The Curious and Questionable History of FISA

FROM RICHARD NIXON AND GEORGE W. BUSH TO EDWARD SNOWDEN

WYLIE STECKLOW

Our founding Fathers birthed this nation as an act of dissent, in part, due to their belief that the British monarchy would continue its violations of an individual's inalienable right to be free to pursue life, liberty, and happiness. For the first 250 years of our history, our political systems checked and successfully balanced the need for security with the basic Fourth Amendment guarantees of freedom from unlawful searches. The advent of technology, excessive—and often unauthorized—use of clandestine activities by the executive branch,[1] and, more recently, the political response to the rise in global and domestic terrorism sacrificed privacy for the facade of security.

Congress acted in 1978, passing the Foreign Intelligence Service Act (FISA) and creating a court, designed to operate in secret proceedings, to oversee surveillance warrants. The FISA Court continued to operate in secret,[2] unhindered by checks and balances, leading to the massive bulk data spying program that was initially denied until disclosed by Edward Snowden in 2013.

Following the controversial Snowden disclosures, leaders with diverse backgrounds and ideologies urged Congress to make changes to the FISA Court. Congress acted, and in the late days of 2015 changes to the FISA process became effective, removing the broad language of § 215 of the PATRIOT Act (discussed below) and creating independent advocates to represent the citizenry in the FISA Court. But how did this spying program continue in secret and unchecked for all these years? Are the changes enacted by Congress sufficient to balance the needs of protecting us from terrorism and safeguarding our privacy?

The FISA Court Is a Nixon Legacy

FISA was born in the aftermath of unlawful behavior of the executive branch of government.[3] President Richard Nixon did not restrict his spying to Watergate and one specific opposition candidate.[4] Following Nixon's resignation, Senate investigations uncovered unconstitutional domestic intelligence activities that violated the Fourth Amendment,[5] authorized by Nixon against political and activist groups.

In response, Congress passed FISA, which established both judicial oversight (the FISA Court)[6] and a process for the government to obtain surveillance warrants for covert intelligence gathering within the United States for the purpose of collecting foreign intelligence and/or foreign counterintelligence.[7] The FISA Court consists of 11 Article III district judges (increased from seven by the PATRIOT Act), each unilaterally appointed by the Chief Justice of the Supreme Court.[8] Due to national security concerns, this court and its proceedings were closed to the public, held ex parte, and were nonadversarial.[9] The court heard evidence presented solely by those seeking the surveillance warrants, though there have been amicus submissions in specific instances.[10] Since the establishment of the FISA Court, various statutory amendments have expanded FISA's scope while loosening its oversight, culminating in the passage of the USA PATRI-

OT Act in the immediate aftermath of 9/11. Since fall 2001, efforts by congressional leaders, constitutional litigation by the American Civil Liberties Union (ACLU) and Electronic Freedom Foundation (EFF), among others, as well as the very public disclosure by Edward Snowden, have challenged the functionality and constitutionality of the FISA Court and its regular operations.

FISA Critics

The FISA Court has many critics, ranging from the Electronic Privacy Information Center to HBO's John Oliver.[11] Citing the court's non-adversarial nature and statistical approval of 99.7 percent of warrant requests,[12] critics call the FISA Court a rubber stamp. Proponents of the court indicate that many requests are withdrawn and modified, so the high warrant approval rate is misleading. Yet, during the 25 years from 1979 to 2013, more than 35,000 requests were submitted, and just 533 of these were modified before being authorized.[13]

Advocates in ex parte proceedings, including those who appear in the FISA Court, are under the obligation of heightened candor.[14] Critics of the FISA Court cite the ex parte nature of the court's proceedings as a contributing factor for the court's failings. FISA Court Judge James Robertson agreed with this assessment, stating that an informed court needs to hear both sides of an argument, especially when the warrantless surveillance program is involved.[15] The government proved that human fallibility must be considered in the FISA process in September 2000, when it self-reported violations of the obligation of heightened candor in at least 75 different warrant applications presented to the FISA Court.[16] Yet, despite these many criticisms and dissents, after the attacks of 9/11, the failings of the FISA Court process were disregarded by Congress.

FISA Role Greatly Expands After 9/11

Section 215 of the PATRIOT Act expanded the FISA Court's authority by (1) eliminating any restriction on the type of business that could be the subject of a warrant from solely hotels, motels, or car/truck rental agencies to any business and (2) broadening the authority as to the type of business record that could be seized. Previously, records could only be seized if the government could provide "specific articulable facts giving reason to believe" that the subject of an investigation was a "foreign power or the agent of a foreign power."[17] Section 215 expanded the scope from records to any tangible thing and lowered the burden of proof so that the government only needs to submit that the records were being sought in relation to a foreign intelligence investigation or to protect against international terrorism or clandestine intelligence activities.[18]

