14-42

IN THE
United States Court of Appeals
FOR THE
Second Circuit

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION,
Plaintiffs–Appellants,

– v. –

JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; CHARLES T. HAGEL, in his official capacity as Secretary of Defense; ERIC H. HOLDER, in his official capacity as Attorney General of the United States; and JAMES B. COMEY, in his official capacity as Director of the Federal Bureau of Investigation,
Defendants–Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF OF *AMICUS CURIAE*, FORMER MEMBERS OF THE CHURCH COMMITTEE AND LAW PROFESSORS IN SUPPORT OF PLAINTIFFS-APPELLANTS

LAURA K. DONOHUE*
Professor of Law
Georgetown University Law Center
600 New Jersey Ave., NW
Washington, DC 20001
(202) 662-9455
lkdonohue@
law.georgetown.edu
**Admitted pro hac vice*

ERWIN CHEMERINSKY*
Dean, Distinguished Professor of Law
University of California, Irvine
School of Law
401 E. Peltason Dr.
Suite 1000
Irvine, CA 92697
(949) 824-7722
echemerinsky@law.uci.edu

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **Page(s)**

STATUTES

OTHER AUTHORITIES

INTEREST OF *AMICUS CURIAE*

Amici write in support of Plaintiffs-Appellants to provide the Second Circuit with the historical context that gave rise to the Foreign Intelligence Surveillance Act.[1] They urge this Court to find that the telephony metadata collection program is unlawful and to enjoin the government from continuing the program under the Verizon order or any successor thereto.

The *Amicus Curiae* includes (a) former members of the 1975-76 Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities ("Church Committee"), and (b) law professors who teach and write about Legal History, Constitutional Law, National Security Law, Internet Law, and Privacy Law. *Amici* have a strong interest in ensuring that the executive branch acts in a manner consistent with the U.S. Constitution and the statutes governing foreign intelligence surveillance.

In the first category, *amicus* Gary Hart served as a U.S. Senator from Colorado 1975-1987, during which time he was a member of the Church Committee. He was a charter member of the Senate Intelligence Oversight Committee and a member of the Senate Armed Services Committee. From 1998 to 2001, he co-

[1] In August 2013 *Amici* submitted a similar brief to the Supreme Court in support of Petitioner in *In re Electronic Privacy Information Center*, No. 13-58 (2013) and to the Southern District of New York in support of Plaintiff in *Clapper v. ACLU*, 1:13-cv-3994. Neither party either authored or contributed funding to this brief. Consent for filing this brief has been requested and obtained from both Appellant/Petitioner and Appellee/Respondent.

chaired the U.S. Commission on National Security in the 21st Century. He chairs the Department of Defense's Threat Reduction Advisory Committee.

Amicus Walter Mondale, Vice President of the United States 1977-1981 and a U.S. Senator from Minnesota 1964-1976, served on the Church Committee and chaired the subcommittee that drafted the final report on domestic intelligence activities. Having helped to uncover the abuses in which the National Security Agency and others engaged, he subsequently helped to facilitate the writing and passage of the Foreign Intelligence Surveillance Act.

In the second category, *amicus* W. David Ball is an Assistant Professor at Santa Clara Law. He is on the Advisory Board of the Bill of Rights Defense Committee and Co-chair of the Corrections Committee of the American Bar Association's Criminal Justice Section, and he writes and teaches on Criminal Justice and Fourth Amendment Law.

Amicus William C. Banks, Board of Advisors Distinguished Professor and Professor of Law at Syracuse University College of Law, directs the Institute for National Security and Counterterrorism. He writes and teaches on Constitutional Law and National Security Law.

Amicus Annemarie Bridy is an Associate Professor at the University of Idaho College of Law, where she specializes in Internet Law and Intellectual Property Law. She is active in the leadership of the Association of American Law Schools Internet and Computer Law Section.

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

Amicus 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.

Amicus 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.

Amicus 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.

Amicus 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.

