# 14-42

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES Page(s)

*A* Brian Carver is an Assistant Professor at the University of California, Berkeley, where he writes and teaches on Technology Law and Information Law.

*A* Fred H. Cate is Distinguished Professor and C. Ben Duton Professor of Law at Indiana University, Maurer School of Law. He is the Director of the Center for Applied Cybersecurity Research and the Director of the Center for Law, Ethics, and Applied Research in Health Information.

*A* Erwin Chemerinsky is the founding Dean, Distinguished Professor of Law, and Raymond Pryke Professor of First Amendment Law at the University of California, Irvine, School of Law. His areas of expertise include Constitutional Law, Civil Rights, and Civil Liberties.

*A* Ralph D. Clifford is a Professor of Law at the University of Massachusetts School of Law, where he writes and teaches on Intellectual Property and Cyberlaw.

*A* Julie Cohen is a Professor of Law at Georgetown Law, where she writes and teaches on Privacy Law and governance of communications networks. She is a member of the Advisory Board of the Electronic Privacy Information Center and the Advisory Board of Public Knowledge.

*A*

and the Law, where she writes and teaches on Constitutional Law, National Security Law, and Legal History.

*A* Susan Freiwald is a Professor of Law at the University of San Francisco School of Law, where she writes and teaches on Cyberlaw and information privacy.

*A* A. Michael Froomkin is the Laurie Silvers & Mitchell Rubenstein Distinguished Professor of Law at the University of Miami School of Law, where he writes and teaches on Constitutional Law, Internet Law, and Privacy Law. He is on the Advisory Board of the Electronic Frontier Foundation and a non-resident Fellow of the Center for Democracy & Technology and the Yale Law School Information Society Project.

*A* Ahmed Ghappour is a Clinical Instructor of Law in the Civil Rights Clinic and the Director of the National Security Defense Project at the University of Texas School of Law. He is a National Security Committee member of the National Association of Criminal Defense Lawyers.

*A* Shubha Ghosh is the Vilas Research Fellow & Professor of Law at the University of Wisconsin Law School, where he writes and teaches on Intellectual Property, Internet Law and Privacy Law. He is a member of the Executive Committee of the American Association of Law Schools' Section on Internet and Computer Law.

Jennifer Stisa Granick is the Director of Civil Liberties at the

*A* Karl Manheim is a Professor of Law at Loyola Law School, Los Angeles, where he writes and teaches in the areas of Constitutional Law, Cyberlaw and Technology, and Privacy.

*A* Ranjana Natarajan is a Clinical Professor at the University of Texas School of Law, where she directed the National Security Clinic 2009-2013, and where she is now the Director of the Civil Rights Clinic. She writes and teaches on Constitutional Law, National Security Law, and Privacy Law.

*A* David W. Opderbeck, Professor of Law at Seton Hall University Law School, is the Director of the Gibbons Institute of Law, Science & Technology, where he writes and teaches on the regulation of access to scientific and technological information.

*A* Peter Raven-Hansen is the Glen Earl Westen Research Professor of Law at George Washington University Law School, where he writes and teaches on Constitutional Law, National Security Law, and Counterterrorism Law. He is the Co-director of the National Security and U.S. Foreign Relations Law Program.

*A* Kim Lane Scheppele is Rockefeller Professor of International Affairs at the Woodrow Wilson School and the D

*A* Jessica Silbey is a Professor of Law at Suffolk University Law School, where she teaches and writes on Intellectual Property and Constitutional Law.

*A* Katherine J. Strandburg is the Alfred B. Engelberg Professor of Law at New York University School of Law, where she teaches and writes on Intellectual Property, Cyberlaw, and Information Privacy Law. She joins as an in her individual capacity and not on behalf of New York University School of Law.

Amicus Peter Swire is the Huang Professor at the Georgia Institute of Technology Scheller College of Business and was appointed by President Obama to the five-member Review Group that reported in December 2013 on the Section 215 metadata collection program. He served as Chief Counselor for Privacy in the Office of Management and Budget under President Clinton, and was Special Assistant to the President for Economic Policy in 2009-2010.

*A* Jonathan Weinberg is a Professor of Law at Wayne State University, where he writes and teaches on Constitutional Law, Internet Law, and Privacy Law. A former Justice Department and FCC lawyer, he chaired a working group created by ICANN (the Internet Corporation for Assigned Names and Numbers), to develop recommendations on the creation of new top-level Internet domains.

## SUMMARY OF ARGUMENT

Congress introduced the Foreign Intelligence Surveillance Act of 1978 to prevent the National Security Agency ("NSA") and other federal intelligence-gathering entities from engaging in broad domestic surveillance. The legislature

In the early 1970s, public allegations related to intelligence agencies' impropriety, illegal activities, and abuses of authority prompted both Houses of Congress to create temporary committees to investigate the accusations: the House Select Committee on Intelligence, and the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. H.R. Res. 138, 94th Cong. (1975); H.R. Res. 591, 94th Cong. (1975); S. Res. 21, 94th Cong. (1975).