An Ignoble Legacy Lives On: From Richard Nixon to the Bush White House

Even with the § 215 expansion of warrant authority, Nixon's unconstitutional conduct that begot the FISA Court was repeated in the Bush White House in the aftermath of 9/11. The President's Surveillance Program (PSP) secretly authorized the National Security Agency (NSA) to monitor—without search warrants—phone calls, Internet activity, text messages, and other communications involving any party believed by the NSA to be outside the United States, even if the other end of communication was within the United States.[19] The program, called Stellarwind, was not disclosed to the FISA Court or the American public.[20] Even the Bush legal team questioned its legality, which led to a bizarre hospital bedside confrontation between two members of the White House staff: Acting U.S. Attorney General James Comey and U.S. Attorney General John Ashcroft, who was at the time in the intensive care unit of a Washington, D.C., hospital.[21]

In 2005, *The New York Times* reported on Stellarwind,[22] and Vice President Dick Cheney responded, "It's good, solid, sound policy. … It's the right thing to do."[23] Judge Harold A. Baker, a former FISA Court judge disagreed: "The president was bound by the law 'like everyone else.' If a law like the Foreign Intelligence Surveillance Act is duly enacted by Congress and considered constitutional, the president ignores it at the president's peril."[24] In December 2005, Judge James Robertson resigned from the FISA Court in protest because the Bush administration's Stellarwind program was bypassing the court on warrantless wiretaps.[25] Numerous representatives on both sides of the aisle expressed concern about the scope and legality of the Bush Presidential Surveillance Program seeking congressional review, including Sens. Chuck Hagel, R-Neb.; Olympia Snowe, R-Maine; Arlen Specter, R-Penn.; Dianne Feinstein, D-Calif.; Carl Levin, D-Mich.; and Ron Wyden, D-Ore., all of whom were members of the Senate Intelligence Committee.[26]

In 2007, public outcry and pressure from Congress arising due to the public disclosure of the Stellarwind program forced the Bush Administration to end the NSA warrantless surveillance program and return oversight to the FISA Court. Yet, similar to its response to the self-reported violations of heightened candor in the FISA Court in 2000, in the aftermath of the improper surveillance conduct secretly authorized by the Bush White House, Congress again failed to tighten the checks and balances of privacy and security. Instead, the FISA Amendments Act of 2008 loosened the FISA Court oversight and expanded the availability of the government's warrant powers. This 2008 Act authorized warrantless electronic surveillance for up to one-year periods if the target was a foreigner living abroad, if requested jointly by the Director of National Intelligence and the Attorney General. The Act also increased—from 48 hours to seven days—the length of time Americans living abroad could be surveilled without a FISA Court warrant.[27]

As the Bush Administration entered its twilight, a presidential hopeful weighed in on the need to balance privacy and security:

> I will provide our intelligence and law enforcement agencies with the tools they need to track and take out the terrorists without undermining our Constitution and our freedom. That means no more illegal wiretapping of American citizens. No more national security letters to spy on citizens who are not suspected of a crime. No more tracking citizens who do nothing more than protest a misguided war. No more ignoring the law when it is inconvenient.

Sen. Barack Obama made these statements in 2007, adding that "the FISA court works."[28]Once he became president, Obama weighed in again on the FISA Court, promising to declassify a significant FISA Court ruling relating to 9/11.[29] In a public speech, he indicated that he agreed the country "needed a more robust public discussion" about "the balance between security and liberty."[30]

Meanwhile, a self-taught computer cybersecurity expert named Edward Snowden ascended the heights of covert cyberactivity within the CIA, obtaining the significant security clearance required of those working for outside contractors. In 2012, while working for Dell and assigned as a contractor to U.S. National Security Agency

facilities in the United States and Japan,[31] Snowden became alarmed at the secretive nature of the massive domestic spying program and its unconstitutional nature. He began to download documents concerning the existence of the program onto his thumb drive.[32] In 2013, while with U.S. military contractor Booz Allen Hamilton, he continued to download thousands of documents affirming the existence and breadth of this program.[33]

Snowden's Tipping Point: Lying to the American Public in the Sacred Halls of Congress

Annually, the Senate Intelligence Committee holds open public briefings on worldwide threats to inform the public on issues of global security and how our government is handling these concerns. It is a crime to lie before Congress, punishable by censure, criminal conviction, and in some cases even jail time. Recently, former Major League Baseball pitcher Roger Clemens was indicted and tried for perjury in his testimony before Congress.[34] On March 12, 2013, the heads of the various intelligence agencies, including Director of National Intelligence James Clapper, CIA Director John Brennan, National Counterterrorism Center Director Matthew Olsen, FBI Director Robert Mueller, Director of the Defense Intelligence Agency Lt. Gen. Michael T. Flynn, and Assistant Secretary of State for Intelligence and Research Philip Goldberg appeared before the Senate Intelligence Committee. Toward the end of the public session, after a contentious back-and-forth, Sen. Ron Wyden, D-Ore., asked Clapper: "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?" Clapper replied, " No sir. Not wittingly. There are cases where they could inadvertently perhaps collect, but not wittingly." [35]