Amicus Laura K. Donohue is a Professor of Law at Georgetown University Law Center, as well as the Director of Georgetown's Center on National Security

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

Amicus 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.

Amicus 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.

Amicus 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.

Amicus 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.

Amicus Jennifer Stisa Granick is the Director of Civil Liberties at the

Stanford Center for Internet and Society. Her work focuses on computer crime and security, electronic surveillance, consumer privacy, data protection, copyright, trademark and the Digital Millennium Copyright Act.

Amicus Robert A. Heverly is an Associate Professor and Interim Director of the Government Law Center at Albany Law School of Union University, where he writes and teaches on Intellectual Property, Cyberlaw, and Communications Law.

Amicus Anne Klinefelter is the Director of the Law Library and an Associate Professor of Law at the University of North Carolina, where she writes and teaches on Privacy Law and First Amendment Law.

Amicus Edward Lee is a Professor of Law and the Director of the Program in Intellectual Property Law, as well as the Norman and Edna Freehling Scholar at IIT Chicago-Kent College of Law, where he writes and teaches on the First Amendment and Internet Law.

Amicus Mark A. Lemley is the William H. Neukom Professor at Stanford Law School, as well as the Director of the Stanford Program in Law, Science, and Technology, where he writes and teaches on Intellectual Property, Internet Law and Privacy Law.

Amicus David Levine is an Associate Professor of Law at Elon University School of Law, where he writes and teaches on Intellectual Property Law at the intersection of technology and public life. He is an affiliate scholar at the Center for Internet and Society at Stanford Law School.

Amicus 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.

Amicus 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.

Amicus 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.

Amicus 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.

Amicus Kim Lane Scheppele is Rockefeller Professor of International Affairs at the Woodrow Wilson School and the Director of the Program in Law and Public Affairs at Princeton University, where she writes about and teaches Comparative Constitutional Law. She has taught National Security Law at the University of Pennsylvania Law School, at the Yale Law School, and in the PhD program in National Security Studies at Princeton.

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

Amicus 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 *amicus* 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.

Amicus 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

sought to prevent a recurrence of the abuses of the 1960s and 1970s that accompanied the Cold War and the rapid expansion in communications technologies.

Congress circumscribed the NSA's authorities by limiting them to foreign intelligence operations. It added additional constraints, requiring that the target be a foreign power or an agent thereof, insisting that such claims be supported by probable cause, and heightening the protections afforded to U.S. citizens' information.

The government argues that *all* telephone calls in the United States, including those of a wholly local nature, are "relevant" to foreign intelligence investigations. This claim contradicts the purpose of the statute, which is to limit the conditions under which U.S. persons' information can be collected, analyzed, and distributed.

The Foreign Intelligence Surveillance Court plays a key role in determining the validity of each person targeted. Reading 50 U.S.C. § 1861 as authorizing the wholesale collection of all telephony data delegates such decisions to the executive, further rendering FISA's restrictions meaningless.

ARGUMENT

I. Congress Introduced the Foreign Intelligence Surveillance Act to Prevent Intelligence Agencies from Engaging in Broad Domestic Surveillance

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); *replaced and expanded by* 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. Kaiser, Cong. Research Serv., *Legislative History of the Senate Select Committee on Intelligence* 2 (Aug. 16, 1978); William Newby Raiford, Cong. Research Serv., 76-149F, *To Create a Senate Select Committee on Intelligence: A Legislative History of Senate Resolution 400* (Aug. 12, 1976).

The Senate Select Committee, Chaired by Senator Frank F. Church (D-ID), with the assistance of Senator John G. Tower (R-TX) as Vice Chairman, was a bipartisan initiative. Its membership included eleven Senators, six drawn from the majority party and five from the minority party. 1 *Intelligence Activities: Senate Resolution 21: Hearings Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States of the United States Senate*, 94th Cong., 1st Sess., at ii (1975). The Senate overwhelmingly supported the

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, *Rockefeller Commission Report*, 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_ room/2011/50000_declassified_docs.shtml.

