surveillance of Professor Xi's communications was unreasonable under the Fourth Amendment. 32

1. The warrantless surveillance of Professor Xi lacked core safeguards that courts require when assessing the reasonableness of electronic surveillance.....35

2. The warrantless surveillance of Professor Xi lacked sufficient "post-seizure" protections to be reasonable under the Fourth Amendment.....37

Conclusion 42

TABLE OF AUTHORITIES

Cases

[*Redacted*],
No. [Redacted] (FISC Apr. 26, 2017) 41

[*Redacted*],
No. [Redacted] (FISC Aug. 30, 2013) 7

Andrews v. Scuilli,
853 F.3d 690 (3d Cir. 2017) 18

Ashcroft v. Iqbal,
556 U.S. 662 (2008) 11, 19, 22

Betker v. Gomez,
692 F.3d 854 (7th Cir. 2012) 18

Blunt v. Lower Merion Sch. Dist.,
767 F.3d 247 (3d Cir. 2014) 10

Boykin v. KeyCorp,
521 F.3d 202 (2d Cir. 2008) 11

Brigham City v. Stuart,
547 U.S. 398 (2006) 32

Chism v. Washington,
661 F.3d 380 (9th Cir. 2011) 18

Coolidge v. New Hampshire,
403 U.S. 443 (1971) 22, 33

Dalia v. United States,
441 U.S. 238 (1979) 25

Doe v. U.S. Air Force,
812 F.2d 738 (D.C. Cir. 1987) 13, 16, 17

Ferguson v. City of Charleston,
532 U.S. 67 (2001) 13

Foglia v. Renal Ventures Mgmt., LLC,
754 F.3d 153 (3d Cir. 2014) 10, 22

Fortune Players Grp., Inc. v. Quint,
No. 16-cv-00800, 2016 WL 4091401 (N.D. Cal. Aug 2, 2016) 33

Fox v. Dist. of Columbia,
851 F. Supp. 2d 20 (D.D.C. 2012) 16

Franks v. Delaware,
438 U.S. 154 (1978) 18

Free Speech Coal., Inc. v. Attorney General,
825 F.3d 149 (3d Cir. 2016) 22, 33

Hassan v. City of New York,
804 F.3d 277 (3d Cir. 2015) 15

Hedgepeth v. WMATA,
386 F.3d 1148 (D.C. Cir. 2004) 16

Hernandez-Cuevas v. Taylor,
723 F.3d 91 (1st Cir. 2013) 18

In re Avandia Mktg., Sales Practices & Prod. Liab. Litig.,
804 F.3d 633 (3d Cir. 2015) 10

In re Directives Pursuant to Section 105B of FISA,
551 F.3d 1004 (FISCR 2008) 28, 38, 41

In re Horizon Healthcare Servs. Inc. Data Breach Litig.,
846 F.3d 625 (3d Cir. 2017) 10

In re Proceedings Required by § 702(i) of the FAA,
No. 08-01, 2008 WL 9487946 (FISC Aug. 27, 2008) 8

In re Sealed Case,
310 F.3d 717 (FISCR 2002) 27, 35, 38

J. Roderick MacArthur Found. v. FBI,
102 F.3d 600 (D.C. Cir. 1996) 14

J.A. v. Miranda,
No. PX 16-3953, 2017 WL 3840026 (D. Md. Sept. 1, 2017) 24

Jones v. United States,
357 U.S. 493 (1958) 24

Katz v. United States,
389 U.S. 347 (1967) ..... passim

Laird v. Tatum,
408 U.S. 1 (1972) 14, 15

Leach ex rel. Dyson v. Principal Baum,
No. Civ. A. 04-135, 2004 WL 834732 (E.D. Pa. Apr. 16, 2004) 33

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992) 10

Mayfield v. United States,
599 F.3d 964 (9th Cir. 2010).....13, 16, 17

McDonald v. United States,
335 U.S. 451 (1948) 36

Menard v. Saxbe,
498 F.2d 1017 (D.C. Cir. 1974) 13

New Jersey v. T.L.O.,
469 U.S. 325 (1985) 25

Paton v. La Prade,
524 F.2d 862 (3d Cir. 1975).....16

Phillips v. Cty. of Allegheny,
515 F.3d 224 (3d Cir. 2008).....11, 19

Riley v. California,
134 S. Ct. 2473 (2014).....32

Samson v. California,
547 U.S. 843 (2006) 24, 33, 35

Schuchardt v. President of the United States,
839 F.3d 336 (3d Cir. 2016).....passim

Socialist Workers Party v. Attorney General,
419 U.S. 1314 (1974) 13, 15

Susan B. Anthony List v. Driehaus,
134 S. Ct. 2334 (2014).....10

Tabbaa v. Chertoff,
509 F.3d 89 (2d Cir. 2007).....16

Terry v. Ohio,
392 U.S. 1 (1968) 38

United States v. Biasucci,
786 F.2d 504 (2d Cir. 1986).....35

United States v. Bin Laden,
126 F. Supp. 2d 264 (S.D.N.Y. 2000) 27

United States v. Bobo,
477 F.2d 974 (4th Cir. 1973).....35

United States v. Butenko,
494 F.2d 593 (3d Cir. 1974).....26

United States v. Calandra,
414 U.S. 338 (1974) 17

United States v. Donovan,
429 U.S. 413 (1977) 30, 31, 36

United States v. Duggan,
743 F.2d 59 (2d Cir. 1984).....27, 35

United States v. Duka,
671 F.3d 329 (3d Cir. 2011).....26, 27, 28

United States v. Figueroa,
757 F.2d 466 (2d Cir. 1985).....30

United States v. Galpin,
720 F.3d 436 (2d Cir. 2013).....41

United States v. Ganias,
824 F.3d 199 (2d Cir. 2016).....13

United States v. Hasbajrami,
No. 11-cr-623 (JG), 2016 WL 1029500 (E.D.N.Y. Mar. 8, 2016) 29

United States v. Jacobsen,
466 U.S. 109 (1984) 14

United States v. Jeffers,
342 U.S. 48 (1951) 22

United States v. Jefferson,
571 F. Supp. 2d 696 (E.D. Va. 2008) 13, 14

United States v. Kahn,
415 U.S. 143 (1974) 30, 31

United States v. Martin,
599 F.2d 880 (9th Cir. 1979).....30

United States v. Metter,
860 F. Supp. 2d 205 (E.D.N.Y. 2012) 13

United States v. Mohamud,
843 F.3d 420 (9th Cir. 2016) 29

United States v. Muhtorov,
187 F. Supp. 3d 1240 (D. Colo. 2015) 31

United States v. Ramsey,
431 U.S. 606 (1977) 32

United States v. Sedaghaty,
728 F.3d 885 (9th Cir. 2013) 32, 41

United States v. Tortorello,
480 F.2d 764 (2d Cir. 1973) 35, 38

United States v. Truong Dinh Hung,
629 F.2d 908 (4th Cir. 1980) 26

United States v. U.S. Dist. Court (*Keith*),
407 U.S. 297 (1972) 23, 26

United States v. Verdugo-Urquidez,
494 U.S. 259 (1990) 31, 32

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 23, 31

Wilson v. Health & Hosp. Corp. of Marion Cty.,
620 F.2d 1201 (7th Cir. 1980) 22

Statutes

18 U.S.C. § 2518 32

50 U.S.C. § 1801 ..... passim

50 U.S.C. § 1802 40

50 U.S.C. § 1806 ..... 9, 34

50 U.S.C. § 1881a ..... passim

50 U.S.C. § 1881c 27

Other Sources

Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post, July 5, 2014 6

Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. Times, Oct. 26, 2013 9

Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. Times, Aug. 13, 2014 9

Elizabeth Goitein, *The Ninth Circuit's Constitutional Detour in* Mohamud, Just Security (Dec. 8, 2016) 30

Exec. Order 12333, 46 Fed. Reg. 59,951 (Dec. 4, 1981), as amended .....passim

Foreign Intelligence Surveillance Act Orders 1979–2016, Elec. Privacy Info Ctr. 26

Geoffrey Stone & Michael Morell, *The One Change We Need to Surveillance Law*, Wash. Post, Oct. 9, 2017, ...39

H.R. 4870, 113th Cong. (2014) 40

James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls*, Guardian, Aug. 9, 2013 .....9, 41

John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, Wash. Post, July 18, 2014 39

Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2016* (Apr. 2017) 6

Orin Kerr, *The Surprisingly Weak Reasoning of* Mohamud, Lawfare (Dec. 23, 2016) 31

Peter Swire & Richard Clarke, *Reform Section 702 to Maintain Fourth Amendment Principles*, Lawfare (Oct. 19, 2017) 39

President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* (2013) 30, 40

Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014) .....passim

Ryan Devereaux et al., *Data Pirates of the Caribbean: The NSA is Recording Every Cell Phone Call in the Bahamas,* Intercept, May 19, 2014 7

S.A. 3979, 110th Cong. (2008), 154 Cong. Rec. S607-08 (daily ed. Feb. 4, 2008) 40

Trevor Aaronson, *NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal*, Intercept, Nov. 30, 2017 ..... 9, 21

U.S. Signals Intelligence Directive SP0018 (Jan. 25, 2011) 8, 36, 39

Worldwide Threats: Open Hearing before the S. Select Comm. on Intelligence, 115th Cong. (2018) 12

Introduction

In May 2015, plaintiff Xiaoxing Xi, a professor of physics at Temple University and a naturalized United States citizen, was indicted and arrested for allegedly sharing with entities in China information concerning a "pocket heater" belonging to a United States company. As described in plaintiffs' brief in opposition to the Individual Defendants' and USA's Motions to Dismiss, Professor Xi was wrongly prosecuted, and the indictment against him was dismissed on the government's motion in September 2015.

This brief addresses plaintiffs' separate search and surveillance claims against the Official Capacity Defendants. *See* SAC Count X (ECF 26). As set out in the Second Amended Complaint, in the course of the government's investigation into Professor Xi, and following his arrest, defendants subjected Professor Xi and his family to a host of unlawful searches and seizures. First, in a process that has become routine in investigations like this one, defendants relied on a set of warrantless surveillance tools: they intercepted Professor Xi's emails, text messages, and phone calls with his scientist colleagues in China, storing those communications in massive databases where they were searched and read by FBI agents without obtaining a warrant from any court. The FBI then used this warrantless surveillance to expand its investigation, ultimately targeting Professor Xi for FISA surveillance based on materially false statements and omissions in its applications to the Foreign Intelligence Surveillance Court ("FISC"). And finally, immediately after Professor Xi's arrest, the FBI used a similarly defective criminal warrant to search and seize personal computers, cell phones, digital storage devices, and other private information belonging to each of the plaintiffs. *See* SAC Count X.

