AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

114TH CONGRESS 1ST SESSION/SENATE DOCUMENT 114–5

NATIONAL DEBATE TOPIC FOR HIGH SCHOOLS, 2015–2016

Resolved: The United States Federal Government Should Substantially Curtail Its Domestic Surveillance

NATIONAL DEBATE TOPIC FOR HIGH SCHOOLS, 2015–2016
Pursuant to 44 United States Code, Section 1333

Compiled by the Congressional Research Service
Library of Congress

114TH CONGRESS 1ST SESSION/SENATE DOCUMENT 114–5

NATIONAL DEBATE TOPIC FOR HIGH SCHOOLS, 2015–2016

Resolved: The United States Federal Government Should Substantially Curtail Its Domestic Surveillance

NATIONAL DEBATE TOPIC FOR HIGH SCHOOLS, 2015–2016
Pursuant to 44 United States Code, Section 1333

Compiled by the Congressional Research Service
Library of Congress

U.S. Government Publishing Office
Washington, DC 2015

CHAPTER 13—PARTICULAR REPORTS AND DOCUMENTS

Sec. 1333. National high school and college debate topics

(a) The Librarian of Congress shall prepare compilations of pertinent excerpts, bibliographical references, and other appropriate materials relating to:

(1) the subject selected annually by the National University Extension Association as the national high school debate topic and

(2) the subject selected annually by the American Speech Association as the national college debate topic.

In preparing the compilations the Librarian shall include materials which in his judgment are representative of, and give equal emphasis to, the opposing points of view on the respective topics.

(b) The compilations on the high school debate topics shall be printed as Senate documents and the compilations on the college debate topics shall be printed as House of Representative documents, the cost of which shall be charged to the congressional allotment for printing and binding. Additional copies may be printed in the quantities and distributed in the manner the Joint Committee on Printing directs.

(P.L. 90–620, Oct. 22, 1968, 82 Stat. 1270)

Historical and Revision Notes
Based on 44 U.S. Code, 1964 ed., Supp. III, Sec. 170 [Sec. 276a] (Dec. 30, 1963, Pub. L. 88–246, Secs. 1, 2, 77 Stat. 802)

CONTENTS

	Page
FOREWORD	V
INTRODUCTION	3
SUMMARY	3
BACKGROUND AND RECENT HISTORY OF U.S. DOMESTIC SURVEILLANCE	4
ARTICLES	4
BOOKS	8
GOVERNMENT REPORTS	10
THINK TANKS	12
WEBSITES	14
TYPES OF DOMESTIC SURVEILLANCE	14
ARTICLES	14
BOOKS	17
GOVERNMENT REPORTS	19
THINK TANKS	20
WEBSITES	21
LEGISLATION AND CASE LAW	22
STATUTES	22
BILLS/LEGISLATIVE ACTIVITY	25
CASE LAW	27
DOMESTIC SURVEILLANCE	29
ADVANTAGES	29
ARTICLES	29
BOOKS	30
THINK TANKS	31
WEBSITES	31
DISADVANTAGES	32
ARTICLES	32
BOOKS	33
THINK TANKS	34
SUBJECT BIBLIOGRAPHY	36

Foreword

The 2015-2016 high school debate topic is: "Resolved: The United States Federal Government Should Substantially Curtail Its Domestic Surveillance."

In compliance with 44 U.S.C., Section 1333, the Congressional Research Service (CRS) of the Library of Congress prepared this bibliography to assist high school debaters in researching the topic. This bibliography is intended to assist debaters in the identification of further references and resources on the topic. In selecting items for inclusion in this bibliography, CRS has sampled a wide spectrum of opinions reflected in the current literature on this issue. No preference for any policy is indicated by the selection or positioning of articles, books, or websites cited, nor is CRS disapproval of any policy, position, or article to be inferred from its omission.

The bibliography was prepared by Emily Carr, Elizabeth Schiller, Audrey Crane-Hirsch, Maria Kreiser, and Sundeep Mahendra, Law Librarians, Reference Librarians, and Digital Services Librarian, in the Knowledge Services Group of CRS and in the Law Library of Congress. Editorial assistance provided by Valerie Cervantes, Digital Services Librarian.

The project team leader was Jerry W. Mansfield, Lead Information Services Coordinator, Knowledge Services Group.

We wish the best to each debater as they research, prepare, and present arguments on this year's topic.