The allegations centered on activities undertaken by three organizations: the NSA, the Federal Bureau of Investigation ("FBI"), and the Central Intelligence Agency ("CIA"). Frederick M. Kais 0 0Tm /E.8 ( ) -8491.76 24 cm B1 Tm334.16cm BT 50 0 0 50

establishment of the Select Committee, endorsing its creation by a vote of 82-4. 121 Cong. Rec. 1,416-34 (1975).

The Senate directed the committee to do two things: to investigate "illegal, improper, or unethical activities" in which the intelligence agencies engaged, and to determine the "need for specific legislative authority to govern" the NSA and other agencies. S. Res. 21, 94th Cong. (1975).

The Committee subsequently took testimony from hundreds of people, inside and outside of government, in public and private hearings. The NSA, FBI, CIA, and other federal agencies submitted files. In 1975 and 1976 the Committee issued seven reports and 6 supplemental volumes. Since 1992, another 50,000 pages have been declassified and made publicly available at the National Archives. History Matters, , available at http://history-matters.com/archive/contents/church/contents_church_reports_rockcomm.htm; and Press Release, National Security Agency Central Security Service, The National Security Agency Releases Over 50,000 Pages of Declassified Documents (June 8, 2011), http://www.nsa.gov/public_info/press_

(1975) (Vols. 1-7). The illegal activities, abuse of authority, and violations of privacy uncovered by the Committee spurred Congress to pass the Foreign Intelligence Surveillance Act.

### A. The NSA Has a History of Conducting Broad Domestic Surveillance Programs Under the Guise of Foreign Intelligence

In October 1952

Neither the 1952 Presidential directive, nor National Security Council Intelligence Directive ("NSCID") No. 6, which authorized the CIA to engage in Foreign Wireless and Radio Monitoring, defined the term "foreign communications." NSCID No. 6, Dec. 12, 1947 (National Archives and Records Administration, RG 59, Records of the Department of State, Records of the Executive Secretariat, NSC Files: Lott 66 D 148, Dulles-Jackson-Correa Report, Annex 12); s

, . *5,* , at 6.

NSCID 9, however, entitled Communications Intelligence, defined "foreign communications" as "all communications and related materials . . . of the government and/or their nationals or of any military, air, or naval force, faction, party, department, agency, or bureau of a foreign country, or of any person or persons acting or purporting to act therefor." It included "all other telecommunications and related material of, to, and from a foreign country which may contain information of military, political, scientific or economic value." NSCID No. 9, Jul. 1, 1948 (National Archives and Records Administration, RG 59, Records

The NSA did not (indeed, could not) discuss NSCID 9 during the Church Committee's public hearings. However, the Director of Central Intelligence had issued a directive that the NSA did discuss, which employed a definition of foreign communications that communications between U.S. citizens or entities. , . *5*, , at 9. Accordingly, the NSA focused on communications

. . .

Testifying in 1975 before the Church Committee, Lieutenant General Lew Allen, Jr., Director, National Security Agency explained that the NSA did not at that time, nor had it (with one exception—i.e., individuals whose names were contained on the NSA's watch list) "conducted intercept operations for the purpose of obtaining the communications of U.S. citizens." . Nevertheless, "some circuits which are known to carry foreign communications necessary for foreign intelligence will also carry personal communications between U.S. citizens, one of whom is at a foreign location." .

Central to Allen's assertion was the understanding that, to constitute foreign communications, and to legitimate the collection of information on U.S. citizens, the target of the surveillance must be a foreign power, or an agent of a foreign power, and at least one party to the communications must be outside the country.

The Senate considered even this approach, in light of the broad swathes of information obtained about U.S. citizens, to run afoul of the Fourth Amendment. Two NSA programs, in particular, generated significant concern.

### 2. Project MINARET, Introduced to Collect Foreign Intelligence Information, Ended up Intercepting Hundreds of U.S. Citizens' Communications

Like the Internal Revenue Service ("IRS"), the FBI, and the CIA, the NSA had composed a list of U.S. citizens and non-U.S. citizens subject to surveillance. , . *5,* , at 3. The program, which operated 1967-1973, started out by focusing on the international communications of U.S. citizens traveling to Cuba. It quickly expanded, however, to include individuals (a) involved in civil disturbances, (b) suspected of criminal activity, (c) implicated in drug activity, (d) of concern to those tasked with Presidential protection, and (e) suspected of involvement in international terrorism. . at 10-11.

In 1969 the collection of information on individuals included in the watch list became known as Project MINARET. . at 30. Senators and members of the public expressed alarm about the privacy implications. Of central concern was the potential for such programs to target communications of a wholly domestic nature.

