

SCOLANS FISA Working Group
FISA Reference Guide
May 2014

Bill Banks
Spike Bowman
Laura K. Donohue
John Shenefield

*The following selected FISA-related references are provided
for those interested in background reading.*

BOOKS:

STEWART A. BAKER, *SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM* (Hoover Institution Press 2010), *available at* <http://www.hoover.org/publications/books/8128>.

Baker examines the technologies we love—jet travel, computer networks, and biotech—and finds that they are likely to empower new forms of terrorism unless we change our current course a few degrees and overcome resistance to change from business, foreign governments, and privacy advocates. He draws on his Homeland Security experience to show how that was done in the case of jet travel and border security but concludes that heading off disasters in computer networks and biotech will require a hardheaded recognition that privacy must sometimes yield to security, especially as technology changes the risks to both.

DAVID KRIS AND J. DOUGLAS WILSON, *NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS*, 2d Ed., (2012-2013), *available at* <http://legalsolutions.thomsonreuters.com/law-products/Treatises/National-Security-Investigations-and-Prosecutions-2d/p/100026272>.

In this 2-volume treatise Kris and Douglas present the law governing, and related to, national security investigations. The authors explore the full background of NSIs, both from a pre-9/11 and post-9/11 perspective. It is indispensable reading for FISA, its subsequent amendments, and related guidelines.

ARTICLES:

Matthew A. Anzaldi & Jonathan W. Gannon, *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act: Judicial Recognition of Certain Warrantless Foreign Intelligence Surveillance*, 88 TEX. L. REV. 1599 (2010), *available at* http://findarticles.com/p/articles/mi_7756/is_201006/ai_n54718729/?tag=content;coll.

Authors evaluate the Protect America Act, the legislative history leading to the enactment of the statute, and its implementation. They also provide insight into the Foreign Intelligence Surveillance Court of Review's decision to uphold the Protect America Act and create a foreign intelligence exception to the Warrant Clause of the Fourth Amendment.

Michael Avery, *The Constitutionality of Warrantless Electronic Surveillance of Suspected Foreign Threats to the National Security of the United States*, 62 U. MIAMI L. REV. 541 (2008), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1139072.

Avery explores the constitutional issues involved in warrantless wiretapping under the Terrorist Surveillance Program. He concludes that the President did not have inherent authority or authority under the Authorization for Use of Military Force to engage in surveillance without a warrant. Further, Avery argues that even with Congressional amendments to FISA in place, warrantless electronic surveillance violates the Fourth Amendment.

James A. Baker, *Symposium Introduction: Intelligence Oversight*, 45 HARVARD J. ON LEGIS. 199 (2008), available at <https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=45+Harv.+J.+on+Legis.+199&srctype=smi&srcid=3B15&key=e4abbc6222a8ca2be9cbd0b027a2b349>.

Baker provides a general introduction to intelligence oversight. He argues that we must do our best to make rational choices regarding the intelligence community based upon a realistic assessment of the costs and benefits of our decisions. Baker continues that proper oversight must be both objective and non-partisan.

William C. Banks, *Is the FISA Amendments Act of 2008 Good Policy? Is It Constitutional?*, 35 WM MITCHELL L. REV. 5007 (2011), available at http://web.wmitchell.edu/national-security-forum/wp-content/uploads/2011/06/3-10_Qs_Banks_Format.pdf.

Banks examines the stresses on the original FISA architecture, TSP, efforts to fold TSP into FISA, the Protect America Act of 2007, and construction of the FAA. Highlighting the significance of the changes made in the FAA to traditional FISA, Banks raises questions about potential further concerns related to Section 702.

William C. Banks, *Programmatic Surveillance and FISA; Of Needles in Haystacks*, 88 TEX. L. REV. 1633 (2010), available at http://findarticles.com/p/articles/mi_7756/is_201006/ai_n54718733/?tag=content;coll.

Banks evaluates the implementation of the FISA Amendments Act of 2008. He explains that modern communications and surveillance technologies have so complicated policy discussions that the values debate has drowned in a sea of misapprehension about the means to implement the policies. Meanwhile, FISA has become so complex that the law further occludes informed policy choices. For these reasons, Banks suggests that the basic architecture of FISA should be recast.

William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209 (2007), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=990728.

Banks suggests that the 1978 compromise that led to enactment of FISA is crumbling under the weight of changes in technology, slapdash amendments, and the Terrorist Surveillance Programs' circumvention of the statute. He continues by suggesting that forms are needed to control programmatic surveillance and to lessen the chance of over-collection and lack of oversight.

William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1 (2000), available at <http://www.wcl.american.edu/journal/lawrev/50/banks.pdf?rd=1>

Banks provides an overview and history of the development of executive authority for national security surveillance, from the founding to 2000, including the intersection of executive and congressional authority in FISA and its implementation.

Ricardo J. Bascuas, *Fourth Amendment Lessons from the Highway and the Subway: A Principled Approach to Suspicionless Searches*, 38 RUTGERS L.J. 719 (2007), available at http://org.law.rutgers.edu/publications/lawjournal/38_3/02BascuasVol.38.3.pdf.

Bascuas argues to eliminate the balance of individual interests against the government's need to search. He continues that Fourth Amendment rights should not vary according to expectations of privacy in the abstract, but should yield to the more concrete protections of property. Bascuas further suggests that "probable cause" should be rearticulated back to its original, more limited meaning, as opposed to the loosely used contexts in which it is currently employed.

Patricia L. Bellia, *The 'Lone Wolf' Amendment and the Future of Foreign Intelligence Surveillance Law*, 50 VILL. L. REV. 425 (2005), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=714244.

Bellia explains that FISA has evolved in a piecemeal fashion since 1978. As such, it has greatly expanded, yet the information structure has not kept pace. She explores the constitutional issues that arose with the evolved uses of FISA and argues that Congress must develop new approaches and policies for ensuring congressional and public accountability.

Stephanie Cooper Blum, *What Really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269 (2009), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1398831.

Blum argues that the real issue posed by the FISA Amendments Act has less to do with substantive provisions of the statute and more to do with a lack of trust in the executives implementing its provisions. She argues that the best strategy for improving secret surveillance is to create a more transparent government.

Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435 (2008), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1151435.

Cate highlights the volume and variety of personal information which the government has access to through regulatory and administrative programs, as well as through private industry. He argues that there is an absence of meaningful limits on that access which leads to compromises in individual privacy and national security. Cate concludes that Congress must take action to impose these limits.

Center for Democracy & Technology, *Minimization Cannot Be Relied Upon to Protect the Rights of Americans Under a Warrantless Surveillance Program*, September 17, 2007, available at <http://www.cdt.org/security/20070917mimization-memo.pdf>.

The author argues that the minimization procedures applicable to the Protect America Act do not provide adequate protection for the rights of American citizens. The current procedures fall short because the targets are poorly defined, the government cannot feasibly deal with so much readily available digital information, and there is a much lower threshold for action after 9/11.

Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J. OF L. & PUB. POL'Y (2014), available at <http://scholarship.law.georgetown.edu/facpub/1294/>.