Although the government dismissed its wrongful indictment, it is retaining copies of the Xis' personal data—storing that information in government databases and searching through it in

ongoing investigations. Plaintiffs seek the expungement of their private information and a declaration that the government's searches and seizures violate the Fourth Amendment.

Defendants move to dismiss these claims, arguing that plaintiffs have not alleged a concrete injury, and that a declaratory judgment would not redress any injury. But the government's continuing retention and searching of the Xis' private information, which it obtained only through its unlawful searches and seizures, is unquestionably an ongoing injury. Moreover, the injunctive and declaratory relief that plaintiffs seek would redress this injury: by requiring the government to destroy its copies, remove the Xis' information from government databases, and stop searching through their information on an ongoing basis.

Defendants also contend that plaintiffs have not plausibly alleged that the criminal search warrants and FISA orders were based on false statements and omissions. But the complaint sets forth in detail the substantial falsehoods about Professor Xi's scientific work that infected the government's search applications, just as they infected its indictment.

Finally, defendants argue that Professor Xi has failed to plausibly allege that he was subject to warrantless surveillance or that this surveillance violated the Fourth Amendment. But Professor Xi's claims are more than plausible: he has pled specific facts—based on official disclosures, media reports, and the government's own dismissed indictment in this case—establishing that his numerous communications with his scientist counterparts in China were subject to warrantless surveillance. Because this surveillance is per se unreasonable under the Fourth Amendment, and because no exception to the warrant requirement applies, Professor Xi's allegations are sufficient to state a Fourth Amendment claim.

While defendants argue that even warrantless surveillance would be "reasonable" under the Fourth Amendment, the Court need not reach that issue in deciding the motion to dismiss. It is

the government's burden to establish reasonableness under the Fourth Amendment—and reasonableness is decided based on the totality of the circumstances, which is more properly addressed on a full factual record developed through discovery, as other courts have recognized. But even if the Court reaches this question, Professor Xi has stated a claim that the government's warrantless access to his communications was unreasonable under the Fourth Amendment. Whatever powers the government may claim to surveil foreigners located overseas, the FBI cannot exploit that authority as a backdoor into the private communications of innocent Americans. In particular, it is unreasonable for the government to do what it did here: intercept Professor Xi's emails using surveillance purportedly directed at foreigners, amass those emails in huge databases of private communications, and then search through them to investigate Professor Xi—without safeguards remotely approaching what the Fourth Amendment requires. Even if the government need not obtain a warrant before it surveils foreigners, reasonableness requires the government to afford greater protection to Americans like Professor Xi who are swept up in this surveillance net.

For these reasons, plaintiffs should be permitted to pursue their claims that the government's surveillance in this case violated their Fourth Amendment rights.

I. Summary of plaintiffs' surveillance claims

A. The searches and surveillance of plaintiffs' communications, personal computers, and cell phones

Professor Xi is a professor of physics at Temple University, and a naturalized U.S. citizen originally from China. SAC ¶¶ 1, 12. He is an internationally recognized expert in the field of thin film superconducting technology and is widely respected by his academic colleagues and graduate students. *Id.* ¶¶ 25, 92–94. Professor Xi lives in Penn Valley, Pennsylvania with his wife, plaintiff Qi Li, also a professor of physics; his daughter, plaintiff Joyce Xi, a 2016 graduate of Yale University; and his younger daughter (who is not a plaintiff). *Id.* ¶¶ 13–14, 34. Professor Xi and

his wife and daughter have brought this action to hold the defendant federal officers and the United States accountable for the extraordinary harms and losses they suffered as a result of a false and baseless prosecution brought against Professor Xi. The facts related to the surveillance and searches of plaintiffs are summarized briefly below.

As described in the complaint, defendants relied on warrantless surveillance to intercept Professor Xi's communications with his scientist colleagues in China, and then exploited that access to wrongly investigate him. SAC ¶¶ 60–65. The NSA has engaged in extensive and concerted surveillance of Chinese universities and research institutions, including those where Professor Xi's counterparts were based. *Id.* ¶¶ 61–62. This warrantless surveillance includes the collection of communications in bulk, whereby virtually all messages and data on a system or network are captured. It also includes surveillance directed at particular organizations, individuals, and Internet addresses. *Id.* ¶ 61. These intercepted communications then make their way into investigations here in the United States. In the investigation leading up to Professor Xi's indictment, defendants searched the vast databases where they store communications intercepted without a warrant, in order to identify and access Professor Xi's private communications without first obtaining court approval. *Id.* ¶¶ 64–65. When the government arrested Professor Xi, it specifically referenced intercepted emails between Professor Xi and scientists at Tsinghua University, where the NSA has siphoned data off of computers, servers, and network backbones connecting Chinese research institutions. *Id*. ¶¶ 61–62. Likewise, the four emails cited by the government in its dismissed indictment were emails that Professor Xi exchanged with scientists working at several of these prominent Chinese research institutions. *Id.*

The government used these warrantless searches as the starting point for even more intrusive searches targeting Professor Xi and his family. *Id.* ¶ 65. Defendants sought FISA orders

and criminal search warrants based on the same false statements and omissions that plagued the government's indictment of Professor Xi. *Id.* ¶¶ 53–59, 67. Relying on FISA orders and criminal search warrants, defendants intercepted plaintiffs' communications, seized plaintiffs' personal computers and cell phones in order to copy and search those devices, and searched Professor Xi's offices. *Id.* ¶¶ 59, 67.

Defendants continue to retain copies of the private communications, data, and papers of plaintiffs obtained through the unlawful searches and seizures. This information includes, but is not limited to, the full contents of their computers and other electronic devices. *Id.* ¶¶ 67, 133. Moreover, defendants are storing plaintiffs' private information in law enforcement and investigative databases, where that information is routinely searched by agents in the course of wholly unrelated investigations. *Id.* ¶ 134.

B. The types of surveillance at issue

1. Criminal and FISA searches requiring a showing of probable cause

The government conducted certain of its searches and seizures pursuant to criminal search warrants as well as FISA orders authorizing the targeting of Professor Xi for electronic and physical searches. *Id.* ¶¶ 59, 67. Like a traditional criminal search, a FISA search requires that the government make a showing to a court that there is "probable cause" to target an individual for surveillance—in the case of FISA, probable cause to believe that the target is a foreign power or agent of a foreign power. 50 U.S.C. § 1801 *et seq.*

2. Warrantless surveillance under Section 702 and Executive Order 12333

Professor Xi was also subject to surveillance under two complementary authorities that the government uses to intercept and exploit Americans' international communications without ever obtaining a warrant.

a. Warrantless interception

Under Section 702 of the Foreign Intelligence Surveillance Act, the government conducts warrantless surveillance on U.S. soil of vast quantities of communications entering and leaving the United States—including communications sent and received by Americans like Professor Xi.[1] The statute permits this warrantless surveillance when two primary conditions are met: first, an analyst must reasonably believe that the "target" of the surveillance is a non-U.S. person or group abroad; and second, a "significant purpose" of the surveillance must be to gather "foreign intelligence information," broadly defined. 50 U.S.C. §§ 1881a, 1801(e). In other words, targets need not be agents of a foreign power, suspected of a crime, or even remotely connected to terrorism. Due in part to this low threshold for targeting, Section 702 surveillance is extremely broad in scope: the surveillance involves more than 100,000 targets and captures billions of communications.[2] The government has obtained certifications under Section 702 that specifically authorize warrantless surveillance related to the Chinese government and its components. SAC ¶ 61. This sprawling surveillance apparatus inevitably—and intentionally—sweeps in Americans' emails, telephone calls, and other forms of communications with the government's targets in China and elsewhere.[3] As the FISC has observed, Section 702 surveillance results in the government obtaining

[1] The government conducts Section 702 surveillance in two ways, commonly known as PRISM and Upstream. Under PRISM, the government compels Internet service providers, such as Google and Facebook, to turn over the communications of their customers. Under Upstream, the government compels telecommunications companies, like AT&T and Verizon, to intercept communications in real-time as they flow through Internet backbone cables. *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702*, at 7 (July 2, 2014), https://perma.cc/WD5R-5GKE ("PCLOB Report").

[2] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2016* (Apr. 2017), goo.gl/HurVE8; PCLOB Report 116 (noting the "current number is significantly higher" than in 2011).

[3] Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post, July 5, 2014, https://wapo.st/1MVootx.

"substantial quantities of information concerning United States persons and persons located inside the United States who are entitled to Fourth Amendment protection."[4]

The second form of warrantless surveillance at issue is conducted under EO 12333.[5] This surveillance is, in many ways, complementary to Section 702: it is primarily conducted outside the United States, and it provides broad latitude for the government to conduct surveillance on both U.S. and non-U.S. persons. Although Americans may not be *intentionally* targeted under EO 12333, Americans' communications are frequently sent, routed, or stored abroad—where they may be collected in the course of the NSA's surveillance activities. Like Section 702, EO 12333 authorizes the government to conduct surveillance for the purpose of collecting "foreign intelligence"—a term defined so broadly that it appears to permit surveillance of virtually any non-U.S. person, including surveillance of their communications with Americans. EO 12333 § 3.5(e). Significantly, EO 12333 and its implementing regulations permit "bulk collection"—that is, the indiscriminate collection of electronic communications or data.[6] Recent disclosures indicate that the government operates a host of large-scale programs under EO 12333, many of which involve the collection of vast quantities of emails, phone calls, and text messages.[7] Press reports describe how the government has engaged in extensive and concerted warrantless surveillance of Chinese universities and scientific research institutions, including surveillance of Tsinghua University, where the NSA siphoned data in bulk off of computers, servers, and network backbones connecting thousands of Chinese research institutions. SAC ¶ 61.

---

[4] [*Redacted*], No. [Redacted], at 24 (FISC Aug. 30, 2013), https://perma.cc/GR62-FNQC.

[5] Exec. Order 12333, 46 Fed. Reg. 59,951 (Dec. 4, 1981), as amended, *available at* https://bit.ly/2GNTqqq.

[6] Press Release, White House, *Presidential Policy Directive 28—Signals Intelligence Activities* § 2 & n.5 (Jan. 17, 2014), https://perma.cc/F3ZN-58JE ("PPD-28").