Mary B. Mazanec, Director
Congressional Research Service

NATIONAL DEBATE TOPIC FOR HIGH SCHOOLS, 2015-2016

RESOLVED: THE UNITED STATES FEDERAL GOVERNMENT SHOULD SUBSTANTIALLY CURTAIL ITS DOMESTIC SURVEILLANCE

AN ANNOTATED BIBLIOGRAPHY ON THE 2015-2016 HIGH SCHOOL DEBATE TOPIC

Compiled by
Audrey Crane-Hirsch, Maria Kreiser, Sundeep Mahendra, and Elizabeth Schiller - Reference Digital Services, and Law Librarians in the Knowledge Service Group of CRS and Emily Carr, Senior Legal Reference Librarian in the Law Library of Congress under the direction of project team leader Jerry W. Mansfield, Lead Information Services Coordinator, Knowledge Services Group
August 2015

Introduction

The 2015-2016 high school debate topic is: "Resolved: The United States Federal Government Should Substantially Curtail Its Domestic Surveillance." The topic is selected annually by ballot of the delegates from the National Catholic Forensic League, the National Debate Coaches Association, and the National Speech and Debate Association, all organized under the umbrella organization, the National Federation of State High School Associations.

The conflict between national security objectives and privacy became a popular topic for debate when it was disclosed in June 2013, by former defense contractor Edward Snowden, that the National Security Agency was engaging in extensive surveillance inside the United States in order to fight crime and to reduce the threat of terrorism. The magnitude of the disclosure shocked many people, including Members of Congress, who were unaware of the extent of the surveillance. Many civil rights advocates viewed the surveillance as an assault on liberty, while law enforcement and national security officials saw the programs as essential weapons in the war on terror, the fight against nuclear weapons proliferation, and the general protection of U.S. national security.

This selective bibliography, with brief annotations, is intended to assist debaters in identifying resources and references on the national debate topic. It lists citations to books, congressional publications, journal articles, legal cases, organizations, and websites. The bibliography is divided into four broad sections, "Background and Recent History of U.S. Domestic Surveillance," "Types of Domestic Surveillance," "Legislation and Case Law," and "Advantages and Disadvantages of Domestic Surveillance."

Summary

The purpose of the bibliography is to provide students with a brief overview of information related to the 2015-2016 high school debate topic.

This compilation is not intended to provide complete coverage of the topic. Further research on the topic may be accomplished at high school, research, depository, and public libraries.

In addition to the resources included in this bibliography, there are many more international organizations, U.S. Government agencies, private think tanks, and non-governmental organizations (NGOs) that provide information on the debate topic and sub-topics on their websites. Debaters are encouraged to consult the Internet as well as library resources for their research.

Background and Recent History of U.S. Domestic Surveillance

Articles

Bedi, Monu. "Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory." *Boston University Law Review*, vol. 94, no. 6 (December 2014): 1809-1880.
Applying mosaic theory to social networking communications over the Internet, this article examines the concept of associational rights as a key principle to the argument that social networking communications merit privacy protections.

Cassidy, Anne. "Who's Watching You?" *Georgetown Law Magazine* (Spring/Summer 2015): 20-30.
This article discusses the recent news about privacy issues and the public's increasing concern over data breaches, cybercrime, and government surveillance. The author speaks with experts about the demand for new forms of control over privacy and lawyers' potential roles in these emerging systems.

Hibbard, Christa M. "Wiretapping the Internet: The Expansion of the Communications Assistance to Law Enforcement Act to Extend Government Surveillance." *Federal Communications Law Journal*, vol. 64, no. 2 (2011-2012): 371-399.
Examines the competing interests related to expanding the Communications Assistance to Law Enforcement Act (CALEA), which was passed in 1994 to regulate telephone and broadband companies to ensure compliance with court orders. Part II provides a background of wiretap and surveillance law. The author argues that there is not sufficient information to justify an expansion to CALEA.

Joh, Elizabeth E. "Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion." *Arizona Law Review*, vol. 55, no. 1 (2013): 997-1030.
The author challenges the idea that those who evade surveillance are criminals. This article discusses the importance of small, ordinary acts of resistance that the author calls privacy protests, their place in constitutional criminal procedure, and their potential social value in the struggle over the meaning of privacy.

Lee, Timothy B. "The NSA's secrecy is bad for the NSA." *WashingtonPost.com* (June 19, 2013).
Available online at:
[http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/19/the-nsas-secrecy-is-bad-for-the-nsa/].
This article reports on the NSA's release of new information about privacy safeguards in its surveillance programs and asks: "Why wasn't this information made public years ago?" The author argues that the NSA hurts its own reputation and encourages the public to assume the worst when it keeps this information secret.