Donohue argues that the Section 215 bulk telephony metadata program runs contrary to the purpose of FISA and violates the statutory language by failing to satisfy the requirement that records sought be "relevant to an authorized investigation", by violating the requirement that information otherwise be obtainable via subpoena duces tecum, and that places restrictions on pen registers and trap and trace devices. The author also addresses Fourth Amendment concerns in light of the Court's recent jurisprudence.

Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, Georgetown Law Scholarly Commons (2014), available at

http://scholarship.law.georgetown.edu/do/search/?q=author_lname%3A%22Donohue%22%20AND%20author_fname%3A%22Laura%22&start=0&context=890094&sort=date_desc.

Donohue discusses the evolution of Section 702 and argues that the NSA has sidestepped the statutory restrictions related to targeting via the “to, from, or about” nomenclature, created a presumption of non-U.S. person status, and failed to adopt minimum standards that would require the agency to ascertain whether a target is within domestic bounds. As part of post-targeting minimization and analysis the author considers the purpose of the analysis, the scope of the minimization procedures, the use of U.S. person information to query the data and recombinant information. Donohue argues that both areas, as well as retention and dissemination of data, raise Fourth Amendment concerns.

Laura K. Donohue, *FISA Reform, I/S: A J. OF L. & POL’Y FOR THE INFO. SOCIETY* (2014), available at <http://scholarship.law.georgetown.edu/facpub/1318/>.

Donohue offers a new taxonomy for how to think about FISA reform. Rooted in examination of how, since 1978, technology has altered the types of information available, as well as methods of transmission and storage, the author divides foreign intelligence gathering into two categories: front-end collection and back-end analysis and use. Each category contains a counterpoise structured to ensure the appropriate exercise of Congressionally-mandated authorities. For the front-end, this means balancing the manner of collection with requirements for approval. For the back-end, this means offsetting implementation with transparency and oversight.

Stephen Dycus, *Congress’s Role in Cyber Warfare*, 4 J. NAT’L SECURITY L. & POL’Y 155 (2010), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1486767.

Dycus argues that the future of the United States may depend on our ability not only to protect ourselves from enemies armed with cyber weapons, but also to use such weapons wisely ourselves. He urges collaboration amongst the various intelligence agencies and suggests the need for Congress to establish its role in the development of policies for war on a digital battlefield.

Jonathon D. Forgang, “*The Right of the People*”: *The NSA, The FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas*, 78 FORDHAM L. REV. 217 (2009), available at http://law.fordham.edu/assets/LawReview/Forgang_October_2009.pdf.

Forgang concludes that the Fourth Amendment requires U.S. intelligence agencies to obtain a specific warrant before engaging in overseas surveillance of American citizens. He argues for further amendments to FISA, including a comprehensive and individualized warrant process that protects both privacy and national security.

William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma – A History*, 11 LEWIS & CLARK L. REV. 1099 (2007), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1098940.

Funk argues that the original purpose of FISA was to gather foreign intelligence, rather than for obtaining evidence to be used in criminal trials. Subsequent misinterpretations by the Department of Justice and the Foreign Intelligence Surveillance Court led to the creation of the so-called “wall,” which was contrary to the original intent of the statute. Furthermore, Funk argues that the attempts to clarify this requirement under the Patriot Act were unnecessary and gave rise to other constitutional issues.

Mark H. Gitenstein, *Nine Democracies and the Problems of Detention, Surveillance, and Interrogation*, in LEGISLATING THE WAR ON TERROR 7 (Benjamin Wittes ed., 2009) available at <http://books.google.com/books?id=vcE8Bg1WGH8C&lpg=PP1&ots=3OhgrqJmMi&dq=Legislation%20the%20War%20on%20Terror%20%3A%20An%20Agenda%20for%20Reform&pg=PA7#v=onepage&q&f=false>.

Gitenstein surveys the responses of a number of democratic countries in order to identify three fundamental problems that the United States has struggled with since the September 11 attacks: the circumstances under which a government may detain individuals without criminal process; the proper limits on interrogation

techniques; and the circumstances under which a government may subject persons whom it does not detain to domestic electronic surveillance.

Scott J. Glick, *FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security*, 1 HARV. NAT'L SECURITY J. 88 (2010), available at

http://www.harvardnsj.com/wp-content/uploads/2010/05/Vol.1_Glick_Final.pdf

Glick examines the Foreign Intelligence Court of Review's decision to let stand certain restrictions on the government's use of FISA. He argues that the court reached an erroneous conclusion in regard to the scope of the government's power. Also, the author takes a comprehensive and fresh look at the legislative history of FISA's purpose requirement, both before and after the Court of Review's decision. He concludes by proposing legislation that would remove the restrictions placed on the government by the Court of Review.

Matthew R. Hall, *Constitutional Regulation of National Security Investigation: Minimizing the Use of Unrelated Evidence*, 41 WAKE FOREST L. REV. 61 (2006), available at

<http://lawreview.law.wfu.edu/documents/issue.41.61.pdf>.

Hall formulates a proposal for the constitutional regulation of national security investigations in order to address common apprehensions about such actions. He argues that minimization should evolve to limit the use of evidence, acquired through national security investigations, which are unrelated to a national security matter.

Beryl A. Howell, *Seven Weeks: The Making of the USA Patriot Act*, 72 GEO. WASH. L. REV. 1145 (2004), available at

http://heinonline.org/HOL/Page?handle=hein.journals/gwlr72&div=53&g_sent=1#1159.

Focusing on the experiences of the Senate Judiciary Committee, Howell outlines the considerations and compromises made throughout the seven-week process of producing the USA Patriot Act. He argues that due to the expediency of the process, there was little chance to build public understanding of, or confidence in, the compromises embodied in the legislation. For this reason, he suggests that there needs to be ongoing efforts to inform the public of the implications of the legislation.

Alexander W. Joel, *Choosing Both: Making Technology Choices at the Intersections of Privacy and Security*, 88 TEX. L. REV. 1401, 1751 (2010), available at

http://findarticles.com/p/articles/mi_7756/is_201006/ai_n54718732/.

Joel provides an overview of the dilemma between utilizing technology for intelligence activities and continuing to protect civil liberties and privacy interests. He suggests that the question faced is not whether a balance should be struck between these competing interests, but rather how to strike such a balance.

Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STANFORD L. REV (2010), available at

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1348322.

Kerr argues for the creation of technology-neutral policies that will shift the focus from physical space to cyberspace. The author proposes that this can be accomplished in two steps. First, the traditional geographic distinctions should be replaced by content and non-content information distinctions. Second, search warrants should be particularized based on individuals rather than internet accounts to collect contents of protected internet communications.

Orin S. Kerr, *The Modest Role of the Warrant Clause in National Security Investigations*, 88 TEX. L. REV. 1669 (2010), available at

http://findarticles.com/p/articles/mi_7756/is_201006/ai_n54718735/?tag=content;coll.

Kerr grapples with why the Warrant Clause of the Fourth Amendment remains so modest in national security contexts. He provides alternative explanations for this development. The author concludes that the Warrant Clause must remain modest in the context of national security.

Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225 (2008), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1000398.

Kerr argues that FISA insufficiently addresses changing technology as subject identity and location pose substantial challenges. He suggests that a new approach based on separate authorities for surveillance, which would depend on whether identity and/or location are known, should be developed to handle the realities of modern communication networks.

Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STANFORD L. REV. 503 (2007), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=976296.

Kerr suggests that reasonable expectations of privacy take on different meanings within different contexts. There is no single top-down test for what is reasonable, but rather there are four separate models. He concludes that solidifying and understanding these models will allow judges to better frame their decisions and create better guidance for Fourth Amendment protections.

David S. Kris, *On the Bulk Collection of Tangible Things*, 1 LAWFARE RESEARCH PAPER SERIES (2013), available at <http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf>.

Kris analyzes five legal issues related to the Section 215 telephony metadata program: NSA dependence on the theory as to the “relevance” to an FBI terrorism “investigation”; direction from FISC to produce metadata to the NSA, not to the FBI; the timing of the production required from the provider (daily and ongoing); restrictions on the use and dissemination of the data (including the RAS query standard); and whether and to what extent the legal arguments in support of bulk telephony metadata collection could apply to other kinds of business records.

David S. Kris, *Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Introduction*, LAWFARE BLOG (May 18, 2013), available at <http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-introduction/#.UsG0H45xKPc>.

_____. *Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Challenges*, LAWFARE BLOG (May 19, 2013), available at <http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-challenges/#.UsG0Y45xKPc>.

_____. *Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Approach*, LAWFARE BLOG (May 20, 2013), available at <http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-approach/#.UsGzi45xKPc>

Kris wrote this three-part blog post prior to the Snowden releases, looking at FISA reform, considering potential challenges to alterations to the current regime, and contemplating possible future approaches.

David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act*, BROOKINGS INST. (2008), available at http://www.brookings.edu/papers/2007/1115_nationalsecurity_kris.aspx.

Kris discusses the justification for and meaning behind the Protect America Act, the Responsible Surveillance that is Overseen, Reviewed and Effective Act and the FISA Amendments Act. The author suggests that there exists a need to expand beyond the 1978 conceptions of security to an approach that accounts for changes in telecommunications technology and increased globalization. (This Kris paper also appears in a slightly updated version in *Legislating the War on Terror: An Agenda for Reform*, Benjamin Wittes, ed., Brookings Press (2009).)

David S. Kris, *Spies, Secrets, and Security: The New Law of Intelligence; The Foreign Intelligence Surveillance Act; The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL’Y REV.

487 (2006), available at <https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&crawlid=1&doctype=cite&docid=17+Stan.+L.+%26+Pol%27y+Rev+487&srctype=smi&srcid=3B15&key=ae9f5113db3db1961eb1ff6a28730ea6>.

Kris provides a history of the rise and fall of the FISA “wall.” He argues that both security and liberty can be better protected with the wall down than with the wall up as foreclosure of the use of civilian courts may elicit the use of less desirable remedies.

Craig S. Lerner, *The Reasonableness of Probable Cause*, 81 TEXAS L. REV. 951 (2003), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=784564.

Lerner argues for a reappraisal of the concept of probable cause and a shift to an approach that factors in the gravity of the offense being investigated and the intrusiveness of the search being proposed. The author presents a background on the development of the conception of probable cause and applies the new proposed probable cause approach to the case of Zacarias Moussaoui.

J.I. Nelson, *How the NSA Warrantless Wiretap System Works*, February 7, 2006, available at <http://www.nerdyloirrin.net/jerry/politics/Warrantless/WarrantlessFACTS.html>.

Nelson provides an educated guess as to how the NSA Warrantless Wiretap System Works. He argues that old safeguards do not work with the new systems.

J.I. Nelson, *Mini-Tutorial: The National Infrastructures for Voice and for Data Communications*, July 19, 2006, available at <http://www.nerdyloirrin.net/jerry/politics/Warrantless/WarrantlessBKGND.html>.

Nelson provides an explanation of the inability to extend old wiretapping laws to new technologies. He explains that in order to tap one person’s line on the internet, you must tap everything, as there are no “lines.”

Paul Ohm, *The Argument Against Technology-Neutral Surveillance Laws*, 88 TEX. L. REV. 1685 (2010), available at http://findarticles.com/p/articles/mi_7756/is_201006/ai_n54718734/?tag=content;coll.

Ohm breaks his discussion into three parts, offering, in turn, the best arguments for tech neutrality, the underappreciated counterarguments to those arguments, and the case for tech specificity. Ultimately, he tries to counter the pervasively held attitude that tech-specific laws are indefensible mistakes to be avoided. Instead, he suggests that, quite often, tech specificity is the wiser course and the best way to balance the government's need to provide security with the right to privacy.

Diane Carraway Piette & Jesselyn Radack, *Piercing the “Historical Mists”: The People and Events Behind The Passage of FISA and the Creation of the “Wall,”* 17 STAN. L. & POL’Y REV. 437 (2006), available at http://webcache.googleusercontent.com/search?q=cache:zWoomWOGd3kJ:2009transition.org/liberty-security/index.php%3Foption%3Dcom_docman%26task%3Ddoc_download%26gid%3D7%26Itemid%3D+%2217+Stan.+L.+%26+Pol%27y+Rev+437%22&cd=6&hl=en&ct=clnk&gl=us.

Carraway analyzes the events leading to and motives behind the passage of FISA, focusing on the reasons for the construction of the “wall.” She explains that understanding the true motives for the creation of FISA is critical to informed decision making in amending the statute in the wake of the warrantless domestic wiretapping uproar.

Daniel L. Pines, *The Central Intelligence Agency’s “Family Jewels”: Legal Then? Legal Now?*, 84 INDIANA L. J. 637 (2009), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1330108.

Pines explains that history shows that after the initial hype surrounding supposed illegal intelligence techniques dissipates, the activity is often concluded to be legal. He compares the laws at the time of the “Family Jewels” with the current laws applying to the same activities.

Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245 (2008), available at http://lawreview.uchicago.edu/sites/lawreview.uchicago.edu/files/uploads/75.1/75_1_Posner.pdf.

Posner considers how modern life and the ubiquitous nature of technology affect the voluntary and involuntary disclosure of personal information, arguing that modernity “has habituated most Americans to radically diminished informational privacy” even as it has made it possible for intelligence agencies to collect significant amounts of information outside Title III and FISA. The author focuses on recent amendments to FISA and suggests that only the point at which sentient beings conduct a search are Fourth Amendment questions raised. Posner then offers a number of potential ways to further amend FISA.

Robert C. Power, “*Intelligence*” Searches and Purpose: A Significant Mismatch Between Constitutional Criminal Procedure and the Law of Intelligence-Gathering, 30 PACE L. REV. 620 (2010), available at

http://works.bepress.com/cgi/viewcontent.cgi?article=1021&context=robert_power.