The Committee found that broad domestic surveillance programs, conducted under the guise of foreign intelligence collection, had undermined U.S. citizens' privacy rights. *Intelligence Activities: Senate Resolution 21: Hearings Before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States of the United States Senate*, 94th Cong., 1st Sess.

(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, President Truman issued a classified memo that laid out the future of U.S. signals intelligence and created the NSA. Presidential Memorandum, Oct. 29, 1952, amending National Security Council Intelligence Directive No. 9, Mar. 10, 1950 (National Archives and Records Administration, RG 59, Records of the Department of State, Records of the Executive Secretariat, NSC Files: Lot 66 D 195). Truman's aim was to (a) strengthen U.S. signals intelligence capabilities, (b) support the country's ability to wage war, and (c) generate information central to the conduct of foreign affairs. 5 *Intelligence Activities: Senate Resolution 21: Hearings before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States of the United States Senate*, 94th Cong., 1st Sess. 9 (1975) (hereinafter *Church Committee Report, Vol. 5*).

The NSA's mission, accordingly, was to obtain foreign intelligence from foreign electrical communications. *Id.* at 6 (statement of General Lew Allen, Jr., Director, National Security Agency).

1. The NSA Understood Foreign Intelligence to Involve the Interception of Communications Wholly or Partly Outside the United States and Not Targeted at U.S. Persons

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*ee also Church Committee Report*, *Vol. 5, supra*, 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 of the Department of State, Records of the Executive Secretariat, NSC Files: Lot 66 D 195); s*ee also* NSCID No. 9, Mar. 10, 1950, *supra*.

"Foreign communications" thus turned upon the nature of the entity engaged in communications: i.e., a foreign power, or an individual acting on behalf of a foreign power.

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 *excluded* communications between U.S. citizens or entities. *Church Committee Report, Vol. 5*, *supra*, at 9. Accordingly, the NSA focused on communications *conducted wholly or partly outside the United States and not targeted at U.S. persons*.

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." *Id.* 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." *Id.*

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. *Church Committee Report, Vol. 5, supra*, 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. *Id.* at 10-11.

In 1969 the collection of information on individuals included in the watch list became known as Project MINARET. *Id.* 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

> based, my concern is whether that pressure could be resisted on the basis of the law or not . . . [W]hat we have to deal with is whether this incredibly powerful and impressive institution . . . could be used by President 'A' in the future to spy upon the American people. . . [W]e need to . . . very carefully define the law, spell it out so that it is clear what [the Director of the NSA's authority is and is not]. *Id.* at 36.

Senator Mondale then asked NSA Director General Lew Allen whether he would object to a new law clarifying that the NSA did *not* have the authority to collect domestic information on U.S. citizens. Allen indicated that he did not object. *Id.* at 36.

Project MINARET, which represented the type of surveillance program that FISA was designed to forestall, was not nearly as extensive as the telephony metadata program at issue in this case. Over the course of Project MINARET, for instance, the watch list expanded to include approximately 1,650 U.S. citizens in total. *Id.* at 12. At no time were there more than 800 U.S. citizens' names on the list, out of a population of about 200 million Americans. *Id.* at 30, 33-34.

Today, in contrast, there are approximately 316 million Americans, United States Census Bureau, U.S. and World Population Clock (Aug. 28, 2013), http://www.census.gov/popclock/, most of whom would have been subject to the Verizon (and similar) orders issued by the Foreign Intelligence Surveillance Court ("FISC"). This number eclipses the total number of U.S. citizens subject to one of the most egregious programs previously operated by the NSA, which gave rise to FISA in the first place.

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. Testimony of General Lew Allen, Director, National Security Agency, *Church Committee Report, Vol. 5, supra*, at 36.

In contrast, the Order issued in April 2013 by FISC *requires* the collection of information "wholly within the United States, including local telephone calls." *In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc., on Behalf of MCI Communication Services, Inc., D/B/A Verizon Business Services*, Secondary Order, No. BR 13-80 (FISA Ct. Apr. 25, 2013).