[7] Ryan Devereaux et al., *Data Pirates of the Caribbean: The NSA is Recording Every Cell Phone Call in the Bahamas*, Intercept, May 19, 2014, https://bit.ly/2JdJ05g.

b. Lack of individualized judicial review

Neither Section 702 nor EO 12333 surveillance involve warrants or any form of individualized judicial review. The government does not dispute this. Under Section 702, the FISC has a "narrowly circumscribed" role. *In re Proceedings Required by § 702(i) of the FAA*, No. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008). Unlike under Title III or traditional FISA, no court approves the targets of Section 702 surveillance. Instead, the FISC's role consists principally of reviewing, once a year, the government's "targeting" and "minimization" procedures, which set certain rules that agency analysts must follow when selecting targets and handling intercepted communications. 50 U.S.C. § 1881a(a), (i). Under EO 12333, the absence of judicial involvement is even starker: the surveillance is not subject to any form of judicial review at all.

c. Warrantless retention, querying, and use

Not only are Americans' communications collected in vast quantities under Section 702 and EO 12333, they are also retained, searched, and used in later investigations—including in domestic criminal investigations far removed from the original foreign-intelligence purpose of the surveillance. *See* SAC ¶¶ 63–64. The government's "minimization" procedures, which supposedly protect the privacy of Americans swept up in the surveillance, are weak by design. As a default rule, they permit the government to keep most intercepted communications, including those of Americans, in vast government databases for as long as five years. PCLOB Report 60; U.S. Signals Intelligence Directive SP0018 § 6 (Jan. 25, 2011), https://perma.cc/SH4G-XJUW ("USSID 18"). During that time, agents and analysts routinely search through them—including by using Americans' names or email addresses to investigate particular Americans. PCLOB Report 55–60; USSID 18 §§ 4–6. These "backdoor searches" allow the government to target and read the communications of Americans without obtaining a warrant or any individualized judicial

authorization.[8] In short, these warrantless queries are designed to extract and access communications that the government *knows* are protected by the Fourth Amendment.

d. Government efforts to conceal warrantless surveillance of Americans

Even when the government uses information gleaned from warrantless surveillance in the course of a criminal investigation, it regularly conceals that fact from the individuals like Professor Xi whom it seeks to prosecute. SAC ¶ 66. Although the government is required to provide notice of Section 702 surveillance in criminal proceedings, *see* 50 U.S.C. § 1806, it has adopted policies and practices that thwart that requirement. Indeed, for five years after the enactment of Section 702, the Department of Justice failed to provide notice of this surveillance to a single criminal defendant, based on a notice policy that it has never publicly disclosed; and it continues to use "parallel construction" and other strategies to avoid providing notice today.[9] Similarly, when it comes to EO 12333 surveillance, officials have claimed that individuals like Professor Xi have "no right to know if 12333 intercepts provided a tip from which investigators derived other evidence."[10]

II. Legal standards

The government has challenged the plausibility of plaintiffs' complaint pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). Under Rule 12(b)(1), the government challenges

---

[8] *See* James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls*, Guardian, Aug. 9, 2013, https://goo.gl/DDg2zZ.

[9] Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. Times, Oct. 26, 2013, https://nyti.ms/1aKvksP; Trevor Aaronson, *NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal*, Intercept, Nov. 30, 2017, https://bit.ly/2ExuYYJ (describing how Section 702 was secretly used to surveil criminal defendant).

[10] Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. Times, Aug. 13, 2014, http://nyti.ms/1wPw6l0.

plaintiffs' standing. Gov't Officials' MTD 15–18 (ECF 38). Under Rule 12(b)(6), the government contends that the complaint fails to plausibly allege a Fourth Amendment violation. *Id.* at 20–38.

To establish standing, a complaint must plausibly allege (1) an "injury in fact" that is "concrete and particularized" and "actual or imminent," not "conjectural" or "hypothetical"; (2) a "causal connection" between the injury and the defendant's conduct; and (3) a likelihood that a favorable decision will "redress" the injury. *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014). The Third Circuit has repeatedly explained that, "'[a]t the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim.'" *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 633–34 (3d Cir. 2017) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992)). In the context of a motion to dismiss, "the [i]njury-in-fact element is not Mount Everest. The contours of the injury-in-fact requirement, while not precisely defined, are very generous, requiring only that claimant allege some specific, identifiable trifle of injury." *Blunt v. Lower Merion Sch. Dist.*, 767 F.3d 247, 278 (3d Cir. 2014).

When assessing a facial challenge under Rule 12(b)(1) or 12(b)(6), a motion to dismiss may be granted only if, accepting all well-pleaded allegations as true and viewing them in the light most favorable to the plaintiff, the court finds that the plaintiff's claims are not plausible. *See In re Avandia Mktg., Sales Practices & Prod. Liab. Litig.*, 804 F.3d 633, 637–38 (3d Cir. 2015); *In re Horizon Healthcare Servs.*, 846 F.3d at 633. When applying the plausibility standard, all reasonable inferences must be drawn in favor of the plaintiff. *Foglia v. Renal Ventures Mgmt., LLC*, 754 F.3d 153, 154 n.1 (3d Cir. 2014). A court must not weigh the probability of competing explanations; rather, after crediting the plaintiff's factual allegations, it must determine whether

the complaint shows more than the "sheer possibility" that the plaintiff has stated a claim. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2008).

Importantly, "the plausibility standard does not impose a heightened pleading requirement, and . . . Federal Rule of Civil Procedure 8(a) continues to require only a 'showing' that the pleader is entitled to relief." *Schuchardt v. President of the United States*, 839 F.3d 336, 347 (3d Cir. 2016). The Third Circuit has underscored that, "although *Twombly* and *Iqbal* emphasized the plaintiff's burden of pleading sufficient 'factual matter,' the Supreme Court also expressly 'disavow[ed]' the requirement that a plaintiff plead 'specific facts.'" *Id.* (quoting *Boykin v. KeyCorp*, 521 F.3d 202, 215 (2d Cir. 2008)); *see also Phillips v. Cty. of Allegheny*, 515 F.3d 224, 233–34 (3d Cir. 2008) ("The [Supreme] Court emphasized . . . that it was neither demanding a heightened pleading of specifics nor imposing a probability requirement.").

III. The government's ongoing retention and searching of plaintiffs' personal data and communications establishes their standing to seek injunctive and declaratory relief.

The Xis have plausibly pled that they suffer an ongoing injury due to the government's retention and routine searching of their personal communications and data, which it unlawfully obtained. Because the expungement of this information and declaratory relief will redress these harms, plaintiffs have standing.

A. The government's ongoing retention and searching of plaintiffs' personal data and communications is an injury-in-fact.

Both before and after Professor Xi's arrest in May 2015, defendants unlawfully obtained plaintiffs' personal data and communications, using a panoply of surveillance tools to dig deeply into their private lives. First, the government intercepted Professor Xi's communications—including emails, text messages, and phone calls made to his academic contacts and family members abroad—using its warrantless surveillance tools. Although Congress has forbidden the government from using warrantless surveillance to intentionally *target* the communications of

Americans like Professor Xi, the FBI and NSA nonetheless rely on these tools to collect Americans' communications with family, friends, and colleagues abroad. SAC ¶ 60. Defendants used information acquired through this warrantless surveillance to obtain FISA orders and criminal search warrants, allowing them to conduct further searches and surveillance specifically targeting Professor Xi. *Id.* ¶ 65. Through these searches, defendants made records of the Xis' telephone conversations, emails, and text messages, as well as copies of the Xis' private data stored on their home and office computers and their personal cell phones. *Id.* ¶¶ 67, 83–86.

Although all charges against Professor Xi have since been dismissed, the unlawfully acquired private data belonging to him and his family remain stored in massive law enforcement and investigative databases. *Id.* ¶¶ 84, 86. Moreover, these records are not merely sitting there, untouched. Rather, the government routinely searches (or "queries") these databases as part of law enforcement investigations. The government searches these databases using telephone numbers, email addresses, and other keywords; it even intentionally searches for the communications of specific U.S. persons, like Professor Xi. *See* PCLOB Report 59. These database searches are so common in FBI investigations that the government has called them the "FBI's Google." SAC ¶ 64. Indeed, *every time* the FBI opens a new national security investigation, it queries the pool of data it has already amassed. PCLOB Report 59. It does the same with "some frequency" in the course of regular criminal investigations. *Id.* This means that the Xis' private communications are not just retained, but continue to be searched routinely in the course of wholly unrelated investigations.[11]

[11] Recent testimony by FBI Director Christopher Wray indicates that, so long as the Xis' private information remains in the government's hands, it is especially likely to be subject to further searches, scrutiny, and intrusions, simply because Professor Xi is a Chinese-American scientist who has often pursued research with scientist colleagues in China. *See* Worldwide Threats: Open Hearing before the S. Select Comm. on Intelligence, 115th Cong. at 1:15:55 (2018), https://bit.ly/2Gcva0r ("The use of non-traditional [Chinese] collectors, especially in the academic setting—whether it's professors, scientists, students—we see in almost every field office that the

This retention and searching of the Xis' personal data and communications is an ongoing infringement of plaintiffs' privacy interests—an injury-in-fact for Article III standing purposes. *See, e.g.*, *Mayfield v. United States*, 599 F.3d 964, 971 (9th Cir. 2010) (agreeing with the district court that the plaintiff "continue[s] to suffer a present, on-going injury due to the government's continued retention of derivative material from the FISA seizure"); *Menard v. Saxbe*, 498 F.2d 1017, 1023–24 (D.C. Cir. 1974) (holding that retention of records is a "cognizable legal injury"). Contrary to the government's claims, this is so even though the government has returned plaintiffs' physical belongings, because it still retains copies of plaintiffs' electronic information. *See, e.g.*, *Doe v. U.S. Air Force*, 812 F.2d 738, 740 (D.C. Cir. 1987) (rejecting the government's argument that "its return of plaintiff's materials has 'completely and unequivocally eradicated the effects of the alleged violation,'" because the "retention of the information prevents the 'eradication' from being complete"); *United States v. Ganias*, 824 F.3d 199, 217 (2d Cir. 2016); *United States v. Metter*, 860 F. Supp. 2d 205, 212 (E.D.N.Y. 2012); *United States v. Jefferson*, 571 F. Supp. 2d 696, 702 (E.D. Va. 2008). Moreover, plaintiffs' harms go beyond mere retention: they include the further intrusions and injuries stemming from the government's ongoing searches of their illegally obtained information. *See, e.g.*, 50 U.S.C. § 1801(h) (restricting the retention, dissemination, and *use* of private information concerning U.S. persons); *id.* § 1881a(f) (regulating "queries" under Section 702); *Ferguson v. City of Charleston*, 532 U.S. 67, 76 & n.9 (2001) (stating that drug testing of urine sample and reporting of results to police were elements of Fourth Amendment injury, contrary to dissent's view); *Socialist Workers Party v. Attorney General of U.S.*, 666 F. Supp. 621, 623 (S.D.N.Y. 1987) ("The Government contends that there should be no

---

FBI has around the country. . . . They're exploiting the very open research and development environment that we have, which we all revere, but they're taking advantage of it. So one of the things we're trying to do is view the China threat as not just a whole-of-government threat but a whole-of-society threat on their end.").

injunctive relief because there is no threat of future unconstitutional use of the legally obtained information . . . . But this ignores the fact that *any* use or dissemination of this material would be tainted with illegality.").