Power examines whether the distinction between a criminal investigatory purpose and a foreign intelligence purpose can, or even should be dispositive of Fourth Amendment issues. He argues that the courts have overlooked that the under a Fourth Amendment totality of the circumstances approach, the changes have created an easy road to conduct extraordinarily intrusive warrantless searches without probable cause.

Michael P. Robottie, *Grasping the Pendulum: Coordination Between Law Enforcement and Intelligence Officers Within the Department of Justice in a Post-“Wall” Era*, 64 N.Y.U. ANN. SURV. AM. L. 751 (2009), available at <https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=64+N.Y.U.+Ann.+Surv.+Am.+L.+751&srctype=smi&srcid=3B15&key=c49033dd919fa78014d86287e37f09dd>.

Robottie explores how the FISA purpose requirement has caused the pendulum to swing from coordination between law enforcement officers and intelligence officers to no coordination and back again. He evaluates the impact that this variance has had on the investigative capabilities of the federal government.

Jed Rubinfeld, *The End of Privacy*, 61 STAN. L. REV. 101 (October 2008), available at <http://www.stanfordlawreview.org/content/volume-61>.

Rubinfeld argues that the Fourth Amendment has been misconstrued to guarantee a right to privacy. The “reasonable expectation of privacy” falls short in addressing situations of suspicion-based incarceration of unlawful enemy combatants. Instead, the author contends that what the Fourth Amendment really guarantees is a right of security.

Theodore W. Ruger, *Chief Justice Rehnquist’s Appointments to the FISA Court: An Empirical Perspective*, 101 NW. U. L. REV. 239, 244 (2007).

Ruger assesses Chief Justice Rehnquist’s twenty-five appointments to FISC, concluding that they represented a conservative cohort inclined to favor the government on Fourth Amendment issues in the course of their ordinary judicial work, and noting that their overall conservatism was consistent with the views held by the majority of judges on the inferior federal bench during the same time. Ruger further notes that the judges appointed to FISC-R appeared to be more uniformly conservative in their judicial philosophy.

Nathan Alexander Sales, *Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy*, 9 I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY, (2014), available at <http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Sales-Article.pdf>.

Sales considers arguments supporting and opposing programmatic surveillance as manifest through the Section 215 and Section 702 programs, with particular focus on anti-unilateralism, legislative clarity, transparency/accountability and anti-mission-creep, as well as operational considerations such as internal and external checks, minimization requirements, and technological safeguards. Sales notes that from the information publicly available, the NSA programs go some way towards meeting these requirements but could be adjusted further to better conform to the principles he discusses.

Nathan Alexander Sales, *Mending Walls: Information Sharing After the USA Patriot Act*, 88 TEX. L. REV. 1795 (2010), available at http://findarticles.com/p/articles/mi_7756/is_201006/ai_n54718737/.

Sales provides an overview of how the enactment of the Patriot Act has effected information sharing between government agencies. He breaks his discussion into three parts: to weigh the advantages and disadvantages of information sharing; to identify some of the remaining legal restrictions on data exchange, as well as their policy justifications; and to consider whether the underlying values of these laws can coexist with expanded sharing.

Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287 (2008), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1116783.

Schwartz proposes that areas of telecommunications law are in need of reform and suggests an initial set of necessary steps to accomplish this. He focuses on creation of telecommunications surveillance law that will both minimize the impact of surveillance on civil liberties and maximize its efficacy for law enforcement purposes.

Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance*, 17 STAN. L. & POL'Y REV. 531 (2006), available at <https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&srctype=smi&srcid=3B15&doctype=cite&docid=17+Stan.+L.+%26+Pol%27y+Rev+531&key=669200f11abe324910415c5a22ed27ac>.

Schulhofer addresses the values and dangers of the Patriot Act's attempts to expand FISA. He argues that the steps went much farther than necessary and failed to create new safeguards to replace those they had dismantled. Schulhofer calls for substantial corrective measures to keep the FISA process running smoothly and without such dangerously expansive provisions.

Paul M. Schwartz, *Warrantless Wiretapping, FISA Reform, and the Lessons of Public Liberty: A Comment on Holmes's Jorde Lecture*, 97 CAL. L. REV. 407 (2009), available at <http://www.law.berkeley.edu/institutes/bclt/pubs/schwartz/SchwartzWiretapping.pdf>.

Schwartz argues that for there to be participation in a democracy, individuals must have an underlying capacity for self-determination provided by some personal privacy. Therefore, private liberty is a precondition for public liberty. As such, information must be adequately protected from government intrusion.

Richard Henry Seamon, *Domestic Surveillance for International Terrorists: Presidential Power and Fourth Amendment Limits*, 35 HASTINGS CON. L. QUARTERLY 449 (2008), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013123.

Seamon argues that the President has inherent authority to conduct surveillance when it is reasonably necessary to do so for the sake of a national security emergency, even if contrary to an Act of Congress. He continues that a national security emergency will qualify as an exigent circumstance under the Fourth Amendment. With these principles in mind, Seamon examines the Terrorist Surveillance Program from inception through 2007.

Peter M. Shane, *Foreword: The NSA and the Legal Regime for Foreign Intelligence Surveillance*, 9 I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY, (2014), available at <http://moritzlaw.osu.edu/students/groups/is/online-nsa-symposium/>.

Shane lays out the history of the interception of communications and provides a broader context for an online NSA Symposium responding to the releases June 2013 through February 2014. Contributors to the symposium include Laura K. Donohue, Reed E. Hundt, Shayana Kadidal, John Mueller, Bryce Clayton Newell, Nathan Alexander Sales, Mark G. Stewart, Katherine Strandburg, Stephen I. Vladeck, John Yoo, and Mark D. Young.

Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343 (2008), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=990030.

Solove addresses specific issues of data mining. He argues that privacy concerns are substantially greater than are typically accounted for, while security benefits need to be analyzed with more scrutiny. He continues that more thorough understanding of the benefits and risks must be facilitated by greater transparency.

Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEORGE WASHINGTON L. REV. 1701 (2004), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=445180.

Solove explores deeply-rooted and systematic problems within electronic surveillance law. He argues that this area of law is overly intricate, has failed to evolve with changing technology, and has insufficient oversight mechanisms. Solove suggests changes to be made to surveillance law in order to address these insufficiencies.

Geoffrey R. Stone, *The NSA's Telephone Metadata Program Is Unconstitutional*, HUFFINGTON POST, Jan. 9, 2013, available at http://www.huffingtonpost.com/geoffrey-r-stone/the-nsas-telephone-meta-d_b_4571523.html.

_____. *Is the NSA's Bulk Telephony Meta-Data Program Constitutional: Part II*, HUFFINGTON POST, Jan. 6, 2014, available at http://www.huffingtonpost.com/geoffrey-r-stone/is-the-nsas-bulk-telephon_b_4549449.html

_____. *Is the NSA's Bulk Telephony Metadata Program Constitutional?*, HUFFINGTON POST, Jan. 3, 2014, available at http://www.huffingtonpost.com/geoffrey-r-stone/is-the-nsas-bulk-telephon_b_4538173.html.