Michelman, Scott. "Who Can Sue Over Government Surveillance." *UCLA Law Review*, vol. 57, no. 1 (October 2009): 71-114.
The author argues that the Supreme Court's 1972 decision in Laird v. Tatum and general principles of standing law form a coherent doctrine under which courts can adjudicate important constitutional questions about government surveillance regimes.

Nakashima, Ellen. "Court Ruling Boosts Case for Ending Collection of U.S. Phone Records." *WashingtonPost.com* (May 8, 2015).
Available online at: [https://www.washingtonpost.com/world/national-security/court-ruling-could-undermine-political-support-for-nsa-surveillance-program/2015/05/08/f6245228-f5ac-11e4-bcc4-e8141e5eb0c9_story.html].
This article reports on the landmark ruling by a federal appeals court in New York, which found that the National Security Agency's collection of millions of Americans' phone records was unlawful.

Peterson, Andrea. "Obama Says NSA Has Plenty of Congressional Oversight. But One Congressman Says It's a Farce." *WashingtonPost.com* (October 9, 2013).
Available online at: [http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/09/obama-says-nsa-has-plenty-of-congressional-oversight-but-one-congressman-says-its-a-farce/].
In reporting on concerns over congressional oversight of intelligence programs, this article discusses the oversight Congress has over these programs and the effectiveness of that oversight.

Priest, Dana. "Government Surveillance Spurs Americans to Fight Back." *WashingtonPost.com* (August 14, 2013).
Available online at: [http://www.washingtonpost.com/lifestyle/style/government-surveillance-spurs-americans-to-fight-back/2013/08/14/edea430a-0522-11e3-a07f-49ddc7417125_story.html].
Designers are fighting back against government surveillance by creating fashion that blocks eavesdropping, confuses cameras, and thwarts drones. The author discusses how these designs provoke conversations about government surveillance programs.

Risen, Tom. " 'Patriot Act' Author Seeks 'USA Freedom Act' to Rein in NSA." *USNews.com* (October 10, 2013).
Available online at: [http://www.usnews.com/news/articles/2013/10/10/patriot-act-author-seeks-usa-freedom-act-to-rein-in-nsa].
This article reports on the 2013 debates over legislation to end bulk data collection by the National Security Agency. Specifically, it discusses the Freedom Act and the challenges it faces from both parties.

Sasso, Brendan. "Rep. Amash: Intelligence Committees Undermine Oversight." *TheHill.com* (October 9, 2013).
Available online at: [http://thehill.com/policy/technology/327603-rep-amash-intelligence-committees-undermine-oversight].
The author reports on criticisms of Congressional committees in the debates over Congress's role in controversies over intelligence agencies' actions.

Sasso, Brendan. "Sen. Wyden Vows to Battle 'Skin Deep' NSA Reforms." *TheHill.com* (October 9, 2013).
Available online at: [http://thehill.com/policy/technology/327497-sen-wyden-vows-to-battle-skin-deep-nsa-reforms].
The author discusses the October 2013 legislative debates over proposals to ratify NSA's surveillance programs. It covers the controversies surrounding several different programs as well as critiques of the programs' potential effectiveness.

Sasso, Brendan and Kate Tummarello. "Patriot Act Author Preps Freedom Act to Rein in NSA." *TheHill.com* (October 9, 2013).
Available online at: [http://thehill.com/policy/technology/327637-overnight-tech-patriot-act-author-preps-freedom-act-to-rein-in-nsa].
Mr. Sasso continues coverage of the October 2013 debates over legislation to rein in surveillance programs.

Schwarz, Hunter. "NSA: The 2016 Issue that Defies Partisanship." *WashingtonPost.com* (May 8, 2015).
Available online at: [http://www.washingtonpost.com/blogs/the-fix/wp/2015/05/08/nsa-the-issue-that-unites-hillary-clinton-with-ted-cruz/].
The author reports on the New York federal appeals court ruling that held mass collection of phone records by the NSA to be illegal. Responses from 2016 presidential hopefuls are included. According to the author, declared and potential 2016 candidates were silent or about this major ruling.

Semitsu, Junichi P. "From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance." *Pace Law Review*, vol. 31, no. 1 (Winter 2011): 291-381.
Social media users in the United States lack a reasonable expectation of privacy from government surveillance of virtually all of their online activity, despite many platforms' privacy settings. The author believes this is a problem and wants to call attention to it.