The government's retention and searching of the Xi's private data and communications also constitutes an injury-in-fact because it interferes with their possessory interests: their ability to control the use of that information. *See Jefferson*, 571 F. Supp. 2d at 704 (explaining that "copying the contents of a person's documents by way of photographs or written notes . . . interfere[s] with the person's sole possession of the information contained in those documents," and holding that taking photographs of documents and notes on their contents "each constitute both a search and a seizure of the information contained in those documents"); *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (a seizure occurs when "there is some meaningful interference with an individual's possessory interests" in property); *Katz v. United States*, 389 U.S. 347, 353 (1967) ("[E]lectronically listening to and recording the petitioner's words . . . constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

Defendants' cases are not to the contrary. In those cases, plaintiffs lacked standing because the harms for which they sought redress—potential consequences flowing from the government's retention of *lawfully* obtained information—were deemed too speculative. *See* Gov't Officials' MTD 17–18 & n.7; *Laird v. Tatum*, 408 U.S. 1, 13 (1972); *J. Roderick MacArthur Found. v. FBI*, 102 F.3d 600, 601, 606 (D.C. Cir. 1996). In contrast, here, the harms plaintiffs seek to redress are concrete, immediate, and ongoing, and flow from the government's retention of illegally obtained

information.[12] Given defendants' retention and routine searching of the Xis' communications and data, plaintiffs have more than sufficiently alleged an injury-in-fact sufficient to satisfy Article III.

B. Plaintiffs' injuries will be redressed by the injunctive and declaratory relief they seek.

Plaintiffs have also plausibly alleged that the relief they seek will redress the harms flowing from defendants' retention and searching of their private communications and data. As the Third Circuit recently noted, "[g]iven the range of available remedies, redressability is easily satisfied." *Hassan v. City of New York*, 804 F.3d 277, 294 (3d Cir. 2015). Here, plaintiffs have requested two forms of relief: (1) injunctive relief requiring defendants "to return to plaintiffs all information in their custody or control obtained from plaintiffs' electronic devices, communications, and papers, and, to the extent that information cannot be returned, to expunge or otherwise destroy that information," SAC Prayer ¶ C; and (2) a declaration that defendants violated plaintiffs' Fourth Amendment rights by subjecting all plaintiffs to unlawful searches and seizures. SAC Prayer ¶ D. Because both the injunctive and declaratory relief plaintiffs seek will redress their injuries, plaintiffs have standing to seek these remedies.

[12] Defendants rely on *Laird* to argue that plaintiffs' "'fear' that any information currently in the Government's possession may be 'misused' at some future time . . . is too speculative to constitute an injury in fact." Gov't Officials' MTD 17. But the allegations in *Laird* are entirely different in kind from the allegations here. *See Laird v. Tatum*, 408 U.S. 1 (1972). There, the Supreme Court addressed an Army surveillance program involving attendance at meetings open to the public. *Id.* at 9. The challengers in that case did not allege that the surveillance itself was unlawful. Nor did they complain of any "specific action of the Army against them," or "attempt to establish" that the misuse of this information against them in the future was "a definitely foreseeable event." *Id.* at 3, 9–10. Instead, the challengers described their injury as a First Amendment chilling effect. *Id.* at 13. Here, in contrast, plaintiffs have alleged that they were specifically subjected to unlawful government surveillance, and that the government has both retained that illegally obtained information *and* continues to search it on a routine basis as part of unrelated investigations. *Cf. Socialist Workers Party v. Attorney General*, 419 U.S. 1314, 1319 (1974) (distinguishing the "general chilling effect" insufficient for standing in *Laird* from the "much more specific" allegations of harm in that case).

Defendants' arguments to the contrary misapprehend both the injuries that plaintiffs continue to suffer and the relief available. First, it is well-established that a demand to expunge illegally obtained information supports standing. *See Tabbaa v. Chertoff*, 509 F.3d 89, 96 & n.2 (2d Cir. 2007) ("[P]laintiffs possess Article III standing based on their demand for expungement."); *Hedgepeth v. WMATA*, 386 F.3d 1148, 1152 (D.C. Cir. 2004); *Paton v. La Prade*, 524 F.2d 862, 868 (3d Cir. 1975); *Fox v. Dist. of Columbia*, 851 F. Supp. 2d 20, 29 (D.D.C. 2012). Second, defendants mischaracterize plaintiffs' claim for declaratory relief as based on nothing more than the fear of future unlawful surveillance, *see* Gov't Officials' MTD 19, but this is not so. Instead, plaintiffs seek declaratory relief to redress the ongoing harm caused by the government's retention and routine searches of their unlawfully obtained information.

This retention and searching is a continuing and prospective injury amenable to declaratory relief. As the D.C. Circuit held in *Doe v. U.S. Air Force*, 812 F.2d 738, when the government retains information it obtained through an unconstitutional search and seizure, "a declaratory judgment that the materials and information were obtained by violating the Constitution would constitute relief." *Id.* at 740. This is so because "[a] court may properly assume that the government would respond to such a declaration by surrendering the retained copies and information obtained by means determined to have been unconstitutional." *Id.*

Defendants rely on *Mayfield v. United States*, 599 F.3d 964 (9th Cir. 2010), *see* Gov't Officials' MTD 19, but that reliance is misplaced. In *Mayfield*, the plaintiff sought a declaratory judgment that certain statutory provisions of FISA were "facially unconstitutional," while seeking as redress the government's return or destruction of all derivative materials it had obtained from Mayfield by unconstitutional means. 599 F.3d at 969. The Ninth Circuit held that the declaratory relief Mayfield sought would not require the government "to destroy or otherwise abandon the

materials." *Id.* at 971–72. For the reasons explained in *Doe*, 812 F.2d at 740, the Ninth Circuit erred. But even if *Mayfield* were correct, it would not preclude the type of declaratory relief sought here—which is directed at both the retention *and* the querying of the Xis' private information in government databases. The government has acknowledged that it routinely conducts such queries in its investigations; indeed, because of the vast quantity of digital information collected, those queries are one of the principal means by which FBI agents exploit all this data. *See* PCLOB Report 59; SAC ¶ 64 (describing the "FBI's Google"). A declaration that the prospective querying of the Xis' information violates their Fourth Amendment rights to be free of unreasonable searches and seizures would plainly afford them relief.

The government also invokes *United States v. Calandra*, 414 U.S. 338 (1974), to argue that because the exclusionary rule "does not foreclose the Government from making other uses" of illegally obtained information or "preclude the Government from retaining possession of the materials," it therefore follows that the declaration plaintiffs seek would not redress their injuries. *See* Gov't Officials' MTD 20. But the exclusionary rule is a court-created evidentiary rule applied in criminal cases. It says nothing about what relief is available to *civil* litigants challenging illegal Fourth Amendment searches. *See Calandra*, 414 U.S. at 347. The reach of the exclusionary rule thus has no bearing on the availability of declaratory relief to redress the Xis' ongoing Fourth Amendment injuries.

IV. Plaintiffs have plausibly alleged the violation of their Fourth Amendment rights.

A. Plaintiffs have plausibly alleged that they were subjected to criminal searches and FISA searches based on false affidavits.

The government contends that the Xis have not "plausibly" alleged that they were subjected to criminal searches and FISA searches on the basis of false affidavits, *see* Gov't Officials' MTD 21, but the complaint easily satisfies that standard, SAC ¶¶ 54–57, 59, 67. The

government's argument is duplicative of one made by defendant Haugen, and it fails for the very same reasons. Pl. Opp. to Haugen-MTD 27–35 (ECF 41) (incorporated herein by reference). The law clearly establishes that materially false, misleading, or fabricated allegations in a warrant application violate the Fourth Amendment. *See, e.g.*, *Andrews v. Scuilli*, 853 F.3d 690, 698 (3d Cir. 2017); *Betker v. Gomez*, 692 F.3d 854, 860 (7th Cir. 2012); *Chism v. Washington*, 661 F.3d 380, 392 (9th Cir. 2011). The government appears to concede this, but then simply ignores the specific facts set forth in the Xis' complaint. Gov't Officials' MTD 23. In brief, those factual allegations make clear that the assertions in the search warrants and the FISA orders were flawed just as the assertions in the indictment were flawed: they were the result of multiple falsehoods and/or omissions concerning (1) the basic superconductor technology at the heart of the alleged fraud; (2) the purpose of Professor Xi's international scientific collaborations; and (3) the contents of Professor Xi's communications with his scientist colleagues in China, none of which involved the STI pocket heater. SAC ¶¶ 55(a)–(g), 56–57, 59, 67. The complaint further alleges that these substantial falsehoods and omissions were material to the findings of probable cause, *id.* ¶¶ 59, 67, 127, 130, and that they were intentionally, knowingly and/or recklessly made by federal agents, *id.* ¶¶ 55–57, 59, 67. That is all that is required at this stage of the case to establish that the searches and seizures of the Xis' private communications and belongings violated the Fourth Amendment.[13]

[13] The government cites several criminal cases following *Franks v. Delaware*, 438 U.S. 154 (1978), to suggest that the Xis must, in essence, *prove* their claims in the pleadings by specifying each and every false allegation or misleading omission in the search applications. *See* Gov't Officials' MTD 22–23. But that is wrong. Whatever standard applies to criminal defendants seeking a *Franks* hearing, it is the plausibility standard that applies in this civil suit, as defendants themselves acknowledge. *See Hernandez-Cuevas v. Taylor*, 723 F.3d 91, 100–03 (1st Cir. 2013).