_____. *The NSA's Telephone Meta-data Program: Part III*, HUFFINGTON POST, Dec. 31, 2013, available at http://www.huffingtonpost.com/geoffrey-r-stone/the-nsas-telephone-meta-d_b_4524272.html.

_____. *The NSA's Telephone Meta-data Program: Part II*, HUFFINGTON POST, Dec. 28, 2013, available at http://www.huffingtonpost.com/geoffrey-r-stone/the-nsas-telephone-meta-d_b_4512258.html.

_____. *The NSA's Telephone Meta-data Program: Part I*, HUFFINGTON POST, Dec. 25, 2013, available at http://www.huffingtonpost.com/geoffrey-r-stone/nsa-meta-data_b_4499934.html.

Stone, who served on the President's Review Board, writes a six-part blog post discussing the contours and constitutionality of the Section 215 program and concludes that it is unconstitutional. [NB: author has numerous other posts on the program, as well as the Review Board process. See <http://www.huffingtonpost.com/geoffrey-r-stone/>.]

K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2 (2003), available at <http://www.stlr.org/html/volume5/taipale.pdf>.

Taipale argues that new technologies can be controlled to provide security for privacy through value-sensitive technology development strategies. These strategies can account for privacy concerns by building in rule-based processing, selective revelation, and strong credential and audit features. Taipale argues that failing to proceed with government research and development in these technologies will lead to development of other mechanisms that will not provide adequate oversight.

K.A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 YALE J. L. & TECH 128 (2007), available at <http://digitalcommons.law.yale.edu/yjolt>.

Taipale examines how technology and related developments have enabled new threats and new response mechanisms challenging the existing foreign intelligence framework. The author argues for the application of the existing FISA requirements to novel, technologically-enabled circumstances.

K.A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance*, 8 N.Y.U. REV. L. & SECURITY 3, 5-6 (2006), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=889120.

Taipale argues that in light of recent technological developments, FISA is inadequate as an effective safeguard. The author advocates for the use of a new legal mechanism, similar to a *Terry* stop, to be used for pre-approving more sweeping monitoring. FISA would then be used to receive subsequent approval for more targeted monitoring of identified US persons or sources from the initial automated programmatic selection.

Richard P. Terbrusch, *Gathering Foreign Intelligence in Cyberspace: Does the United States Need Another Secret Court?*, 23 QUINNIPIAC L. REV. 989 (2004), available at http://www.lexis.com/research/retrieve?_m=43e280005959a894010a208395eafc63&csvc=le&form=byCitation&fmtstr=FULL&docnum=1&startdoc=1&wchp=dGLbVzz-zSkAl&md5=32fcb18604a97872ea293b3c97ac00d9.

Terbrusch proposes the creation of a Cyber Court, or something like it, patterned after the procedures outlined in FISA. He suggests that such a court may be necessary in order to deal with the emerging international cyber terrorism threat.

Michael J. Woods & Suzanne Spaulding, *Intercepting Lone Wolf Terrorists*, in PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT 81 (Stewart A. Baker & John Kavabagh eds., 2005).

Woods and Spaulding debate the legality and structure of the “lone wolf” amendment, which broadens, and allows the government to use, FISA for surveillance of a non-U.S. person who has no known ties to a terrorist group or entity

John Yoo, *The Legality of the National Security Agency’s Bulk Data Surveillance Programs*, HARV. J. OF L. & PUB. POL’Y (2014), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2369192.

Placing the surveillance programs in a broader historical and legal context, Yoo argues that the Section 215 and Section 702 programs meet FISA’s statutory requirements. Yoo considers two constitutional dimensions, suggesting, first, that even if some aspect of the programs does not fall within Congress’s authorization for foreign intelligence and counter-terrorism surveillance, it would still reside within the President’s Commander-in-Chief authority. Second, Yoo considers that even where the federal government may have the internal authority to conduct surveillance, the Bill of Rights (via the fourth Amendment) may still prohibit its application to citizens or non-citizens in domestic bounds. He then argues that the NSA programs do not, however, violate the Fourth Amendment as currently interpreted by the federal courts.

Mark D. Young, *Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security*, 22 STAN. L. & POL’Y REV. 11 (2011), available at <http://www.questia.com/library/journal/1G1-261729763/electronic-surveillance-in-an-era-of-modern-technology>.

Young reviews the history of electronic surveillance authorities, explaining how these authorities are relevant to contemporary cyber security issues, identifying the insufficiencies of FISA and ECPA, and recommending discrete amendments.

CASES:

FISC Orders and Opinions:

In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc., Secondary Order, No. BR 13-80, at 2 (FISA Ct. Apr. 25, 2013).

In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 13-109 (FISA Ct. 2013), *available at* <http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf>,

U.S. Foreign Intelligence Surveillance Court, Memorandum Opinion, Oct. 3, 2011, p. 29
https://www.aclu.org/files/assets/fisc_opinion_10.3.2011.pdf.

In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 09-09, (FISA Ct. Aug. 13, 2009), *available at* http://www.dni.gov/files/documents/section/pub_August%2019%202009%20Report%20of%20the%20US%20with%20Attachments%2020130910.pdf.

In re Application of the Federal Bureau of Investigation for an Order Requiring the Prod. of Tangible Things From [REDACTED], Order at 4, No. BR 09-06 (FISA Ct. June 22, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Jun%2022%202009%20Order.pdf.

In re Prod. of Tangible Things From [REDACTED], No. BR 08-13, at 12 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

In re Prod. of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Feb. 17, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

In re Prod. of Tangible Things From [REDACTED], Order Regarding Preliminary Notice of Compliance Incident Dated Jan. 15, 2009, No. BR 08-13 (FISA Ct. Jan. 28, 2009), *available at* http://www.dni.gov/files/documents/section/pub_Jan%2028%202009%20Order%20Regarding%20Prelim%20Notice%20of%20Compliance.pdf.

In re Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Dec. 11, 2008), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf,

In re Directives to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008), *available at* <http://www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf>.

In re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Telecommunications Providers] Relating to [REDACTED], Order, No. BR 0605 (FISA Ct. May 24, 2006), *available at* https://www.eff.org/sites/default/files/filenode/docket_06-05_1dec201_redacted.ex_-_ocr_0.pdf.

In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F.Supp.2d 611 (Foreign Int.Surv.Ct. 2002), *available at* <http://www.fas.org/irp/agency/doj/fisa/fisc051702.html>.

In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) (No. 02-001), *available at* <https://www.fas.org/irp/agency/doj/fisa/092502sup.html>.