Senator (later Vice President) Walter Mondale, articulated the Committee's disquiet:

> Given another day and another President, another perceived risk and someone breathing hot down the neck of the military leader then in charge of the NSA: demanding a review based on another watch list, another wide sweep to determine whether some of the domestic dissent is really foreign

The telephony program also goes substantially beyond the previous surveillance operation in its focus on purely local calls. According to the Director the National Security Agency, Project MINARET did not monitor entirely domestic conversations.

Operation SHAMROCK was the cover name given to a program in which the government had convinced three major telegraph companies (RCA Global, ITT World Communications, and Western Union International) to forward international telegraphic traffic to the Department of Defense. . at 57-58. For nearly thirty years, the NSA and its predecessors received copies of most international telegrams that had originated in, or been forwarded through, the United States. . at 58.

Operation SHAMROCK stemmed from wartime measures, in which companies turned messages related to foreign intelligence targets over to military intelligence. In 1947, the Department of Defense negotiated the continuation of the program in return for protecting the companies from criminal liability and public exposure. .

Like Project MINARET, the scope of the program expanded. Initially, the program focused on foreign targets. Eventually, however, as new technologies became available, the NSA began extracting U.S. citizens' communications. . at 58-59. It selected approximately 150,000 messages per month for further analysis, distributing some messages to other agencies. . at 60.

Senators expressed strong concern at the resulting privacy violations, inviting the Attorney General before the Select Committee to discuss "the Fourth Amendment of the constitution and its application to the 20th century problems of intelligence and surveillance." . at 65. Senator Church explained:

> aggravated present ambiguities in the law. The broad sweep of communications interception by NSA takes us far beyond the previous fourth amendment controversies where particular individuals and specific telephone lines were the target. .

The question that confronted Congress was how to control new, sophisticated technologies, thus allowing intelligence agencies to perform their legitimate foreign intelligence activities, without also allowing them to invade U.S. citizens' privacy by allowing them access to information unrelated to national security. .

In the absence of any governing statute, Attorney General Edward H. Levi's approach had been to authorize the requested surveillance only where a clear nexus existed between the target and a foreign power. . at 71. The Attorney General sought to distinguish the process from the British Crown's use of writs of assistance, in the shadow of which James Madison had drafted the Fourth Amendment. . at 71-72. The Founders'

In the 1960s and 1970s the FBI, CIA, IRS, U.S. Army, and other federal entities similarly engaged in broad, domestic intelligence-gathering operations. Details relating to many

personal mail in the United States; (b) infiltrated domestic dissident groups and intervened in domestic politics; (c) engaged in illegal wiretaps and break-ins; and (d) improperly assisted other government agencies. .

In 1972 the Supreme Court had h

(1976). Its successor bill

## II. Congress Inserted Four Protections to Limits the Nature of Foreign Intelligence Gathering

dissenting voice vote." . The House of Representatives, in turn, adopted the Conference Report by a vote of 226 to 176. 124 Cong. Rec. 36,417-18 (1978).

## III. The NSA's Telephony Metadata Program is Inconsistent with FISA

The NSA's telephony metadata program, conducted under 50 U.S.C. § 1861, contradicts FISA's purpose and design. To understand the language otherwise

production of any tangible things (including books, records, papers, documents, and other items)".[2] Uniting and Strengthening America by Providing Appropriate Tools

intelligence activities." USA PATRIOT Improvement

The government's interpretation of "relevant" contradicts Congress' aim in enacting FISA. As discussed above, Congress designed the statute to be used in of foreign intelligence gathering. By limiting the targets of electronic surveillance, requiring probable cause, disallowing investigations solely on the basis of otherwise protected first amendment activities, and insisting on minimization procedures, Congress sought to restrict agencies' ability to violate U.S. citizens' privacy. The business records provision built on this approach, adopting the that prevailed in other portions of the statute, and requiring that agencies obtain orders to collect information on individuals believed to be foreign powers or agents of a foreign power. Congress later deliberately inserted "relevant" into the statute to ensure the continued specificity of targeted investigations.

In addition, Congress empowered the FISC to consider each instance of placing an electronic wiretap. The NSA's program, in contrast, delegates such oversight to the executive, leaving all further inquiries of the databases to the agency involved. Once the NSA collects the telephony metadata, it is the NSA (and not the FISC) that decides which queries to use, and which individuals to target within the database. This change means that the FISC is not performing its most basic function: protecting U.S. persons from undue incursions into their privacy. Instead, it leaves the determination of whom to target to the agency's discretion.

## CONCLUSION

This Court should find the telephony metadata program unlawful and enjoin the government from continuing the program under the Verizon order or any successor thereto.

DATED: March 12, 2014

Respectfully submitted,

LAURA K. DONOHUE*
Professor of Law
Georgetown University
Law Center