B. Professor Xi has plausibly alleged the warrantless surveillance of his communications.

Professor Xi's complaint presents specific, non-conclusory allegations about the warrantless surveillance of his communications with scientist colleagues in China. He has described an extensive surveillance apparatus, conducted under two complementary legal authorities, directed at monitoring Chinese scientific and academic research institutions. He has described the specific institutions the government monitored, his frequent communications with scientist counterparts at these institutions, and some of the specific communications the government intercepted without a warrant and then relied upon when it wrongfully prosecuted him. Not only that, but he has described how the government searches through its databases of warrantlessly collected communications, and how the government incorporates the fruit of this surveillance into FISA applications, like the one in his case. *See* SAC ¶¶ 60–65. These factual, well-pled allegations plausibly state a Fourth Amendment claim.

The government argues that Professor Xi has not alleged certain details related to this warrantless surveillance. Gov't Officials' MTD 25–26, 34–35. But as the Third Circuit has made clear, Professor Xi need not allege every operational detail related to the challenged surveillance (though he has pled a wealth of these facts, as discussed below). *See, e.g.*, *Schuchardt*, 839 F.3d at 347. Rather, accepting Professor Xi's factual allegations as true and drawing all reasonable inferences in his favor, his allegations that his communications were intercepted without a warrant must merely be plausible. *See, e.g.*, *id.*; *Iqbal*, 556 U.S. at 678.

The plausibility threshold has easily been met here. The complaint explains that, according to press reports, the NSA has engaged in extensive and concerted warrantless surveillance of Chinese universities and scientific research institutions. SAC ¶ 61. This warrantless surveillance includes two forms of collection. First, the government warrantlessly collects communications in

bulk, whereby virtually all messages or data on a system or network are captured. *Id.* Indeed, the government has acknowledged that it engages in the bulk interception and collection of communications under EO 12333. *Id.* Second, the government warrantlessly collects the communications of particular organizations, individuals, and Internet addresses. *Id.* For example, the government has obtained certifications under Section 702 that specifically authorize warrantless surveillance related to the Chinese government and its components. *Id.* The complaint also explains that one of Chinese institutions subject to warrantless surveillance prior to Professor Xi's arrest was state-run Tsinghua University, where the NSA siphoned data off of computers, servers, and network backbones connecting Tsinghua with other Chinese research institutions, such as Peking University and Shanghai Jiaotong University. *Id.*

The complaint then alleges how Professor Xi's communications were swept up in the NSA's warrantless surveillance and then used in the government's investigation. In the course of his work, Professor Xi frequently communicated with his scientist counterparts at a number of Chinese research institutions, including the specific universities subject to warrantless surveillance. SAC ¶ 62. Critically, all four of the emails relied upon by the government in its dismissed indictment were emails between Professor Xi and scientists working at Chinese research institutions—including Shanghai Jiaotong University and Peking University. Likewise, defendant Haugen referenced additional intercepted emails between Professor Xi and scientists at Tsinghua University in falsely asserting that Professor Xi had transmitted photographs of the STI pocket heater. *Id.* ¶¶ 62, 55(f). These emails are precisely the kinds of international communications that the government intercepts and exploits using its warrantless surveillance tools. *Id.* ¶¶ 60–61.

These well-pled allegations are further supported by Professor Xi's explanation of how the government incorporates the fruit of this surveillance into its FISA applications. *Id.* ¶¶ 64–65. In the early stages of investigations, FBI agents regularly rely on communications that the government has acquired without a warrant. *Id.* ¶ 65. As the Privacy and Civil Liberties Oversight Board has reported, FBI agents routinely conduct searches of databases containing the fruits of warrantless surveillance. *See id.* ¶ 64; PCLOB Report 59. These searches—which are designed to identify and exploit the communications of Americans collected without a warrant—are so common in FBI investigations that the government has referred to them as the "FBI's Google." SAC ¶ 64. The government then uses these warrantless sources of information in the applications it submits to the FISA Court—which is what happened in the investigation of Professor Xi. *Id.* ¶ 65. Even when the government uses information obtained or derived from warrantless surveillance in the course of a criminal investigation, as it did here, it regularly takes active steps to conceal the nature of its surveillance from defendants. *Id.* ¶ 66; *see* Section I.B.2.d, *supra*.[14]

The government is wrong to complain that Professor Xi, at this stage of the case, cannot identify with certainty which of these two *legal authorities* the government relied on to access his private communications. Whether the government relied on the authority of Section 702 and/or EO 12333 may bear on the government's legal justification for the surveillance; but it does not bear on the plausibility of Professor Xi's claim, as a factual matter, that his communications were intercepted and then queried without a warrant. Indeed, because warrantless searches are

[14] The government suggests that if it had used Section 702 surveillance, Professor Xi would have received notice of that fact. *See* Gov't Officials' MTD 33–34. But that is contrary to the well-pled allegations in the complaint, SAC ¶ 66, and it is belied by the government's conduct in other cases where it has concealed its use of Section 702. *See* Trevor Aaronson, *NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal*, Intercept, Nov. 30, 2017, https://bit.ly/2ExuYYJ. Notably, the government does not even attempt to argue that Professor Xi would have been told of the EO 12333 surveillance used to intercept his communications.

presumptively unconstitutional, *Katz*, 389 U.S. at 357, it is ultimately the government's burden to establish that its surveillance of Professor Xi was reasonable under the Fourth Amendment by identifying the legal basis for those searches. *See Coolidge v. New Hampshire*, 403 U.S. 443, 454–55 (1971); *Free Speech Coal., Inc. v. Attorney General*, 825 F.3d 149, 168–71 (3d Cir. 2016); *Wilson v. Health & Hosp. Corp. of Marion Cty.*, 620 F.2d 1201, 1208 (7th Cir. 1980) (citing *United States v. Jeffers*, 342 U.S. 48, 51 (1951)). For now, taking Professor Xi's factual, well-pled allegations as true, and drawing all inferences in his favor, it is more than plausible that his emails were subject to warrantless surveillance and querying. *See, e.g.*, *Iqbal*, 556 U.S. at 678; *Foglia*, 754 F.3d at 154. That is all that is required.

Indeed, Professor Xi's allegations of warrantless surveillance are more plausible than the allegations that survived a motion to dismiss in a recent Third Circuit case involving Section 702, *Schuchardt v. President of the United States*, 839 F.3d 336 (3d Cir. 2016). In *Schuchardt*, the plaintiff alleged that his communications were subject to a mass surveillance program under Section 702, known as PRISM, that collects "substantially all" email sent by Americans. *Id.* at 346. The government moved to dismiss the complaint on standing grounds, arguing that Schuchardt's allegation about the scope of PRISM was implausible. *See id.* The district court granted the motion, but the Third Circuit vacated that decision, holding that Schuchardt had plausibly alleged standing. Although the court acknowledged that "[s]everal commentators and the few courts that have examined PRISM appear to agree with the Government's view of the program's 'targeted' nature," *id.* at 352–53, it concluded that Schuchardt's allegations were plausible. The court emphasized that the plausibility threshold is a low one: it observed that "[t]he language of the leaked materials Schuchardt relies on is imprecise," and that "Schuchardt's alleged facts—*even if proven*—do not conclusively establish that PRISM operates as a dragnet on the

scale he has alleged." *Id.* at 351–52 (emphasis added).[15] It nonetheless allowed the case to proceed.

By contrast, here, Professor Xi's alleged facts, if proven, conclusively establish that his private communications were subject to warrantless surveillance. Like Schuchardt, Professor Xi has alleged that the government's bulk surveillance activities resulted in the acquisition of his email. *See* SAC ¶ 61 (relying on the government's own disclosures and news reports about the breadth of this surveillance). But Professor Xi has alleged even more: he has described the government's targeted surveillance; the specific institutions the government monitored; some of the specific communications intercepted without a warrant; and how the government searches for and uses those communications. *Id.* ¶¶ 61–65. Moreover, unlike Schuchardt, Professor Xi was targeted for traditional FISA surveillance—and, as the complaint explains in detail, it is more than plausible that the government relied on information obtained or derived from warrantless surveillance in its FISA application. *See* SAC ¶¶ 64–65.

C. The surveillance of Professor Xi's communications violated the Fourth Amendment's warrant requirement.

Professor Xi has plausibly alleged that the warrantless surveillance of his private communications violated the Constitution. Under the Fourth Amendment, Americans like Professor Xi have a protected privacy interest in the contents of their communications, including emails. *See United States v. U.S. Dist. Court* (*Keith*), 407 U.S. 297, 313 (1972); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). The government therefore needs a warrant to search

[15] The government seeks to distinguish *Schuchardt* on the ground that, in this case, the complaint incorporates the PCLOB Report by reference. Gov't Officials' MTD 27. But that fact is irrelevant, because—unlike in *Schuchardt*—the PCLOB Report in no way undermines Professor Xi's allegations about the scope of Section 702 surveillance. In fact, the PCLOB Report contains substantial additional *support* for Professor Xi's allegations, including his allegations about the FBI's routine searching of databases of warrantlessly intercepted communications. *See, e.g.*, PCLOB Report 59.

and seize these communications. *See Katz*, 389 U.S. at 357. Without a warrant, the government's searches of Professor Xi's emails were "per se unreasonable." *Id.*

Section 702 and EO 12333 do not require the government to obtain a warrant prior to collecting the emails and phone calls of Americans. Nor do they impose any comparable requirement after the fact—when the government seeks to use these communications in domestic investigations like the one that wrongfully targeted Professor Xi. Although courts have recognized a small number of "jealously and carefully drawn" exceptions to the warrant requirement, *Jones v. United States*, 357 U.S. 493, 499 (1958), surveillance conducted under Section 702 and EO 12333 does not fall within these narrow exceptions. Accordingly, Professor Xi has plausibly pled that the warrantless surveillance of his private communications violates the Fourth Amendment.

Even if an exception to the warrant requirement applies, Professor Xi has plausibly pled that the surveillance of his communications under these authorities fails to satisfy the Fourth Amendment's reasonableness requirement. *See* Section IV.D, *infra*. Reasonableness is a fact-specific inquiry that is assessed under the totality of the circumstances. *See, e.g.*, *Samson v. California*, 547 U.S. 843, 848 (2006). Here, as in many cases, that the Court does not yet have all the facts before it. *See, e.g.*, *Schuchardt*, 839 F.3d at 347–48; *J.A. v. Miranda*, No. PX 16-3953, 2017 WL 3840026, at *3 (D. Md. Sept. 1, 2017) ("[A]t the pleading stage, a plaintiff is not expected to possess complete knowledge of the defendant's alleged wrongful conduct, but need only submit facts sufficient to plead a plausible claim for relief. Indeed, the purpose of discovery is to establish the presence or absence of facts with which the plaintiff intends to prove his claim."). Factual information relevant to the reasonableness analysis is contained in the government's surveillance applications and other records concerning its investigation, which are not yet before the Court. Although Professor Xi has plausibly pled that the warrantless

surveillance of him was unreasonable, should the Court be inclined to hold otherwise, a more developed factual record would assist the Court in assessing the totality of the circumstances surrounding this surveillance. *See* Section IV.D, *infra*.