For Edward Snowden, this public denial was the tipping point. Two months later, the former NSA consultant disclosed, via *The New York Times* and *The Guardian*, the existence of the mass surveillance program that had been approved by the FISA Court. In discussing the rationale for the timing of the disclosure, Snowden credited Clapper's false testimony before the Senate Intelligence Committee: "Sort of the breaking point was seeing the director of National Intelligence, James Clapper, directly lie under oath to Congress. … Seeing that really meant for me there was no going back."[36] The Snowden disclosures, in addition to proving the very existence of this mass domestic data surveillance program, also identified that the head of National Intelligence had lied to the Senate Intelligence Committee and the American public. From Rep. Justin Amash, R-Mich.,[37] to Sen. Rand Paul, R-Ky.,[38] to the author of the PATRIOT Act, Rep. Jim Sensenbrenner, R-Wis.,—who also urged Clapper's prosecution for perjury[39]—to numerous journalists,[40] multiple demands have been made to hold Clapper accountable for lying to Congress and the American people. Yet, none of these calls for justice have resulted in any charge or investigation, and Clapper continues to serve as director of National Intelligence, never being held accountable for lying to the Senate Intelligence Committee and the U.S. citizenry.

Lawyers to the Rescue! The ACLU Sues James Clapper

The Snowden disclosures confirmed the existence of this massive domestic data surveillance program, and civil rights lawyers with the ACLU filed suit, challenging the constitutionality of § 215 of the PATRIOT Act in federal court.[41] On Dec. 27, 2013, Judge William H. Pauley of the Southern District of New York issued a 53-page opinion ruling the NSA's bulk telephony metadata collection program to be lawful and thereby granting the government's motion to dismiss the complaint and denying the ACLU's request for a preliminary injunction. The ACLU immediately appealed this decision. While the appeal was pending, Obama consulted with the Privacy and Civil Liberties Oversight Board and created an outside review group on intelligence and communications technologies to make recommendations for reform.[42]In January 2014, the Privacy and Civil Liberties Oversight Board issued a report on the telephone records program conducted under § 215 of the PATRIOT Act. The report found the program unlawful and provided suggestions for FISA reform.[43] That same month, President Obama addressed the country, stating that he had declassified more than 40 FISA opinions and orders, and "[t]o ensure that the [FISA] Court hears a broader range of privacy perspectives, [President Obama was] also calling on Congress to authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court."[44]Six months later, a three-person Second Circuit panel that included Judges Gerard E. Lynch, Robert D. Sack, and Vernon S. Broderick unanimously reversed the decision on the ACLU appeal, ruling that § 215 of the PATRIOT Act and the statutory scheme to which it relates did not preclude judicial review and that the bulk telephone metadata program was unlawful and not authorized by § 215.[45]

Congress Seeks a Balance Between Security and Privacy

Congress swiftly took action, passing the USA Freedom Act that provided a 180-day sunset provision before eliminating § 215 of the PATRIOT Act. The Freedom Act required the FISA Court to appoint a panel of independent constitutional advocates to appear as amicus curiae on specific cases. The law set a discretionary standard for when the court should seek advocacy from this panel.[46] This was a much-needed correction, as former FISA Court Judge Robertson had previously noted that the FISA Court should hear both sides of a case before deciding, especially when it comes to the massive surveillance warrants authorized by the 2008 FISA amendment.[47]In the first decision to be issued by the FISA Court after the passage of this new law, the court indicated that the case was the type that the new law suggested an amicus curiae be appointed.[48] However, that FISA judge opted not to seek amicus help and added to the debate about whether these amicus advocates should be discretionary or mandatory. Still, the very next published FISA decision saw the appointment of an amicus.[49] The government was taking the position, in a class action brought by the Electronic Freedom Foundation, that the government could not separate out the records required to defend this litigation from the rest of the telephone metadata that was to be destroyed in the time specified by the Freedom Act. The appointed amicus picked apart the government's arguments and urged the FISA Court to reject the government's position and force it to allocate the time and money to separate out the class-action records from the remaining documents that should then be destroyed.[50] On Dec. 2, 2015, five amici curiae advocates were appointed to the FISA Court: Jonathan G. Cedarbaum, John D. Cline, Laura Donohue, Amy Jeffress, and Marc Zwillinger. The ACLU and EFF described these advocates as "impressive."[51]

The Uncertain Future of the FISA Court

Numerous recommendations have been made, including a call for the complete disbandment of this court by Chelsea Manning in *The*

Guardian.[52] Yet, while there is a clear need for vigilant security in today's world, there is an equally clear need to recognize the tension between privacy and First and Fourth amendment rights with these security concerns. Most of the following recommendations fall within one of three categories—privacy, transparency, and functionality—and this section concludes with a recommendation concerning oversight of this secret court and its proceedings. These recommendations are not based on the personal opinions of the author, but were compiled from many sources, including the Brennan Center Report,[53] the Privacy and Civil Liberties Oversight Board,[54] and the President's Review Group on Intelligence and Communications Technologies.[55]