Motions before FISC:

ACLU's Foreign Intelligence Surveillance Court Motion, No. Misc. 13-02 (FISA Ct. 2013)

Yahoo's Foreign Intelligence Surveillance Court Motion, No. Misc 13-05 (FISA Ct. 2013) (challenging the classification of secret court documents);

Google's Foreign Intelligence Surveillance Court Motion, No. Misc. 13-03 (FISA Ct. 2013)

Microsoft's Foreign Intelligence Surveillance Court Motion, No. Misc. 13-04 (FISA Ct. 2013)

Facebook's Foreign Intelligence Surveillance Court Motion, No. Misc. 13-06 (FISA Ct. 2013)

Yahoo's Second Foreign Intelligence Surveillance Court Motion, No. Misc. 13-05 (FISA Ct. 2013)

LinkedIn's Foreign Intelligence Surveillance Court Motion, No. Misc. 13-07 (FISA Ct. 2013)

ACLU's second Foreign Intelligence Surveillance Court Motion, No. Misc. 13-08 (FISA Ct. 2013)

ProPublica's Foreign Intelligence Surveillance Court Motion, No. Misc. 13-09 (FISA Ct. 2013)

Challenges to NSA programs June 2013 – May 2014:

Am. Civil Liberties Union v. Clapper, No. 13-CV-3994 (S.D.N.Y. Oct. 10, 2013) (rejecting the government's argument that plaintiffs lack standing, rejecting plaintiffs' claims under the Administrative Procedure Act; accepting the government's statutory construction of section 215, and determining that *Smith v. Maryland* controls for Fourth Amendment purposes) [NB: Case currently on appeal]

Klayman v. Obama, No. 13-0881, 2013 WL 6598728 (D.D.C. 2013) (finding unconstitutional the Verizon Section 215 order) [NB: Case currently on appeal]

Klayman v. Obama, No. 13-0851, 2013 WL 6571596 (D.D.C. 2013) (challenging the NSA's PRISM surveillance program conducted under FISA Section 702)

Am. Civil Liberties Union v. Clapper, No. 13-CV-3994 (S.D.N.Y. Oct. 10, 2013) (challenging the Verizon Section 215 order)

Smith v. Obama, No. 2:13-CV-00257 (D. Idaho 2013) (challenging the Verizon Section 215 order)

Elec. Privacy Info. Ctr. Petition for a Writ of Mandamus, No. 13-58, (U.S. 2013) (challenging the Section 215 Verizon order) *See also In Re Electronic Privacy Information Center*, No. 13-58 (U.S. 2013) (denying petition for a writ of mandamus).

First Unitarian Church v. Nat'l Sec. Agency, No. 13-3287 (N.D. Cal. 2013) (challenging electronic surveillance)

Electronic Frontier Found. v. U.S. Dep't of Justice, No. 4:11-cv-05221-YGR, at 2, ¶1(b) (N.D. Cal. Jul. 19, 2013) (order responding to the request for records related to Section 215, i.e., orders and opinions of the FISC issued from January 1, 2004 to June 6, 2011, containing a significant legal interpretation of the government's authority or use of its authority under Section 215; and responsive "significant documents, procedures, or legal analyses incorporated into FISC opinions or orders and treated as binding by the Department of Justice or the National Security Agency")

Cases prior to June 2013:

Amnesty International v. McConnell (S.D.N.Y. 2009) (dismissing challenge to FAA on standing grounds), available at

http://www.aclu.org/files/pdfs/safefree/amnestyvmcconnell_opinionandorder.pdf

ACLU v. NSA, No. 06-CV-1024 (E.D. Mich., filed Jan. 17, 2006)

Center for Constitutional Rights v. Bush, No. 06-CV-00313 (S.D.N.Y., filed Jan. 17, 2006).

Hepting v. AT&T, No. C-06-0672-JCS (N.D. Ca, filed Jan. 31, 2006) (class action suit against AT&T and other telecoms providers for participating in the NSA surveillance programs)

CONGRESSIONAL RESEARCH SERVICE REPORTS:

ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF SELECTED ISSUES, (Cong. Research Service Rep. for Congress No. RL34279, Jul. 7, 2008), available at <http://www.fas.org/sgp/crs/intel/RL34279.pdf>.

Addresses tension between national security and civil liberties (particularly the rights of privacy and free speech), the need for efficient and effective foreign intelligence collection from non-U.S. persons located outside the United States (and differing approaches to meet this need), and limitations of liability for electronic communication service providers providing information to the federal government in support for foreign intelligence collection. Discusses Fourth and First Amendments in this context. [NB: This report is also published without the accompanying footnotes. See ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: A SKETCH OF SELECTED ISSUES, (Cong. Research Service Rep. for Congress No. RL34566, Jul. 7, 2008), available at <http://www.fas.org/sgp/crs/intel/RL34566.pdf>.]

ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: COMPARISON OF THE SENATE AMENDMENT TO H.R. 3773 AND THE HOUSE AMENDMENT TO THE SENATE AMENDMENT TO H.R. 3773, (Cong. Research Service Rep. for Congress No. RL34533, Jun. 12, 2008), available at <http://www.fas.org/sgp/crs/intel/RL34533.pdf>.

Discusses hearings and oversight conducted during the 110th Congress with regard to FISA and subsequent proposals to amend the legislation.

ELIZABETH B. BAZAN, P.L. 110-55, THE PROTECT AMERICA ACT OF 2007: MODIFICATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, (Cong. Research Service Rep. for Congress No. RL34143, Feb. 14, 2008), available at <http://www.fas.org/sgp/crs/intel/RL34143.pdf>.

Discusses alterations made to FISA by the PAA of 2007 and their potential impact on and parallels to existing law, as well as recent legislative developments.

ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: COMPARISON OF HOUSE-PASSED H.R. 3773, S. 2248 AS REPORTED BY THE SENATE SELECT COMMITTEE ON INTELLIGENCE, AND S. 2248 AS REPORTED OUT OF THE SENATE JUDICIARY COMMITTEE, (Cong. Research Service Rep. for Congress No. RL34277, Feb. 8, 2008), available at <http://www.fas.org/sgp/crs/intel/RL34277.pdf>.

Addresses competing bills designed to amend FISA, as well as and their legislative history.

ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF THE STATUTORY FRAMEWORK AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW DECISIONS, (Cong. Research Service Rep. for Congress No. RL30465, Feb. 15, 2007), available at <http://www.fas.org/sgp/crs/intel/RL30465.pdf>.

Comprehensive (103 page) report recounts the history of FISA and subsequent amendment of the statute via the 2001 USA PATRIOT Act, the 2002 Homeland Security Act, the 2002 Intelligence Authorization Act, the Intelligence Reform and Terrorism Prevention Act, the 2005 USA PATRIOT Improvement and Reauthorization Act, and the 2006 USA PATRIOT Act Additional Reauthorizing Amendments Act. Report also addresses FISC's publicly-available opinions as well as Exec. Order 12333. [NB: This report updates a previous summary. See ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF THE

STATUTORY FRAMEWORK AND RECENT JUDICIAL DECISIONS, CRS REPORT FOR CONGRESS (2004), *available at* <http://www.fas.org/irp/crs/RL30465.pdf>.]

ELIZABETH B. BAZAN, THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW: AN OVERVIEW, (Cong. Research Service Rep. for Congress No. RL33833, Jan. 24, 2007), *available at* <http://www.fas.org/sgp/crs/intel/RL33833.pdf>.

Summarizes the creation and operation of FISC and FISCR in light of TSP.