1. Warrantless searches are per se unreasonable.

The Fourth Amendment requires that search warrants be issued only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The Supreme Court has interpreted these words to require three things: (1) that any warrant be issued by a neutral, disinterested magistrate; (2) that the government demonstrate probable cause to believe that the evidence sought will aid in a particular apprehension or conviction; and (3) that any warrant particularly describe the things to be seized and the places to be searched. *See Dalia v. United States*, 441 U.S. 238, 255 (1979). Searches conducted without a warrant are "per se unreasonable under the Fourth Amendment." *Katz*, 389 U.S. at 357. Because surveillance under Section 702 and EO 12333 involves no showing of probable cause, no individualized judicial review, and no attempt at particularity, this surveillance is presumptively unconstitutional. *See id.*

2. The foreign-intelligence exception does not apply to the warrantless surveillance of Professor Xi.

The government contends that the warrant requirement does not apply here because Section 702 and EO 12333 surveillance serve a foreign-intelligence purpose and therefore fall within the "special needs" doctrine. *See* Gov't Officials' MTD 28–29, 36–37. This is incorrect for two reasons. Courts recognize an exception to the warrant requirement only "in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring). The warrant requirement is not impracticable here, as

evidenced by FISA itself. Moreover, even if a foreign-intelligence exception to the warrant requirement exists, such an exception applies only in narrow circumstances: when the government is targeting a foreign power or an agent of a foreign power. Yet Section 702 and EO 12333 contain no such requirement, and at this stage of the case, there is no allegation whatsoever that the government was targeting *foreign agents* when it warrantlessly intercepted Professor Xi's communications with scientist colleagues overseas. Consequently, the exception cited by the government simply does not apply.

First, the mere fact that the government conducts Section 702 and EO 12333 surveillance to acquire foreign intelligence information does not render probable cause and judicial review requirements unworkable. In *Keith*, the Supreme Court expressly rejected the government's argument that intelligence needs justified dispensing with the warrant requirement in domestic surveillance cases. 407 U.S. at 316–21. That logic applies with equal force to surveillance directed at targets with a foreign nexus—at least when that surveillance sweeps up Americans' communications, as Section 702 and EO 12333 surveillance do. In addition, history shows that the courts are capable of overseeing foreign intelligence surveillance of Americans' communications: since 1978, the FISC has granted more than 39,000 applications relating to foreign intelligence surveillance.[16] Prior to the passage of FISA, some courts permitted warrantless surveillance of foreign powers and their agents in certain limited circumstances. *See United States v. Butenko*, 494 F.2d 593, 605 (3d Cir. 1974); *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980). But the country's experience with FISA over the past forty years has profoundly undermined the rationale of those cases. *See United States v. Duka*, 671 F.3d 329, 341 (3d Cir. 2011) ("Admittedly, FISA changed the landscape . . . ."); *United States v. Bin Laden*, 126 F. Supp. 2d

[16] *See, e.g.*, Foreign Intelligence Surveillance Act Orders 1979–2016, Elec. Privacy Info Ctr., https://epic.org/privacy/surveillance/fisa/stats/default.html.

264, 272 n.8 (S.D.N.Y. 2000). Indeed, even in the context of surveillance conducted abroad, there is nothing impracticable about interposing a judge between the government and access to Americans' private information. Since the passage of the FISA Amendments Act in 2008, Congress has required prior judicial review and probable cause when the government seeks to target Americans outside the United States. *See* 50 U.S.C. § 1881c.

Second, the Supreme Court has never recognized a foreign-intelligence exception to the warrant requirement. But even if such an exception exists, it applies only where the government targets foreign powers or their agents, and therefore is not broad enough to render the warrantless surveillance of Professor Xi constitutional. Since the passage of FISA, some appellate courts have relied on a kind of foreign-intelligence exception to approve narrow modifications to the Fourth Amendment's probable-cause requirement—but *only* where the surveillance in question was specifically directed at foreign powers or their agents, and predicated on an individualized finding of suspicion. *See, e.g.*, *Duka*, 671 F.3d at 338 (approving court-authorized FISA surveillance of foreign agents); *United States v. Duggan*, 743 F.2d 59, 73–74 (2d Cir. 1984); *In re Sealed Case*, 310 F.3d 717, 720 (FISCR 2002).

Contrary to the government's suggestion, *see* Gov't Officials' MTD 28, the court of appeals in *Duka* did not embrace a wholesale exception to the warrant requirement for foreign-intelligence purposes. Rather, as the opinion makes clear, it considered whether FISA surveillance of foreign agents—predicated on a judicial finding of probable cause—was constitutional. *Duka*, 679 F.3d at 342, 345. Although the court suggested in dicta that pre-FISA cases had recognized "a sort of 'foreign intelligence exception' to the Fourth Amendment's warrant requirement," 679 F.3d at 341, those pre-FISA cases were also limited to surveillance of foreign powers or their agents. The *Duka* court did not have before it, and certainly did not approve, all warrantless

collection of Americans' communications for foreign intelligence purposes. Indeed, the court expressly distinguished cases involving warrantless surveillance, explaining that its analysis was limited to "the constitutionality of a program approved by Congress that requires an executive officer to apply to the judicial branch for a warrant-like order," *id.* at 342, and that requires an Article III judge to make "particularized findings" as to each foreign agent and the proposed surveillance, *id.* at 345.

The warrantless surveillance used to investigate Professor Xi is not constrained by any of these limitations. Neither Section 702 nor EO 12333 is confined to "foreign powers or agents of foreign powers reasonably believed to be located outside the United States"—a limitation that the FISCR deemed critical in *In re Directives Pursuant to Section 105B of FISA*, 551 F.3d 1004, 1012–16 (FISCR 2008). Instead, under both authorities, the government may target *any* non-citizen outside the United States—including innocent scientists, academic researchers, and private citizens—to acquire foreign intelligence information, broadly defined. Moreover, where prior cases required the President or Attorney General to make a probable-cause finding and personally approve the surveillance, *see, e.g.*, *In re Directives*, 551 F.3d at 1014, under Section 702 and EO 12333, individual targeting decisions have been handed off to an untold number of government analysts. Neither Section 702 or EO 12333 involves a judicial finding of probable cause, at any stage, even when an American's emails or phone calls are collected. In short, no court of appeals—including the Third Circuit—has ever recognized a foreign-intelligence exception sweeping enough to render constitutional the warrantless surveillance of Professor Xi in this case. *See* PCLOB Report 90 n.411.

There is no allegation or evidence, at this stage of the case, that the government was targeting a foreign agent when it intercepted Professor Xi's communications—let alone that this

surveillance was based on a judicial finding of probable cause. Accordingly, there is no factual or legal basis to conclude than any foreign-intelligence exception would excuse the warrantless surveillance of Professor Xi's emails and phone calls.

3. The government's warrantless surveillance of foreigners does not excuse its failure to obtain a warrant before exploiting the communications of Americans like Professor Xi.

The government makes a further, even broader argument to defend its warrantless surveillance of Professor Xi under Section 702. It contends that no warrant was needed to access those private communications—even when agents decided to use the "FBI's Google" to search specifically for Professor Xi's emails—because Section 702 surveillance "targets only non-U.S. persons located outside the United States." [17] Gov't Officials' MTD 30. In other words, the government argues that its surveillance of foreigners provides a warrantless backdoor into the communications of Americans who are swept up in that surveillance—a backdoor that FBI agents can readily exploit to pursue investigations of Americans here at home. But the government is wrong to claim that it can ignore the basic Fourth Amendment protections simply by "targeting" foreigners. Even if the government can surveil *foreigners* without a warrant, it must at a minimum obtain a warrant when it later deliberately seeks to use or search for the communications of *Americans* like Professor Xi.

The government cites *United States v. Mohamud*, 843 F.3d 420, 439–41 (9th Cir. 2016), and *United States v. Hasbajrami*, No. 11-cr-623 (JG), 2016 WL 1029500, at *7 (E.D.N.Y. Mar. 8, 2016), to support its claim. *See* Gov't Officials' MTD 30–31. But the rationale that the *Mohamud* and *Hasbajrami* courts relied on—often called the "incidental overhear" rule—has no application

[17] Notably, the government does not raise this argument with respect to its EO 12333 surveillance of Professor Xi, presumably because much of that surveillance is not "targeted" at all—but instead is "bulk" collection. *See* SAC ¶ 61; PPD-28 § 2 & n.5.

to the warrantless surveillance of Professor Xi. Instead, the formative cases establishing the incidental overhear rule apply it only when the government has *already sought and obtained a warrant*—and has thus established probable cause to believe that certain communications will contain evidence of criminal activity. *See United States v. Kahn*, 415 U.S. 143 (1974); *United States v. Donovan*, 429 U.S. 413, 418 (1977); *United States v. Figueroa*, 757 F.2d 466, 471 (2d Cir. 1985); *United States v. Martin*, 599 F.2d 880, 884–85 (9th Cir. 1979). Far from announcing an exception to the warrant requirement, these cases affirm the significance of that requirement.[18]

The *Mohamud* and *Hasbajrami* courts ignored the rationale for the incidental overhear rule, which is inextricably tied to the specific nature and function of a warrant.[19] The warrant process requires courts to carefully circumscribe surveillance, confining it to conversations that constitute evidence of a particular crime and limiting the intrusion as to both the target and any person with whom the target communicates. Thus, when the government has established probable cause to seize certain communications—and has thereby satisfied the necessary Fourth Amendment threshold—its warrant satisfies the privacy interests of all parties to the communications, including parties who are incidentally overheard. *See Figueroa*, 757 F.2d at 471. Because of this, the incidental overhear cases merely stand for the proposition that the government need not obtain multiple warrants to intercept protected communications. *See Kahn*, 415 U.S. at

[18] The government's use of the term "incidental" suggests that its warrantless collection of Americans' communications under Section 702 is a *de minimis* or unintended byproduct, common to all forms of surveillance. In reality, however, the warrantless surveillance of Americans' communications was both the purpose and the direct result of Section 702. *See* PCLOB Report 82, 86–87. Moreover, the *volume* of communications intercepted "incidentally" under Section 702 dwarfs that of communications intercepted incidentally under the original provisions of FISA or Title III. *See* President's Review Group on Intelligence and Comms. Techs., *Liberty and Security in a Changing World* 149 (Dec. 12, 2013), https://perma.cc/9LYQ-DVJL ("PRG Report").