Privacy

Restrict access to the metadata database by requiring a prerequisite standard to be identified, met, and reviewed by the FISA Court before access is granted. The NSA claims to already utilize a standard of reasonable articulable suspicion before a search of the metadata is allowed.[56] Each request approved by the NSA based on a reasonable articulable suspicion should be submitted to the FISA Court for approval. All companies served with subpoenas for mass data collection of their customers should be granted a limited ability to disclose the existence of the subpoena and (in some fashion) the data being sought/disclosed. The standard to be used on disclosure was set down by the President's Review Group: A program of this magnitude should be kept secret from the American people only if (1) the program serves a compelling governmental interest and (2) the efficacy of the program would be substantially impaired if our enemies were to know of its existence.[57]

Functionality

Reduce the number of hops allowed under the surveillance from three to two.[58] Create an easier path for FISA decisions to be reviewed by the FISA Court of Review. Urge FISA judges to seek more assistance in technical areas to understand and accept or reject technical positions taken in surveillance requests. Perhaps appointing a panel of technical experts similar to the constitutional advocates appointed would help FISA judges understand some of the technicalities of the private data being surveilled. Constitutional advocates should continue to be appointed for specific terms, and they should report on how often they are utilized and analyze whether the appointment by request is working. Change the appointment process of FISA Court judges. It cannot be fair representation of our country's diverse citizenry, culture, and values if one individual (Chief Justice of Supreme Court) is the sole and exclusive appointer of each FISA Court judge. The appointment should move from an individual to a group, such as each Supreme Court justice or each chief judge of the circuit courts or the constitutional advocates, or any of the other myriad suggestions. But leaving it this way means that in the last 40 years, only Republican-appointed justices have chosen FISA judges.[59] This in no way should be taken as any type of slight against the current Chief Justice but should be viewed in a forward-thinking manner.

Transparency

Review all prior FISA decisions to determine whether they can be edited and redacted to allow for publication without substantially impairing the program. Publishing more decisions creates more transparency and lifts the veil from this secret court, which is the cornerstone of democratic governance. Create a standard for all new FISA decisions that will allow for publication of more FISA court decisions. Judges should write decisions in a manner that can be easily published with small redactions. To evaluate the success of the constitutional advocate program, data should be collected and disclosed on the number of requests made for advocates, how often advocates file briefs and participate in the FISA proceedings, and other relevant issues that will foster more trust by the citizenry

Oversight

The Privacy and Civil Liberties Oversight Board is an independent, bipartisan agency within the executive branch created by the 9/11 Commission Act of 2007.[60] This organization can be utilized as the auditing and oversight group for the continuing massive data collection operation. It can be tasked with overseeing intelligence activities for foreign intelligence purposes (versus counterterrorism purposes only). It can be an authorized agency to receive whistleblower complaints related to civil liberty issues arising from intelligence community activities. History has proven the absolute need for such independent oversight.

While Clapper Lives on American Salary, Snowden Suffers in Exile

On June 14, 2013, the Department of Justice revealed espionage charges against Snowden.[61] The multiple demands for Snowden to receive clemency and come home, including a petition that had 167,000 signators on Whitehouse.gov,[62] have not been successful.[63] Prior to being elected to office, President Obama was Professor Obama teaching constitutional law at University of Chicago Law School. One can only *hope* that in the twilight of his presidency, he can hark back to his days of professorship and recognize that the healthy public debate surrounding the NSA massive data collection would not exist but for Edward Snowden heeding the words of Supreme Court Justice Louis D. Brandeis[64] and shedding sunlight on this unlawful spying program (whose very existence was denied just months earlier). Clapper continues to live free and on a large government salary as director of this nation's National Intelligence, while Snowden lives in exile. An open and free country should not be punishing a young man for providing information—that should have been public—to journalists who responsibly published this information. Even if Clapper gets away with deceiving our country, let's not also punish Snowden for bringing these deceptions to our attention. President Obama, bring him home. Grant Edward Snowden clemency. ⊙

Wylie Stecklow is a partner in Stecklow & Thompson, a downtown NYC civil rights litigation boutique firm. He is the FBA's national Civil Rights Law Section chair-elect and the SDNY Chapter vice president. He is a founding member of the National Action Network's Legal Rights Nights, a recipient of U.S. Congress Special Recognition for Community Service, NYC Council Certificate for Outstanding Citizenship, and Manhattan Borough President's Certificate of Recognition for Community Service. In 2004, he served in top hat and tails as General Counsel for Billionaires for Bush. In 2008, he represented more than 180 individuals arrested during the Sean Bell day of action. In 2011, his firm, retained by the Occupy Wall Street General Assembly, organized pro bono *representation for over 200 Occupy arrestees.*

Endnotes

[1]*See United States v. Ehrlichman*, 546 F.2d 910, 914 (D.C. Cir. 1976) (describing history of "the Special Investigations" or "Room 16" unit within the Nixon White House and some of the burglaries and other "covert operations" the unit performed), *See, e.g., Ellsberg v. Mitchell*, 709 F.2d 51, 53-55 (D.C. Cir. 1983) (noting that the defendants, members of the Nixon Administration, admitted to wiretapping "one of plaintiffs' attorneys or consultants" on direct orders of the President), James Risen and Eric Lichtblau,"Bush Lets US Spy on Callers Without Courts," The New York Times (Dec. 16, 2005), *available at* www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html

[2]*See United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 310 (D. Conn. 2008) ("Courts have uniformly held that ex parte and in camera inspections are the 'rule' under FISA, and that disclosures and adversary hearings are the 'exception, occurring only when necessary.'") (quoting *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. N.Y. 1984) and collecting cases). *See also* 50 U.S.C. §§ 1802(b), 1805(a) (authorizing FISA Court proceedings to be *ex parte*), 50 U.S.C. § 1805(c)(2)(B) (providing that upon the applicant's request, the FISA Court order authorizing surveillance "shall" direct any common carrier or similar entity through which the surveillance is performed to "protect [the] secrecy" of the surveillance).