ELIZABETH B. BAZAN, FOREIGN INTELLIGENCE SURVEILLANCE ACT: SELECTED LEGISLATION FROM THE 108TH CONGRESS, (Cong. Research Service Rep. for Congress No. RL32608, Jan. 11, 2005), *available at* <http://www.fas.org/sgp/crs/intel/RL32608.pdf>.

Discusses impact of intelligence reform bills on FISA.

ELIZABETH B. BAZAN AND BRIAN T. YEH, INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004: “LONE WOLF” AMENDMENT TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, (Cong. Research Service Rep. for Congress No. RS22011, Dec. 19, 2006), *available at* <http://www.fas.org/sgp/crs/intel/RS22011.pdf>.

Discussing amendments to the definition of “agent of a foreign power” to include individuals engaged in international terrorism or activities in preparation therefor.

ELIZABETH B. BAZAN, GINA MARIE STEVENS, AND BRIAN T. YEH, GOVERNMENT ACCESS TO PHONE CALLING ACTIVITY AND RELATED RECORDS: LEGAL AUTHORITIES, (Cong. Research Service Rep. for Congress No. RL33424, Aug. 20, 2007), *available at* <http://www.fas.org/sgp/crs/intel/RL33424.pdf>.

Addresses recently-released public information about NSA collection programs and progress of related litigation, as well as statutory authorities regarding access by the government, for either foreign intelligence or law enforcement purposes, to information related to telephone calling patterns or practices.

RICHARD A. BEST, JR., THE NATIONAL SECURITY AGENCY: ISSUES FOR CONGRESS, (Cong. Research Service Rep. for Congress No. RL30740, Jan. 16, 2001), *available at* <http://www.fas.org/irp/crs/RL30740.pdf>

Discusses need for NSA to adapt to changing geopolitical and technological environment.

JARED P. COLE, ANDREW NOLAN, REFORM OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS: A BRIEF OVERVIEW, (Cong. Research Service Rep. for Congress No. R43451, Mar. 31, 2014), *available at* <http://www.fas.org/sgp/crs/intel/R43451.pdf>.

Addresses proposals related to changes to application procedures, as well as the practices and procedures of FISC and FISC-R.

CONGRESSIONAL RESEARCH SERVICE, THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW: AN OVERVIEW (Cong. Research Serv. No. RL33833, Jan. 24, 2007).

CHARLES DOYLE, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: LEGAL BACKGROUND, (Cong. Research Service Rep. for Congress No. RL33320, Jan. 3, 2014), *available at* <http://www.fas.org/sgp/crs/intel/RL33320.pdf>.

Discussing USA PATRIOT Act alterations to NSLs, the later DOJ IG reports, and subsequent amendment via the USA PATRIOT Improvement and Reauthorization Act, as well as further changes to NSLs recommended

by the President's Review Group on Intelligence and Communications Technologies. [NB: an abridged version of this report is also available. See CHARLES DOYLE, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE AT THE LEGAL BACKGROUND, (Cong. Research Service Rep. for Congress No. RS22406, Jan. 3, 2014), available at <http://www.fas.org/sgp/crs/intel/RS22406.pdf>.]

EDWARD C. LIU, REAUTHORIZATION OF THE FISA AMENDMENTS ACT, OVERVIEW (Cong. Research Serv. No. R42725, Apr. 8, 2013), available at <http://www.fas.org/sgp/crs/intel/R42725.pdf>.

Discussing H.R. 5949 (which extended Title VII of FISA until Dec. 31, 2017), and addressing the contours of Title VII, as well as the subsequent litigation.

EDWARD C. LIU, AMENDMENTS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) EXTENDED UNTIL JUNE 1, 2015, (Cong. Research Service Rep. for Congress No. R40138, Jun. 16, 2011), available at <http://www.fas.org/sgp/crs/intel/R40138.pdf>.

Discusses extension of three FISA-related provisions: USA PATRIOT Act Section 206 (amending FISA to permit roving wiretaps); USA PATRIOT Act Section 215 (tangible goods); and the Intelligence Reform and Terrorism Prevention Act Section 6001(a) (amending FISA to permit "lone wolf" targeting).

EDWARD C. LIU, RETROACTIVE IMMUNITY PROVIDED BY THE FISA AMENDMENTS ACT OF 2008, (Cong. Research Service Rep. for Congress No. RL34600, Jul. 25, 2008), available at <http://www.fas.org/sgp/crs/intel/RL34600.pdf>.

Discusses the arguments for and against retroactive immunity, the various retroactive immunity mechanisms proposed to be included in the FISA Amendments Act, and the likely effect of the mechanism adopted by Congress on lawsuits facing telecommunications providers.

EDWARD C. LIU AND CHARLES DOYLE, GOVERNMENT COLLECTION OF PRIVATE INFORMATION: BACKGROUND AND ISSUES RELATED TO THE USA PATRIOT ACT REAUTHORIZATION, Cong. Research Service Rep. for Congress No. R40980, Jun. 16, 2011), available at <http://www.fas.org/sgp/crs/intel/R40980.pdf>.

Discussing controversial aspects of the USA PATRIOT Act and exploring the arguments that undergirded support for and opposition to the measures.

EDWARD C. LIU, ANDREW NOLAN, RICHARD M. THOMPSON II, OVERVIEW OF CONSTITUTIONAL CHALLENGES TO NSA COLLECTION ACTIVITIES AND RECENT DEVELOPMENTS, Apr. 1, 2014, available at <http://www.fas.org/sgp/crs/intel/R43459.pdf>.

Notes judicial developments with regard to the NSA programs and discusses the constitutional challenges to the NSA's acquisition of Internet communications of overseas targets under FISA.

ANDREW NOLAN, FOREIGN SURVEILLANCE AND THE FUTURE OF STANDING TO SUE POST-CLAPPER, (Cong. Research Service Rep. for Congress No. R43107, Jul. 10, 2013), available at <http://www.fas.org/sgp/crs/intel/R43107.pdf>.

Re-visiting *Clapper* in light of the NSA documents released June/July 2013 and noting the myriad lawsuits filed in the immediate aftermath.

ANDREW NOLAN, RICHARD M. THOMPSON II, VIVIAN S. CHU, REFORM OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS: INTRODUCING A PUBLIC ADVOCATE, (Cong. Research Service Rep. for Congress No. R43260, Mar. 21, 2014), available at <http://www.fas.org/sgp/crs/intel/R43260.pdf>.

Considers the legal nature of the office of a public advocate, Article II's Appointments Clause, and Article III restrictions.

ANDREW NOLAN, RICHARD M. THOMPSON II, REFORM OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURTS: PROCEDURAL AND OPERATIONAL CHANGES, (Cong. Research Service Rep. for Congress No. R43362, Jan. 16, 2014), *available at* <http://www.fas.org/sgp/crs/intel/R43362.pdf>.

Discussing the potential admission of *amici curiae* for FISC hearings, the possibility of requiring FISC to sit en banc, and alterations to FISC's voting rules.