3. The NSA's Operation SHAMROCK Involved the Large-scale Collection of U.S. Citizens' Communications from Private Companies

During the Senate hearings, much concern was expressed about whether to make public a second, highly classified, large-scale surveillance program run by the NSA. *Church Committee Report, Vol. 5*, *supra*, at 48-57, 60-61, 63. The committee decided to discuss the program in open session because it was illegal and violated the Fourth Amendment. *Id.* at 57 (statement of Senator Frank Church, Chairman, Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States of the United States Senate).

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. *Id.* 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. *Id.* 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. *Id.*

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. *Id.* at 58-59. It selected approximately 150,000 messages per month for further analysis, distributing some messages to other agencies. *Id.* 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." *Id.* at 65. Senator Church explained:

> In the case of the NSA, which is of particular concern to us today, the rapid development of technology in the area of electronic surveillance has seriously

> 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. *Id.*

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. *Id.*

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. *Id.* 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. *Id.* at 71-72. The Founders' objection to such instruments was simple: were the government to be granted the authority to break into and to search individuals' homes without cause, the private affairs of every person would be subject to inspection. *Id.* at 72.

In contrast, Levi argued, the exercise of electronic wiretaps for foreign intelligence gathering fell subject to Attorney General review. Nevertheless, he recognized the need for new laws to address the ambiguity that attended the use of modern technologies. The Senators agreed. *See, e.g., id.* at 64-65, 84, 125.

B. Other Intelligence Agencies Similarly Engaged in Sweeping Data Collection Programs

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 of these programs, such as the FBI's COINTELPRO and the CIA's Operation CHAOS, were uncovered by the exhaustive investigations of Senate Select Committee. *See, e.g.,* 6 *Intelligence Activities: Senate Resolution 21: Hearings Before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States of the United States Senate*, 94th Cong., 1st Sess. (1975).

The Church Committee was not the only forum in which such programs were addressed. In 1975 President Ford issued an executive order establishing the President's Commission on CIA Activities Within the United States ("Rockefeller Commission"). Executive Order No. 11,828, 3 C.F.R. 933 (1975). Ford appointed Vice President Nelson Rockefeller as Chair. *Commission on CIA Activities Within the United States: Announcement of Appointment of Chairman and Members*, 11 Weekly Comp. Pres. Doc. 25 (Jan. 5, 1975).

The public charges to which the Rockefeller Commission responded included large-scale domestic surveillance of U.S. citizens; retaining dossiers on U.S. citizens; and aiming such collection efforts at individuals who disagreed with government policies. *Report to the President by the Commission on CIA Activities Within the United States* 9 (June 1975). The Commission's aim was further supplemented by allegations that for the past twenty years the CIA had (a) intercepted and opened

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. *Id.*

Like the Senate Select Committee, a key question confronting the Rockefeller Commission was how to define the term "foreign intelligence"—a crucial step in protecting Americans' right to privacy. Accordingly, in its first recommendation, the Rockefeller Commission advised that Section 403 of the 1947 National Security Act be amended to make it explicit that the CIA's activities solely related to "foreign intelligence." *Id.* at 12. Any involvement of U.S. citizens could only be *incidental* to foreign intelligence collection. *Id.*

The Commission reinforced the strict separation between foreign targets and U.S. persons through its second recommendation: that the President, via Executive Order, "prohibit the CIA from the collection of information about the domestic activities of United States citizens (whether by overt or covert means), the evaluation, correlation, and dissemination of analyses or reports about such activities, and the storage of such information." *Id.* at 15.

The revelation of these programs undermined citizens' confidence in the intelligence agencies. 124 Cong. Rec. 36,415 (1978). An important question facing Congress was how to rebuild confidence in the system, and how to empower the intelligence agencies to conduct electronic surveillance, while protecting the privacy rights of U.S. citizens.

In 1972 the Supreme Court had held that the electronic surveillance of domestic groups, even where security issues might be involved, required that the government first obtain a warrant. The "inherent vagueness of the domestic security concept", and the significant possibility that it be abused to quash political dissent, underscored the importance of the Fourth Amendment—particularly when the government was engaged in spying on its own citizens. *United States v. U.S. District Court*, 407 U.S. 297 (1972).