[3]*See United States v. Ehrlichman*, 546 F.2d 910, 914 (D.C. Cir. 1976) (describing history of "the Special Investigations" or "Room 16" unit within the Nixon White House and some of the burglaries and other "covert operations" the unit performed).

[4]*See, e.g., Ellsberg v. Mitchell*, 709 F.2d 51, 53-55 (D.C. Cir. 1983) (noting that the defendants, members of the Nixon Administration, admitted to wiretapping "one of plaintiffs' attorneys or consultants" on direct orders of the President).

[5]See Final Report of the Select Committee on Presidential Campaign Activities, S. Rep. No. 93-981, 93d Cong., 2d Sess., 564 (1974). *See also* Napolitano, Hon. Andrew J., "Is the FISA Court Constitutional?", Creators.com (Sept. 26, 2013), *available at* www.creators.com/opinion/judge-napolitano/is-the-fisa-court-constitutional.html.

[6]The act also created the FISA Court of Review, which rarely hears appeals, hearing its first appeal in 2002. Its jurisdiction is limited to the "denial of any application made under this Act." (emphasis added). *See* Foreign Intelligence Surveillance Act of 1978, Act Oct. 25, 1978, Pub. L. No. 95-511, § 1, 92 Stat. 1783, codified at 50 U.S.C. §§ 1801 *et seq*. *See* 50 U.S.C. §1803(b). *See also* "Foreign Intelligence Surveillance Court of Review - Further Readings," *available at* http://law.jrank.org/pages/6961/Foreign-Intelligence-Surveillance-Court-Review.html (last accessed May 27, 2016).

[7]McAdams III, James G., "Foreign Intelligence Surveillance Act (FISA): An Overview," Federal Law Enforcement Training Centers, *available at* www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf (last accessed May 27, 2016).

[8]*See* 50 U.S.C. § 1803(a)(1).

[9]*See* 50 U.S.C. §§ 1802(b), 1805(a).

[10]Brief on Behalf of Amicus Curiae National Association of Criminal Defense Lawyers in Support of Affirmance," filed Sept. 26, 2002, NACDL Amicus Committee, *In re Appeal from July 19, 2002 Decision of the United States Foreign Intelligence Surveillance Court,* Case No. 02-001 (U.S. Foreign Intel. Surveillance Ct. of Review), *available at* www.epic.org/privacy/terrorism/fisa/nacdl_fisa_brief.pdf.

[11]"Last Week Tonight with John Oliver: Government Surveillance (HBO)" (Video), LastWeekTonight (first aired April 5, 2015), HBO Networks, *available at* www.edwardsnowdennews.com/edward-snowden/last-week-tonight-with-john-oliver-government-surveillance-hbo.

[12]From a statistical analysis by Electronic Privacy Information Center, during the 25 years from 1979–2004, 99.7 percent of warrant requests were granted. Foreign Intelligence Surveillance Act Court Orders, 197-2015," Electronic Information Privacy Center, *available at* www.epic.org/privacy/wiretap/stats/fisa_stats.html (last visited May 27, 2016).

[13]*Id.*

[14]ABA Model Rules of Professional Conduct (2009), R. 3.3(d) ("In an *ex parte* proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer that will enable the tribunal to make an informed decision, whether or not the facts are adverse.").

[15]Dan Robert, "US must fix secret FISA courts, says top judge who granted surveillance orders," The Guardian (July 9, 2013), *available at* www.theguardian.com/law/2013/jul/09/fisa-courts-judge-nsa-surveillance.

[16]Philip Shenon, "Secret Court Says F.B.I. Aides Misled Judges in 75 Cases," The New York Times (Aug. 23, 2002), *available at* www.nytimes.com/2002/08/23/us/secret-court-says-fbi-aides-misled-judges-in-75-cases.html.

[17]Muslim Cmty. Ass'n v. Ashcroft, 459 F. Supp. 2d 592, 597 (E.D. Mich. 2006) (citing 50 U.S.C. § 1861(b)(2)).

[18]*See* Muslim Cmty. Ass'n v. Ashcroft, 459 F. Supp. 2d 592, 597 (E.D. Mich. 2006) (citing 50 U.S.C. § 1861(b)(2)).