[19] *See* Elizabeth Goitein, *The Ninth Circuit's Constitutional Detour in* Mohamud, Just Security (Dec. 8, 2016), https://goo.gl/G8wT3X.

153. By contrast, the "complete absence of prior judicial authorization would make an [incidental] intercept unlawful." *Donovan*, 429 U.S. at 436 n.24. Here, because the government did not obtain a warrant at all—not even one directed at Professor Xi's scientist counterparts—the incidental overhear doctrine simply does not apply.[20]

The surveillance of Professor Xi—like other Section 702 and EO 12333 surveillance—did not involve a warrant. SAC ¶¶ 60–64. There was no showing of probable cause; there was no individualized judicial review; and there was no attempt at particularity. That the government's "target" was not a U.S. person may be sufficient to allow the government to warrantlessly surveil *that* person. But the Fourth Amendment's protection is nowhere limited to "targets."[21] Even if the government claims to be targeting someone who lacks Fourth Amendment rights, it is not entitled to ignore the rights of an American like Professor Xi, who *is* entitled to that protection.

United States v. Verdugo-Urquidez, 494 U.S. 259, 277–78 (1990), is not to the contrary. The Supreme Court's analysis in *Verdugo* focused exclusively on Fourth Amendment protections available to foreign nationals located abroad. That decision did not excuse the government from complying with the warrant requirement when it searches the communications of a U.S. person who is on U.S. soil, like Professor Xi. *See id.* at 274–75. Similarly, nowhere did the Court's analysis suggest that searches of Americans' international communications are exempt from the

[20] The third criminal Section 702 case cited by the government, *United States v. Muhtorov*, 187 F. Supp. 3d 1240 (D. Colo. 2015), also involves a fundamental doctrinal error. *See* Gov't Officials' MTD 31, 33. The district court there reasoned that the defendant's privacy interest in his email was "at least somewhat diminished when transmitted to a third party over the internet." *Muhtorov*, 187 F. Supp. 3d at 1255. But the third-party doctrine does not apply to the contents of private emails that are not deliberately shared with a third party. *See, e.g.*, *Warshak*, 631 F.3d at 286–88 ("[A] subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial [internet service provider].").

[21] *See* Orin Kerr, *The Surprisingly Weak Reasoning of* Mohamud, Lawfare (Dec. 23, 2016), https://www.lawfareblog.com/surprisingly-weak-reasoning-mohamud.

Fourth Amendment's warrant requirement. To the contrary, Americans' international letters, phone calls, and emails have long been protected by a warrant requirement. *See, e.g.*, *United States v. Ramsey*, 431 U.S. 606, 623–24 (1977) (citing regulations requiring a warrant to read the contents of international letters); 18 U.S.C. § 2518 (warrant required for the interception of phone calls, including international calls).

In sum, regardless of whether the warrant requirement applies to the communications of foreigners overseas, it unquestionably reaches the communications of Americans. To the extent the government argues that it cannot know in advance when it will "incidentally" collect these protected communications, there is a practical and familiar solution. The government must, at a minimum, obtain a warrant after the fact—when it deliberately seeks to use or search its databases for the communications of Americans like Professor Xi. Such a requirement is not unusual. Especially in the context of electronic searches, courts and Congress have frequently required the government to obtain a warrant after its initial seizure or search. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473 (2014) (requiring government to obtain a warrant before searching cell phone lawfully seized incident to arrest); 50 U.S.C. § 1801(h)(4) (requiring government to obtain a warrant within 72 hours of incidentally intercepting U.S. person's communications); *United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013) (requiring government to obtain a warrant before conducting new search of lawfully seized computer hard-drive). The Fourth Amendment required the same after-the-fact warrant here, when agents decided to use or search for Professor Xi's protected communications.

D. The warrantless surveillance of Professor Xi's communications was unreasonable under the Fourth Amendment.

Regardless of whether the warrant requirement applies, "the ultimate touchstone of the Fourth Amendment is reasonableness." *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). Thus,

even if the government were excused from complying with the warrant requirement, it must still establish that it afforded Professor Xi sufficient safeguards to render the infringement on his privacy—including the interception, querying, and use of his communications—reasonable under the circumstances. Reasonableness is assessed based upon "the totality of the circumstances," *Samson*, 547 U.S. at 848, and it is the government's burden to establish that any warrantless search was reasonable. *See, e.g.*, *Coolidge*, 403 U.S. at 455; *Free Speech Coal.*, 825 F.3d at, 168–69. This analysis is a fact-intensive inquiry that other courts have deferred until a factual record is before them. *See Fortune Players Grp., Inc. v. Quint*, No. 16-cv-00800, 2016 WL 4091401, at *6–7 (N.D. Cal. Aug 2, 2016) (denying motion to dismiss complaint that challenged warrantless search, finding that "Plaintiffs have alleged plausible facts that the search conducted by Defendants was unreasonable" and that "it is clear to the Court that reasonableness, generally, is a question for the fact-finder armed with evidence from discovery, and is not proper for a motion to dismiss"); *Leach ex rel. Dyson v. Principal Baum*, No. Civ. A. 04-135, 2004 WL 834732, at *2 (E.D. Pa. Apr. 16, 2004) ("The legality of the search is—at least in part—a factual question. This is a motion to dismiss, and because there is no record the Court cannot make any determinations as to the reasonableness of Defendant's conduct.").

This Court should likewise defer any reasonableness analysis. While both Section 702 and EO 12333 involve far-reaching warrantless surveillance, that surveillance is implemented in multiple ways. The breadth and intrusiveness of the surveillance used against Professor Xi may bear on the reasonableness analysis. Similarly, the manner in which the resulting data was amassed, searched, and then exploited in the government's investigation of Professor Xi is critical.

Discovery will provide additional information about how widely and freely the FBI exploited its warrantless backdoor into Professor Xi's communications during the course of its investigation. [22]

In any event, even if the Court reaches the question of reasonableness, Professor Xi has more than plausibly alleged that the warrantless exploitation of his communications in this case was unreasonable. The question is not whether the government is permitted to surveil foreigners without first obtaining a warrant. The question is what basic protections the government must afford Americans like Professor Xi who are swept up in that warrantless surveillance. The government's conduct was unreasonable because it exploited an immense loophole to investigate and ultimately prosecute an American: it not only intercepted Professor Xi's private communications without a warrant, but it then proceeded to store them in vast government databases where agents deliberately queried and used those communications to investigate Professor Xi here on U.S. soil—without any of the safeguards that the Fourth Amendment requires. SAC ¶¶ 60–65.

The government was not entitled to completely bypass Professor Xi's Fourth Amendment rights in this way. To the extent the government claims it is unable to avoid *intercepting* Americans' communications in the first instance, reasonableness requires it to apply Fourth Amendment protections at another critical juncture: when agents deliberately seek to *use or query* Americans' private communications in their investigations. Rather than imposing the robust "post-seizure" limitations required by the Fourth Amendment, Section 702 and EO 12333 permit the backdoor access that agents exploited here. Accordingly, Professor Xi has plausibly stated a claim that the surveillance of him was unreasonable.

[22] Should the government contend that the information sought through discovery is classified or subject to the state secrets privilege, FISA provides a straightforward process for judicial review and disclosure of that information under appropriate security measures. *See* 50 U.S.C. § 1806(f).

1. The warrantless surveillance of Professor Xi lacked core safeguards that courts require when assessing the reasonableness of electronic surveillance.

As described above, reasonableness is determined by examining the "totality of the circumstances," in order to "assess[], on the one hand, the degree to which [government conduct] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Samson*, 547 U.S. at 848 (internal citation omitted). In the context of electronic surveillance, reasonableness requires that government eavesdropping be "precise and discriminate" and "carefully circumscribed so as to prevent unauthorized invasions" of privacy. *Berger*, 388 U.S. at 58; *see United States v. Bobo*, 477 F.2d 974, 980 (4th Cir. 1973).

Courts assessing the lawfulness of electronic surveillance have looked to FISA and Title III as measures of reasonableness. *See United States v. Biasucci*, 786 F.2d 504, 510 (2d Cir. 1986). While the limitations on foreign-intelligence surveillance may differ in some respects from those applicable to law-enforcement surveillance, "the closer [the challenged] procedures are to Title III procedures, the lesser are [the] constitutional concerns." *In re Sealed Case*, 310 F.3d at 737.

Section 702 and EO 12333 abandon the three core safeguards—individualized judicial review, a finding of probable cause, and particularity—that courts have relied on to uphold the constitutionality of both FISA and Title III. *Duggan*, 743 F.2d at 73–74 (FISA); *In re Sealed Case*, 310 F.3d at 739–40 (FISA); *United States v. Tortorello*, 480 F.2d 764, 772–73 (2d Cir. 1973) (Title III).

First, Section 702 and EO 12333 fail to interpose "the deliberate, impartial judgment of a judicial officer . . . between the citizen and the police." *Katz*, 389 U.S. at 357. The Fourth Amendment reflects a judgment that "[t]he right of privacy [is] too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals." *McDonald v.*

United States, 335 U.S. 451, 455–56 (1948). But under Section 702, the FISC's role consists principally of reviewing targeting and minimization procedures; and under EO 12333, no court has any role at all. Every decision concerning specific surveillance targets is left to the discretion of executive-branch employees, even as these decisions affect countless Americans.

Second, both authorities fail to condition surveillance on the existence of probable cause of any kind. They permit the government to conduct surveillance without proving to a court that the people it seeks to surveil are foreign agents, engaged in criminal activity, or connected—even remotely—with terrorism. 50 U.S.C. § 1881a(a); EO 12333 § 2.3; USSID 18 § 4. They permit the government to conduct surveillance without even an executive-branch determination that its targets fall into any of these categories.

Third, surveillance under these authorities is not particularized. The requirement of particularity "is especially great in the case of eavesdropping," which inevitably results in the interception of unrelated, intimate conversations. *Berger*, 388 U.S. at 56. Under Section 702, the government collects—wholesale and on an ongoing basis—all communications to and from more than one hundred thousand targets. Under EO 12333, the government conducts a wide array of surveillance programs—including bulk surveillance programs—that sweep up the communications of countless Americans. Unlike Title III and FISA, however, Section 702 and EO 12333 do not require the government to identify to *any* court the telephone lines, email addresses, or places at which its surveillance will be directed, or "the particular conversations to be seized." *Donovan*, 429 U.S. at 427 n.15.