Justice Powell, writing for the Court, emphasized the limits on the scope of the decision: "[T]his case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents." *Id.* at 321-322. Different standards and procedures might apply to domestic security surveillance than those required by Title III of the Omnibus Crime Control and Safe Streets Act of 1968. *Id.* at 322. The Court issued an invitation to Congress to pass new laws covering such cases. *Id.* at 323.

C. Congress Passed the Foreign Intelligence Surveillance Act to Prevent Agencies from Using Foreign Intelligence Gathering as an Excuse for Domestic Surveillance

The Foreign Intelligence Surveillance Act of 1976 became the first bill introduced into Congress, supported by the President and Attorney General, that would require judicial warrants in foreign intelligence cases. 124 Cong. Rec. 35,389 (1978); *see also* Foreign Intelligence Surveillance Act of 1976, S. 3197, 94th Cong

(1976). Its successor bill, S.1566, became the Foreign Intelligence Surveillance Act of 1978. 124 Cong. Rec. 35,389 (1978); *see also* Foreign Intelligence Surveillance Act of 1978, S. 1566, 95th Cong (1978).

From the beginning, Congressional members made it clear that the legislation was designed to prevent the types of broad surveillance programs and incursions into privacy represented by Project MINARET, Operation SHAMROCK, COINTELPRO, Operation CHAOS, and other intelligence-gathering initiatives that had come to light.

During consideration of the Conference Report on S. 1566, for instance, Senator Ted Kennedy (D-MA) noted, "The abuses of recent history sanctioned in the name of national security highlighted the need for this legislation." 124 Cong. Rec. 34,845 (1978). The debate represented the "final chapter in the ongoing 10-year debate to regulate foreign intelligence electronic surveillance." *Id.* With the passage of FISA, the Senate would "at long last place foreign intelligence electronic surveillance under the rule of law." *Id.* Senator Birch Bayh, Jr. (D-IN) echoed Kennedy's sentiments, "This bill, for the first time in history, protects the rights of individuals from government activities in the foreign intelligence area." *Id.* Senator Charles Mathais (R-MD) noted that enactment of the legislation would be a milestone, ensuring "that electronic surveillance in foreign intelligence cases will be conducted in conformity with the principles set forth in the fourth amendment." 124 Cong. Rec. 35,389 (1978) (statement of Senator Mathais).

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

Congress purposefully circumscribed the NSA's authorities by adopting four key protections.

First, Congress required that the target of surveillance be a foreign power or an agent of a foreign power. The Senate initially defined "foreign power", with regard to terrorist groups, to mean a foreign-based entity. The House amendments, in contrast, understood "foreign power" to include groups engaged in international terrorism or activities in preparation therefor. The Conference adopted the House definition, with the idea that limiting such surveillance solely to foreign-based groups would be unnecessarily burdensome. 124 Cong. Rec. 33,782 (1978); *see also* 50 U.S.C. § 1801. In both Houses, underlying the definition of "foreign power" was the understanding that information would be collected specifically in regard to single individuals or entities tied to foreign powers. 124 Cong. Rec. 33,782 (1978). Congress directed that intelligence agencies *first* identify the target in order to justify the resulting incursion into privacy. The data mining telephony program, in contrast, goes about the process in precisely the opposite direction: it uses information obtained through the collection of vast amounts of information to identify potential targets of foreign intelligence interest.

Second, in response to concerns evinced in the Senate with regard to determining whether the (specific) target was a foreign power or an agent thereof, the final bill adopted a standard used in a criminal law: probable cause. 50 U.S.C. §

1805(a)(2). The agency requesting surveillance would have to demonstrate, with some particularity, that the entity to be placed under surveillance was a foreign power or an agent thereof, and that the target was likely to use the facilities to be monitored.