[19]"In December 2005, news agencies began reporting that President George W. Bush had ordered the National Security Agency (NSA) to conduct eavesdropping of some portion of telecommunications in the United States without warrants and that the NSA had obtained the cooperation of telecommunications companies to tap into a significant portion of the companies' telephone and e-mail traffic, both domestic and international." Al-Haramain Islamic Foundation, Inc v. Bush (In re NSA Telcoms. Records Litig.), 633 F. Supp. 2d 949, 955 (N.D. Cal. 2009) (citing James Risen and Eric Lichtblau,"Bush Lets US Spy on Callers Without Courts," The New York Times (Dec 16, 2005)). *See also* In re Nsa Telcoms. Records Litig., 2010 U.S. Dist. LEXIS 136156 (N.D. Cal. Dec. 21, 2010) (stating that the program involved "interception, without court order, of international communications").

[20]Tim Weiner, Enemies: A History of the FBI, 421 (Random House, New York (2012)).

[21]*Id*. at 433-434. *See also* Unclassified Report on the President's Surveillance Program, Report No. 2009-0013-AS, Office of the Inspector General of the Department of Justice, et al. (July 9, 2009).

[22]James Risen and Eric Lichtblau,"Bush Lets US Spy on Callers Without Courts," The New York Times (Dec. 16, 2005), *available at* www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

[23]"Cheney: Bush has right to authorize secret surveillance," CNN (Dec. 20, 2005), *available at* www.cnn.com/2005/POLITICS/12/20/cheney.wiretaps.

[24]Eric Lichtblau, "Judges on Secretive Panel Speak Out on Spy Program," The New York Times (March 29, 2006), *available at* www.nytimes.com/2006/03/29/politics/29nsa.html.

[25]Carol D. Leonnig and Dafna Linzer, "Spy Court Judge Quits In

Protest," The Washington Post (Dec. 21, 2005), *available at* www.washingtonpost.com/archive/politics/2005/12/21/spy-court-judge-quits-in-protest/9dfc1009-6854-4f13-aa34-2eac70c251d5.

[26]Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearings Before the Senate Committee on the Judiciary, 109th Cong. 2nd Session (Feb. 6, 2006), transcript *available at* http://fas.org/irp/congress/2006_hr/nsasurv.html.

[27]See Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, July 10, 2008, 122 STAT. 2436, Pub. L. No. 110–261 (110th Congress), §§ 702(a) & (g)(1)(B).

[28]Barack Obama, Speech at DePaul University Student Activities Center (Oct. 7, 2007), *available at* http://www.c-span.org/video/?201316-1/obama-foreign-policy-speech. *See also* "Savage, Charlie, "Power Wars: Inside Obama's Post-9/11 Presidency," Little Brown and Company, New York (2015).

[29]Lawrence Wright, "The Twenty-Eight Pages," The New Yorker (Sept. 9, 2014), *available at* http://www.newyorker.com/news/daily-comment/twenty-eight-pages .

[30]"Press Release: Remarks by the President on Review of Signals Intelligence," The White House, Office of the Press Secretary (January 17, 2014), *available at* www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

[31]Mark Hosenball, "Snowden downloaded NSA secrets while working for Dell, sources say," Reuters (Aug. 15, 2013), *available at* www.reuters.com/article/usa-security-snowden-dell-idUSL2N0GF11220130815.

[32]"Snowden began downloading NSA files a year earlier than previously reported," RT News (Aug. 16, 2013), *available at* www.rt.com/usa/snowden-documents-dell-nsa-580/.

[33]"Ex-NSA Chief Details Snowden's Hiring at Agency, Booz Allen," The Wall Street Journal (Feb. 4, 2014), *available at* www.wsj.com/articles/SB10001424052702304626804579363651571199832.

[34]"Roger Clemens Indicted for Lying to Congress," CBS News (Aug.19, 2010), *available at* www.cbsnews.com/news/roger-clemens-indicted-for-lying-to-congress/.

[35]Current and Projected National Security Threats to the United States: Hearing Before the Select Committee on Intelligence of the U.S. Senate, 113th Cong. 1st Session (March 12, 2013), transcript (p. 66) *available at* https://fas.org/irp/congress/2013_hr/threat.pdf.

[36]"Snowden-Interview: Transcript," Norddeutscher Rundfunk (radio) (first broadcast Jan. 23, 2014), *available at* www.ndr.de/nachrichten/netzwelt/snowden277_page-2.html.

[37]Carlo Muñoz, "GOP's Amash: Clapper should resign," The Hill (June 12, 2013), *available at* www.thehill.com/policy/defense/305031-rep-amash-calls-for-dni-clapper-to-resign.

[38]Jose Delreal, "Paul slams Clapper over NSA 'lying'," Politico (Dec. 18, 2013), *available at* www.politico.com/story/2013/12/rand-paul-james-clapper-national-security-agency-101306.

[39] Giuseppe Macri "Sensenbrenner: 'Clapper ought to be fired and prosecuted'," The Daily Caller (Dec. 6, 2013), *available at* www.dailycaller.com/2013/12/06/sensenbrenner-clapper-ought-to-be-fired-and-prosecuted.