JOHN W. ROLLINS AND EDWARD C. LIU, NSA SURVEILLANCE LEAKS: BACKGROUND AND ISSUES FOR CONGRESS, (Cong. Research Service Rep. for Congress No. R43134, Sept. 4, 2013), *available at* <http://www.fas.org/sgp/crs/intel/R43134.pdf>.

Summarizing publicly-available information related to the Section 215 bulk metadata collection program and Section 702 upstream collection.

GINA STEVENS AND CHARLES DOYLE, PRIVACY: AN ABBREVIATED OUTLINE OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING, (Cong. Research Service Rep. for Congress No. 98-327, Oct. 9, 2012), *available at* <http://www.fas.org/sgp/crs/intel/98-327.pdf>.

Providing an overview of the Electronic Communications Privacy Act (including Title III, the Stored Communications Act, and criminal pen/trap provisions), as well as FISA.

Gina Stevens, Alison M. Smith, Jordan Seagall, *Memorandum to the Senate Intelligence Committee, Re: Legal Standard for Disclosure of Cell-Site Information and Geolocation Information*, June 29, 2010, *available at* <http://www.fas.org/sgp/crs/intel/crs-csi.pdf>.

Memorandum to Ron Wyden, discussing the legal framework for government requests for geolocation information held by private companies to find a customer's location.

CONGRESSIONAL HEARINGS AND TESTIMONY:

Senate Judiciary Committee Hearing on Continued Oversight of U.S. Government Surveillance Authorities, 113th Cong. (Dec. 11, 2013) (testimony of Deputy Attorney General James M. Cole, Director Keith B. Alexander and General Counsel Robert S. Litt), *available at* <http://www.justice.gov/iso/opa/dag/speeches/2013/dag-speech-131211.html>.

Senate Judiciary Committee Hearing on Continued Oversight of U.S. Government Surveillance Authorities, 113th Cong. (Dec. 10, 2013).

Senate Judiciary Committee Hearing on NSA Spying, 113th Cong. (Nov. 21, 2013).

Senate Judiciary Committee Hearing on Transparency Issues, 113th Cong. (Nov. 13, 2013).

House Intelligence Committee Hearing on FISA/NSA Program, 113th Cong. (Oct. 29, 2013).

Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. On the Judiciary, 113th Cong. (2013) (statement of Laura K. Donohue, Professor of Law, Georgetown University Law Center)

Senate Intelligence Committee Hearing, 113th Cong. (Sept. 26, 2013) (note classified/public sessions).

Hearing of the Senate Select Committee on Intelligence, Chaired by Senator John D. Rockefeller IV (D-WV), Nomination of J. Patrick Rowan to be Assistant Attorney General for National Security, Sept. 25, 2008 (discussing Section 702).

Senate Judiciary Committee Hearing on NSA surveillance, 113th Cong. (July 31, 2013)

House Permanent Select Committee on Intelligence, How Disclosed NSA Programs Protect Americans and Why Disclosure Aids our Adversaries, Chaired by Rep. Michael J. “Mike” Rogers, June 18, 2013 (testimony of Gen. Keith Alexander, Deputy Atton’y Gen. James Cole, NSA Deputy Dir. John Chris Inglis, FBI Deputy Dir. Sean Joyce, General Counsel Office of the Director of National Intelligence Robert Litt); *House Judiciary Committee Hearing on NSA programs*, 113th Cong. (July 17, 2013).

Senate Appropriations Committee Hearing, 113th Cong. (June 12, 2013) (testimony of Gen. Keith Alexander)(testimony of Acting Deputy Homeland Security Secretary Rand Beers; Acting Deputy Commerce Secretary Patrick Gallagher, Director of the National Institute of Standards and Technology; Richard McFeely, Exec. Asst. Dir. Of the Fed. Bureau of Investigation’s Criminal, Cyber, Response and Services Branch).

How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the H. Permanent Select Comm. on Intelligence, 113th Cong. (2013) (statement of James Cole, Deputy Att’y Gen.), available at <http://intelligence.house.gov/video/how-disclosed-nsa-programs-protect-americans-and-why-disclosure-aids-our-adversaries>

The Foreign Intelligence Surveillance Act: Hearing Before the H.R. Permanent Select Comm. on Intelligence., 110th Cong. (2007) (Statement of Kenneth L. Wainstein, Assistant Attorney General, National Security Division, Department of Justice), available at <http://www.justice.gov/archive/nsd/2007/wainstein-HPSCI-statement-9-20-07.pdf>.

Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intelligence, 110th Cong. (2007), available at http://www.fas.org/irp/congress/2007_hr/fisamod.pdf.

Reauthorizing the USA Patriot Act: Ensuring Liberty: Hearing Before Subcomm. on Administrative Oversight and the Courts of the S. Comm. on the Judiciary, 111th Cong. (2009), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_senate_hearings&docid=f:55610.pdf.

Restoring the Rule of Law: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary, 110th Cong. (2008), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_senate_hearings&docid=f:45240.pdf.

Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?: Hearing Before the S. Comm. on the Judiciary, 110th Cong. (2007), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_senate_hearings&docid=f:53358.pdf.

USA Patriot Act: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H.R. Comm. on the Judiciary, 111th Cong. (2009), available at http://judiciary.house.gov/hearings/printers/111th/111-35_52409.PDF.

Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights: Hearing Before the H.R. Comm. on the Judiciary, 110th Cong. (2007), available at <http://judiciary.house.gov/hearings/printers/110th/37599.PDF>.

Wartime Executive Powers and National Security Agency's Surveillance Authority: Hearing Before the S. Comm. on the Judiciary, 109th Cong. (2006) (Testimony of David S. Kris), available at http://judiciary.senate.gov/hearings/testimony.cfm?id=1825&wit_id=944.

ADDITIONAL SOURCES:

ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 2 (Aug. 9, 2013), available at <https://www.documentcloud.org/documents/750211-administration-white-paper-section-215.html>, [http://perma.cc/V7VM-5MAU]

U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 16–18 (2008), available at <http://www.justice.gov/ag/readingroom/guidelines.pdf>.

U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR FBI NATIONAL SECURITY INVESTIGATIONS AND FOREIGN INTELLIGENCE COLLECTION (2003), available at <http://www.fas.org/irp/agency/doj/fbi/nsiguideines.pdf>.

U.S. DEP'T OF JUSTICE, REPORT ON THE NATIONAL SECURITY AGENCY'S BULK COLLECTION PROGRAMS FOR USA PATRIOT ACT REAUTHORIZATION 5 (2011), available at http://www.dni.gov/files/documents/2011_CoverLetters_Report_Collection.pdf

Eric H. Holder, Jr., Att'y General of the United States, Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended 1 (Jan. 8, 2007), available at <http://epic.org/2013/06/nsa-targeting-and-minimization.html>

OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY, ST-06-0018, ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER: TELEPHONY BUSINESS RECORDS (see page 94 of 1846 and 1862 Production),

available at

http://www.dni.gov/files/documents/section/pub_Feb%2012%202009%20Memorandum%20of%20US.pdf.

REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, *available at*

http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.