Third, the statute limited the breadth of surveillance operations by requiring that probable cause could not be established solely on the basis of otherwise protected first amendment activity. *Id.*

Fourth, Congress insisted on minimization procedures to protect activity not related to foreign intelligence from government scrutiny. 50 U.S.C. § 1804(a)(4). The legislature insisted on minimizing not just the analysis of the information, but its "*acquisition* and *retention*." 50 U.S.C. § 1804(h) (emphasis added). The NSA's telephony metadata program, in contrast, makes no effort to limit the acquisition or retention of the information in question. It insists that *all* telephone calls, including those entirely local in nature, be included in the data turned over to the government.

A key principle throughout the debates was the importance of heightened protections where U.S. persons' information may be involved. The conference was deadlocked on this point until the Senate receded and accepted the House language exempting certain particularly sensitive surveillance (i.e., relating solely to foreign powers) from judicial review, on the grounds that (1) such surveillance did not involve U.S. persons; and (2) having removed the most sensitive information from

external review, the Foreign Intelligence Surveillance Court could be given a greater role in protecting the rights of each U.S. person targeted by the government. 124 Cong. Rec. 36,409 (1978).

FISA represents the culmination of a multi-branch, multi-year, cross-party initiative directed at bringing the collection of foreign intelligence within a narrowly circumscribed, legal framework. In 1972 the Senate Committee on the Judiciary's Subcommittee on Administrative Practice and Procedure held extensive hearings on the subject of warrantless wiretapping. 122 Cong. Rec. 7,543 (1976). In 1975 the subcommittee issued a report jointly with a special subcommittee of the Foreign Relations Committee, calling for Congress to introduce legislation governing foreign intelligence collection. *Id.* In 1976 President Ford and Attorney General Levi introduced the first foreign intelligence bill. Foreign Intelligence Surveillance Act of 1976, H.R. 12750, 94th Cong. (introduced in the House, Mar. 23, 1976). President Carter and Attorney General Bell subsequently supported S. 1566, which became FISA. 124 Cong. Rec. 36,409 (1978). Congress consulted the NSA, FBI, CIA, and representatives of interested citizen groups, gaining broad support for the measure. 124 Cong. Rec. 37,738 (1978); 124 Cong. Rec. 36,414 (1978).

Resultantly, the measure passed by significant majorities. S. 1566 passed the Senate 95 to 1. *Id.* H.R. 7308 passed the House 246 to 128. *Id.* In October 1978 the Senate adopted the Conference Report "by an overwhelming voice vote, with no

dissenting voice vote." *Id.* 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 would be to vitiate the statute in terms of the restrictions placed on the intelligence agencies and the responsibilities assigned to the Foreign Intelligence Surveillance Court.

In 1998 Congress amended FISA to authorize the production of certain kinds of business records of those suspected of being foreign powers or agents of a foreign power: documents kept by common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, § 602, 112 Stat. 2396, 2410 (1998).

Congress assigned the terms "foreign power", "agent of a foreign power, "foreign intelligence information", and "international terrorism" *the same meaning* as employed in relation to electronic surveillance. *Id.* Congress required that intelligence agencies follow the same steps as those taken with regard to electronic surveillance: i.e., to submit an application to FISC to obtain an order, which then compels the companies to hand over the records. *Id.*

In 2001 Congress expanded the types of records that could be obtained, authorizing intelligence agencies to apply for an order from FISC "requiring the

production of any tangible things (including books, records, papers, documents, and other items)".[2] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT Act") Act of 2001, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861). Congress eliminated any restriction on the types of businesses or entities on which such an order could be served. *Id.* It retained, however, the general contours of FISA, specifying that such items be obtained in the course of "an investigation to protect against international terrorism or clandestine intelligence activities." *Id.* Congress required that such investigation, where directed towards a U.S. person, not be "conducted solely upon the basis of activities protected by the first amendment to the Constitution." *Id.*

Section 215 of the USA PATRIOT Act (codified at 50 U.S.C. § 1861) was set to expire December 31, 2005. *Id.* Congress has since renewed it seven times. An Act to Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of that