[40]David Keene, "KEENE: James Clapper should resign for lying to Congress," Washington Times (Dec.12, 2013), *available at* www.washingtontimes.com/news/2013/dec/12/keene-failing-to-do-the-honorable-thing.

[41]*ACLU v. Clapper,* No. 13-CV-03994 (S.D.N.Y. 2013).

[42] "Press Release: Remarks by the President on Review of Signals Intelligence," The White House, Office of the Press Secretary (January 17, 2014), *available at* www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

[43] "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court," Privacy and Civil Liberties Oversight Board (Jan. 23, 2014), *available at* https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

[44] Obama, Barack, "Transcript of President Obama on changes to National Security Agency programs," Washington Post (Jan. 17, 2014), *available at* https://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

[45] *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015).

[46] *See* 50 U .S.C. §§ 1803(i)(l) – (i)(2)(B).

[47]Dan Robert, "US must fix secret FISA courts, says top judge who granted surveillance orders," The Guardian (July 9, 2013), *available at* www.theguardian.com/law/2013/jul/09/fisa-courts-judge-nsa-surveillance.

[48] *In re Applications of the Federal Bureau of Investigation for Orders Requiring the Production of Tangible Things,* Docket Nos. BR 15-77, 15-78 (U.S. Foreign Intel. Surveillance Ct., Jun. 17, 2015), *available at* http://www.fisc.uscourts.gov/sites/default/files/BR%20 15-77%2015-78%20Memorandum%20Opinion.pdf.

[49]Jasob, Fischler, "FISC Names Spy Defense Atty Adviser For FBI Metadata Case," Law360 (Sept. 28, 2015), *available at* www.law360.com/articles/708032/fisc-names-spy-defense-atty-adviser-for-fbi-metadata-case.

[50]Tim Cushing, "FISA Court's Appointed Advocate Not Allowing Government's 'National Security' Assertions To Go Unchallenged," TechDirt (Dec. 11, 2015), *available at* www.techdirt.com/blog/?tag=amicus. See Reply Memorandum of Amicus Curiae to the U.S. Response to October 29, 2015 Memorandum of Law, *In re Applications of the Federal Bureau of Investigation for Orders Requiring the Production of Tangible Things,* Docket Nos. BR 15-99 (filed Nov. 9, 2015, U.S. Foreign Intel. Surveillance Ct.), *available at* https://assets.documentcloud.org/documents/2644587/FISC-Amicus-Reply.pdf.

[51]Cyrus Farivar, "America's super-secret court names five lawyers as public advocates," Ars Technica (Nov. 28, 2015), *available at* http://arstechnica.com/tech-policy/2015/11/americas-super-secret-court-names-five-lawyers-as-public-advocates.

[52]Chelsea E. Manning, "FISA courts stifle the due process they were supposed to protect. End them." The Guardian (Nov. 3, 2015), *available at* www.theguardian.com/commentisfree/2015/nov/03/end-fisa-courts-due-process-chelsea-manning.

[53]Elizabeth (Liza) Goitein and Faiza Patel, "What Went Wrong with the FISA Court," Brennan Center For Justice (2015), *available at* www.brennancenter.org/publication/what-went-wrong-fisa-court.

[54]"Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," Privacy and Civil Liberties Oversight Board (July 2, 2014), *available at* https://www.pclob.gov/library/702-Report.pdf

[55]Richard Clarke, *et al.,* "The NSA Report: Liberty and Security in a Changing World," The President's Review Group on Intelligence and Communications Technologies (Dec. 12, 2013), *available at* www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[56]William Saletan, "Going Courtless: The NSA searches its mass data-

continued on page 66

Civil Forfeiture *continued from page 49*

from the necessity of the case, as the only adequate means of suppressing the offence or wrong, or [e]nsuring an indemnity to the injured party.").

[20]*See, e.g.*, *The Brig Malek Adhel*, 43 U.S. (2 How.) at 233 (justifying forfeiture of an innocent owner's vessel under piracy and admiralty laws because of "the necessity of the case, as the only adequate means of suppressing the offence or wrong"); *The Palmyra*, 25 U.S. (12 Wheat.) at 14 (concerning revenue laws); *United States v. The Schooner Little Charles*, 1 Brock. 347, 354 (C.C.D. Va. 1818) (per Marshall, C.J.) (concerning embargo laws).

[21]Boudreaux & Pritchard, 33 San Diego L. Rev. at 101.

[22]*Carroll v. United States*, 267 U.S. 132, 155 (1925).

[23]*United States v. One 1936 Model Ford V-8 De Luxe Coach, Commercial Credit Co.*, 307 U.S. 219, 236 (1939).

[24]*Id*. at 226.

[25]Eric Blumenson & Eva Nilsen, *Policing for Profit: The Drug War's Hidden Economic Agenda*, 65 U. Chi. L. Rev. 35, 42–45 (1998).

[26]*See Federal Asset Forfeiture: Uses and Reforms: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations of the H. Comm. on the Judiciary*, 114th Cong. (2015) (statement of David B. Smith, Smith & Zimmerman, PLLC), *available at* judiciary.house.gov/wp-content/uploads/2016/02/Smith-Testimony.pdf.