Because Section 702 and EO 12333 fail to include these bedrock safeguards, government agents may target essentially any foreigner for surveillance—and may thereby collect the emails and phone calls of all U.S. persons communicating with those foreigners. Indeed, under EO

12333, the government need not target anyone at all, instead often conducting "bulk" surveillance that sweeps in untold volumes of Americans' communications. SAC ¶ 61.[23]

2. The warrantless surveillance of Professor Xi lacked sufficient "post-seizure" protections to be reasonable under the Fourth Amendment.

The warrantless surveillance of Professor Xi involved not just the interception of his communications, but the government's further querying and use of those protected communications in an investigation that specifically targeted him. SAC ¶¶ 64–65. The absence of strong "post-seizure" protections—which left the government free to exploit this backdoor into Professor Xi's communications—is unreasonable under the Fourth Amendment.

The constitutionality of electronic surveillance depends not just on limitations on initial collection, but also on the restrictions on later retention and use. Because Section 702 and EO 12333 are extremely permissive at the outset—allowing the broad, continuous collection of billions of communications—post-seizure restrictions on the use of this information are critical to the Fourth Amendment analysis. In assessing such restrictions, the government's justification for its initial search matters. Where, as here, the government justifies warrantless surveillance by asserting that its foreign targets lack Fourth Amendment rights (or that it is engaging in bulk surveillance with no target at all), the government's subsequent use and querying of *Americans'* communications without any individualized judicial approval is unreasonable. *See In re*

[23] The government's discussion of the statutory prohibition on "reverse targeting" is a red herring. *See* Gov't Officials' MTD 33–34. Plaintiffs' complaint acknowledges that, under both Section 702 and EO 12333, the government is not permitted to "target" Americans directly when it initiates the surveillance. SAC ¶ 60. Nonetheless, the FBI and NSA routinely obtain the communications of Americans who are in contact with the vast number of overseas targets, *see id.*—what the government calls "incidental collection." Gov't Officials' MTD 32. Moreover, even though the government is prohibited from specifically targeting Americans at the *outset* of its surveillance, it effectively targets Americans *after* acquiring their communications by searching its vast databases—without a warrant—for email accounts and other identifiers associated with individual Americans like Professor Xi. SAC ¶ 64.

Directives, 551 F.3d at 1015 (finding warrantless surveillance of foreigners reasonable only after the government represented that it was not amassing databases of Americans' incidentally collected communications); *see generally Terry v. Ohio*, 392 U.S. 1, 19 (1968) ("The scope of the search must be strictly tied to and justified by the circumstances which rendered its initiation permissible." (quotation marks omitted)).

Because of the "inherent dangers" and overbreadth of electronic searches, courts have long looked to post-seizure limitations when analyzing the reasonableness of surveillance. *Berger*, 388 U.S. at 58–60 (faulting New York's eavesdropping statute for permitting broad retention and use, and for failing to require notice to those surveilled); *see also, e.g.*, *Tortorello*, 480 F.2d at 772–73, 783–84 (upholding Title III based in part on post-seizure procedures); *In re Sealed Case*, 310 F.3d at 740 (upholding traditional FISA based in part on post-seizure procedures).

While the government concedes that post-seizure protections are relevant to reasonableness, it misleadingly argues that Section 702 "minimization" procedures are comparable to those under Title III and traditional FISA. *See* Gov't Officials' MTD 32. In reality, Section 702 procedures are far weaker, especially when considered in the context of the surveillance as a whole. Under both Title III and traditional FISA, minimization operates as a *second* layer of protection against the retention, use, and dissemination of information relating to U.S. persons. The first layer of protection comes from the requirement of individualized judicial authorization for each surveillance target. In contrast, Section 702 procedures allow the government to collect Americans' communications on U.S. soil without a warrant or anything approaching one. They allow the government to retain those communications for five years by default—and to pool them in massive centralized databases. And they allow agents to conduct queries that deliberately target Americans' communications after they are collected—including for use at the earliest stages of

ordinary criminal investigations—as a matter of course. *See* PCLOB Report 55–60. EO 12333's post-seizure protections are likewise inadequate in light of the breadth of the collection under that authority. *See* SAC ¶ 63; John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, Wash. Post, July 18, 2014, http://wapo.st/1wPuzv2. They too allow the government to retain communications for five years by default, to pool them in massive databases, and to query those databases using identifiers associated with Americans, without any judicial approval. *See* USSID 18 §§ 4–6.

Given the breadth of Section 702 and EO 12333 collection and the absence of traditional Fourth Amendment safeguards at the outset, the lack of strong post-seizure protections is fatal to the reasonableness of the surveillance used in this case. Even if the government cannot always know whether surveillance directed at a given foreigner will sweep up protected communications involving Americans, that fact does not excuse the government from obtaining individualized judicial approval when it *later* seeks to use communications that it knows are protected. At the very least, reasonableness requires the provision of strong safeguards for Americans after the government intercepts their private communications.[24]

Such protections are workable. Indeed, a number of proposals would provide additional post-seizure protections for Americans' communications acquired through warrantless foreign intelligence surveillance. During the debate that preceded Section 702, then-Senator Barack Obama co-sponsored an amendment that would have prohibited the government from (1) acquiring a communication without a warrant if it knew "before or at the time of acquisition that the communication [was] to or from a person reasonably believed to be located in the United

[24] *See* Peter Swire & Richard Clarke, *Reform Section 702 to Maintain Fourth Amendment Principles*, Lawfare (Oct. 19, 2017), https://goo.gl/RHqdND; Geoffrey Stone & Michael Morell, *The One Change We Need to Surveillance Law*, Wash. Post, Oct. 9, 2017, http://wapo.st/2hZ1xJx.

States," and (2) accessing Americans' communications collected under Section 702 without a warrant. *See* S.A. 3979, 110th Cong. (2008), 154 Cong. Rec. S607-08 (daily ed. Feb. 4, 2008). More recently, the President's Review Group concluded that a warrant requirement should be imposed for searches for Americans' communications in Section 702 and EO 12333 databases, and the House of Representatives passed a bill that would prohibit the retention and use of Americans' communications. *See* PRG Report 28-29; H.R. 4870, 113th Cong. § 8127 (2014). There is no practical reason why these limitations—which have the effect of requiring safeguards only for the communications of Americans like Professor Xi—could not be imposed here.

More generally, both Congress and courts have often addressed similar problems when confronted with broad seizures of digital information. In response, they have imposed rules to ensure that the government's *use* of seized data does not exceed its Fourth Amendment authority. These rules routinely require the government either to refrain from using information beyond the scope of its legal authority or to secure additional court authorization after the fact.

For instance, in the case of traditional FISA surveillance, Congress imposed strict minimization rules to ensure that warrantless surveillance directed exclusively at foreign powers—for example, surveillance of foreign embassies—does not intrude upon the rights of U.S. persons swept up in that surveillance. *See* 50 U.S.C. §§ 1801(h)(4), 1802(a)(1). If the government learns after that fact that it has collected an American's communications without a warrant, it is required to destroy the protected communications within 72 hours or to obtain an individualized FISC order to retain them. *Id.* § 1801(h)(4). Because this surveillance is warrantless and targeted at foreign powers, it is closely analogous to that conducted under Section 702.

In the case of warrantless surveillance conducted under Section 702's predecessor statute, the Protect America Act, the FISCR held the surveillance reasonable only after finding that the

government was not amassing a searchable database of Americans' incidentally collected communications (as it does under Section 702). *See In re Directives*, 551 F.3d at 1015. Similarly, the FISC prohibited the NSA from conducting backdoor searches of its Section 702 databases for years—an after-the-fact restriction designed to protect Americans' privacy.[25]

In the case of computer hard-drive searches, where data is often intermingled, courts have also recognized the importance of post-seizure restrictions. Even when the government lawfully seizes the full contents of a device pursuant to a warrant, it may only search for the particular information authorized by its original probable-cause warrant—at least not without further court authorization. *See United States v. Galpin*, 720 F.3d 436, 446–47 (2d Cir. 2013); *Sedaghaty*, 728 F.3d at 913.

In each of these instances, either courts or Congress have imposed workable solutions, in order to ensure that the government's electronic searches are properly confined. Similarly here, the mere fact that the government is "targeting" foreigners—or conducting bulk surveillance—when it acquires Americans' protected communications is not a valid reason to jettison all the safeguards that Professor Xi would otherwise have been afforded by a warrant. While post-seizure restrictions could adequately protect the rights of Americans caught up in the government's warrantless surveillance net, the procedures used to surveil Professor Xi did the opposite—they gave investigators license to exploit his communications. Because of this, the government's surveillance was unreasonable.

[25] The NSA was prohibited from conducting backdoor searches on all communications acquired through Section 702 until 2011, and on a particularly sensitive subset of those communications until 2017. *See* James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls*, Guardian, Aug. 9, 2013, https://goo.gl/DDg2zZ; [*Redacted*], No. [Redacted], at 28 (FISC Apr. 26, 2017), https://perma.cc/7X2S-VAS7.

Conclusion

For the foregoing reasons, Plaintiffs Xiaoxing Xi, Qi Li, and Joyce Xi respectfully request that the Court deny the Official Capacity Defendants' motion to dismiss.

Respectfully submitted,

/s/ Patrick Toomey
Patrick Toomey
Ashley Gorski
Jonathan Hafetz
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
(212) 549-2654 (fax)
ptoomey@aclu.org

David Rudovsky
Jonathan H. Feinberg
Susan M. Lin
KAIRYS, RUDOVSKY, MESSING, FEINBERG & LIN LLP
The Cast Iron Building
718 Arch Street, Suite 501 South
Philadelphia, PA 19106
(215) 925-4400
(215) 925-5365 (fax)

Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I, Patrick Toomey, hereby certify that on April 9, 2018 the foregoing Plaintiffs' Response in Opposition to the Official Capacity Defendants' Motion to Dismiss the Complaint was filed via the Court's ECF system and, as such, was served on the below counsel:

Paul E. Werner
Trial Attorney
United States Department of Justice
Civil Division, Tort Branch
P.O. Box 7146
Washington, D.C. 20044
Paul.Werner@usdoj.gov

Elizabeth Tulis
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, D.C. 20044
Elizabeth.Tulis@usdoj.gov

/s/ Patrick Toomey
Patrick Toomey