[2] Congress also amended FISA to require that applicants to FISC certify that "a significant purpose" of the surveillance be to obtain foreign intelligence. 50 U.S.C. § 1804(a)(7)(B). This shift, from the prior language that "the" purpose be to obtain foreign intelligence, had the effect of removing a wall that had built up within the Department of Justice between intelligence officers and criminal prosecutors. The government argued that the latter should be allowed to advise the former concerning the initiation, operation, continuation, or expansion of FISA searches or surveillance. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 623 (FISA Ct. 2002). The Foreign Intelligence Surveillance Court of Review upheld the change. *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002). This alteration recognizes parallels between criminal violations and national security threats. It does not shift the focus of the statute to allow intelligence agencies to collect information on millions of Americans not suspected of any wrongdoing.

Act and the Lone Wolf Provision of the Intelligence Reform and Terrorism Prevention Act of 2004 to July 1, 2006, Pub. L. No. 109-160, 119 Stat. 2957 (2005) (extension until Feb. 3, 2006); An Act To Amend the USA PATRIOT Act to Extend the Sunset of Certain Provisions of Such Act, Pub. L. No. 109-170, 120 Stat. 3 (2006) (extension until Mar. 10, 2006); USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006) (extension until Dec. 31, 2009); Department of Defense Appropriations Act, 2010, Pub. L. No. 111-118, 123 Stat. 3409 (2009) (allowing for a short-term, 60-day extension of 50 U.S.C. 1861 until February 28, 2010); An Act to Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011, Pub. L. No. 111-141, 124 Stat. 37 (2010) (extension until Feb. 28, 2011); FISA Sunsets Extension Act of 2011, Pub. L. No. 112-3, 125 Stat. 5 (2011) (extension until May 27, 2011); PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011) (extension until June 1, 2015).

In 2005, in the course of extending the tangible goods provision, Congress added language tying the section more closely to FISA's overarching structure. It required applicants to submit a statement of facts, establishing "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine

intelligence activities." USA PATRIOT Improvement and Reauthorization Act of 2005 § 106, 120 Stat. at 196 (codified as amended at 50 U.S.C. § 1861). Congress required in addition "an enumeration of the minimization procedures" related to the retention and dissemination of any tangible things obtained under 50 U.S.C. § 1861. *Id.*

The government argues that the NSA's telephony metadata program is consistent with the language of 50 U.S.C. § 1861 in that *all* telephone calls in the United States, including those of a wholly local nature, are "relevant" to foreign intelligence investigations.

This interpretation contradicts Congress' intent in introducing § 215. At the introduction of the measure Senator Arlen Specter explained that the purpose of the language was to create an incentive for the government to use the authority only when it could demonstrate a connection to a *particular* suspected terrorist or spy. 151 Cong. Rec., 13,441 (2005). During a House Judiciary Committee meeting on July 17, 2013, Representative James Sensenbrenner (R-WI), reiterated that the reason Congress inserted "relevant" into the statute was to ensure that only information *directly related* to national security probes would be included—not to authorize the ongoing collection of all phone calls placed and received by millions of Americans not suspected of any wrongdoing. *Oversight of the Administration's Use of FISA Authorities: Hearing Before H. Comm. on the Judiciary*, 113th Cong. (2013). Members of the Committee made similar claims. *Id.*

The government's interpretation of "relevant" contradicts Congress' aim in enacting FISA. As discussed above, Congress designed the statute to be used in *specific cases* 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 *same definitions* 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
600 New Jersey Ave., NW
Washington, DC 20001
(202) 662-9455
lkdonohue@
law.georgetown.edu

ERWIN CHEMERINSKY*
Dean, Distinguished Professor of Law
Raymond Pryke Professor of First Amendment Law
University of California, Irvine School of Law
401 E. Peltason Dr.
Suite 1000
Irvine, CA 92697
(949) 824-7722
echemerinsky@law.uci.edu

**Admitted pro hac vice*

On behalf of Amicus Curiae
Former Members of the Church Committee and Law Professors