[27]Dick M. Carpenter et al., *Policing for Profit: The Abuse of Civil Asset Forfeiture* 12–13 & Fig. 4 (2d ed. 2015). The Institute for Justice published this second edition of its landmark comprehensive study evaluating each jurisdiction's forfeiture laws.

[28]18 U.S.C. § 983(c)(1). *See also* Carpenter et al., *supra* note 16 (noting that this is the standard for 31 states as well).

[29]*Id.* at 20 (noting that this is also true for 35 states).

[30]*Id.* at 12; *see also* Jefferson E. Holcomb et al., *Civil Asset Forfeiture, Equitable Sharing, and Policing for Profit in the United States*, 39 J. Crim. Just. 273 (2011).

[31]*See, e.g.*, 28 U.S.C. § 524(c)(1) (establishing the DOJ Assets Forfeiture Fund, which allows forfeiture proceeds to be used for a variety of law-enforcement purposes); 31 U.S.C. § 9705 (establishing the Department of the Treasury Forfeiture Fund).

[32]Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837 (1984).

[33]Carpenter et al., *supra* note 10.

[34]U.S. Dep't of Justice, *FY 2013 Total Net Deposits to the Fund by State of Deposit as of Sept. 30, 2013*, *available at* www.justice.gov/jmd/afp/02fundreport/2013affr/report1.htm.

[35]Carpenter et al., *supra* note 10.

[36]*Id*.

[37]George Mason, Fairfax County Freeholders' Address and Instructions to Their General Assembly Delegates (May 30, 1978), in Jeff Broadwater, George Mason: Forgotten Founder 153 (2006).

[38]For statutes authorizing equitable sharing, see 21 U.S.C. §§ 881(e)(1)(A) and (e)(3), 18 U.S.C. § 981(e)(2), and 19 U.S.C. § 1616a.

[39]Nick Sibilla, *The 14 Most Ridiculous Things Police Bought With Asset Forfeiture* (June 24, 2013), www.buzzfeed.com/nicks29/the-14-most-ridiculous-things-police-bought-with-a-4y3w.

[40]For more information on the Hirsch brothers, visit ij.org/case/long-island-forfeiture/.

[41]For more information on Carole Hinders, visit ij.org/case/iowa-forfeiture/.

[42]For more information on Charles Clarke, visit ij.org/case/kentucky-civil-forfeiture/.

[43]For more information on Russ Caswell, visit ij.org/case/massachusetts-civil-forfeiture/.

[44]Michael Sallah et al., *Stop and Seize*, Wash. Post, Sept. 6, 2014, *available at* www.washingtonpost.com/sf/investigative/2014/09/06/stop-and-seize/.

[45]*See* Shaila Dewan, *Law Lets IRS Seize Accounts on Suspicion, No Crime Required*, N.Y. Times, Oct. 25, 2014, at A1, *available at* www.nytimes.com/2014/10/26/us/law-lets-irs-seize-accounts-on-suspicion-no-crime-required.html?_r=0.

History of FISA *continued from page 64*

base of phone records without real judicial oversight. That's unacceptable." Slate (June 21, 2013), *available at* www.slate.com/articles/technology/technology/2013/06/warrantless_searches_the_court_oversight_of_nsa_phone_surveillance_is_a.html.

[57]"Liberty and Security in a Changing World," Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[58]The phrase "three hops," which comes from NSA honcho John Inglis' testimony to the House Judiciary Committee in July, means that the agency can look at the communications of the person it's targeting, plus the communications of that person's contacts (one hop), plus the communications of those people's contacts (two hops), plus the communications of *those* people's contacts (three hops). Each hop widens the net exponentially, so that if the average person has 40 contacts, a single terrorism suspect could theoretically lead to records being collected on 2.5 million people.

[59]"Since the (current) chief justice began making assignments in 2005, 86 percent of his choices have been Republican appointees, and 50 percent have been former executive branch officials." Scott Horton, "The G.O.P.'s Surveillance Judiciary," Harper's Magazine (July 29, 2013), *available at* http://harpers.org/blog/2013/07/the-gops-surveillance-judiciary.

[60]"About the Board," Privacy and Civil Liberties Oversight Board, *available at* www.pclob.gov/about-us.html (last visited May 27, 2016).

[61]*United States v. Edward Snowden*, No. 13-cr-265 (CMH) (E.D. Va.), Criminal Complaint (filed June 14, 2013), *available at* http://apps.washingtonpost.com/g/documents/world/us-vs-edward-j-snowden-criminal-complaint/496.

[62]"Pardon Edward Snowden," We the People, Your Voice in the White House, *available at* https://petitions.whitehouse.gov/petition/pardon-edward-snowden (last visited May 27, 2016).

[63]Kate Knibbs, "White House Responds to Petition to Pardon Snowden With a Hard Pass, Gizmodo (July 29, 2015), *available at* http://gizmodo.com/white-house-responds-to-petition-to-pardon-snowden-with-1720831190.

[64]"Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman." Hon. Louis Brandeis, "Other People's Money," National Home Library Foundation, 62 (1933).