Shamsi, Hina and Alex Abdo. "Privacy and Surveillance Post-9/11." *Human Rights Magazine*, vol. 38, no. 1 (Winter 2011).
Available online at:
[http://www.americanbar.org/publications/human_rights_magazine_home/human_rights_vol38_2011/human_rights_winter2011/privacy_and_surveillance_post_9-11.html].
As director of the American Civil Liberties Union's National Security Project and staff attorney with the National Security Project, respectively, the authors briefly describe how new technology that promises to deliver ease and connectivity also permits mass government surveillance and data mining. They explore how a structural failure of the

nation's system of checks and balances has permitted the erosion of Americans' privacy rights.

The Hill Staff. "Cybersecurity Hinges on Surveillance Understanding, NSA Director Says." *TheHill.com* (October 9, 2013).
Available online at: [http://thehill.com/policy/technology/327623-cybersecurity-hinges-on-surveillance-understanding-nsa-director-says].
The National Security Agency's Director stated that there is no way the intelligence community can be more transparent.

"U.S. Court Rules NSA Mass Surveillance Illegal." *Amnesty International USA* (May 7, 2015).
Available online at: [http://www.amnestyusa.org/news/press-releases/us-court-rules-nsa-mass-surveillance-illegal].
A press release by Amnesty International announces that the U.S. government's mass surveillance of communications received a major setback when a court of appeals ruled that the National Security Agency's bulk collection of phone records was illegal.

Zaru, Deena. "Dilemmas of the Internet Age: Privacy vs. Security." *CNNPolitics.com* (March 29, 2014).
Available online at: [http://www.cnn.com/2015/02/04/politics/deena-zaru-internet-privacy-security-al-franken/].
This article looks at the dilemmas of the Internet age in a world of smart phones and smart cars, where the Internet follows you wherever you go.

Background and Recent History of U.S. Domestic Surveillance

Books

Arnold, Jason Ross. *Secrecy in the Sunshine Era: The Promise and Failures of U.S. Open Government Laws*. Lawrence, KS: University Press of Kansas, 2014.
A series of laws passed in the 1970s promised the nation unprecedented transparency in government, a veritable "sunshine era." Though citizens enjoyed a new arsenal of

secrecy-busting tools, officials developed a handy set of workarounds, from overclassification to concealment, shredding, and burning. Jason Ross Arnold explores this "dark side" of the sunshine era in a comparative history of presidential resistance to the new legal regime.

Glennon, Michael J. *National Security and Double Government*. New York, NY: Oxford University Press, 2014.
Michael J. Glennon challenges the myth that U.S. security policy is still forged by America's visible "Madisonian institutions" – the President, Congress, and the courts. Their roles, he argues, have become largely illusory, ceding power to a concealed "Trumanite network" – the several hundred managers of the military, intelligence, diplomatic, and law enforcement agencies responsible for protecting the nation, who have come to operate largely immune from constitutional and electoral restraints.

Goldfarb, Ronald, Hodding Carter, David Cole, Thomas S. Blanton, Jon Mills, Barry Seigel, and Edward Wasserman. *After Snowden: Privacy, Secrecy, and Security in the Information Age*. New York, NY: Thomas Dunne Books, 2015.
Includes seven essays by legal and political scholars examining the ramifications of Edward Snowden's information leak. The essays examine questions including: Was Edward Snowden a patriot or a traitor? Just how far do American privacy rights extend? And how far is too far when it comes to government secrecy in the name of security?

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York, NY: Metropolitan Books, 2014.
Journalist Greenwald recounts his meeting with an anonymous source who turned out to be NSA contractor and whistleblower Edward Snowden. Greenwald examines the broader implications of the surveillance detailed in his reporting for *The Guardian* and reveals fresh information on the NSA's unprecedented abuse of power.

Richards, Neil. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. New York, NY: Oxford University Press, 2015.
In this book, Richards argues that when privacy and free speech truly conflict, free speech should almost always win. Only when disclosures of truly horrible information

are made should privacy be able to trump our commitment to free expression. Richards argues that speech and privacy are only rarely in conflict.

Background and Recent History of U.S. Domestic Surveillance

Government Reports

Doyle, Charles. CRS Report R41733. *Privacy: An Overview of the Electronic Communications Privacy Act.* Washington, D.C.: Congressional Research Service.[1]
This report to Congress provides an overview of the Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA). ECPA consists of three parts. The first, often referred to as Title III, outlaws wiretapping and electronic eavesdropping, except as otherwise provided. The second, the Stored Communications Act, governs the privacy of, and government access to, the content of electronic communications and related records. The third outlaws the use and installation of pen registers and trap and trace devices, unless judicially approved for law enforcement or intelligence-gathering purposes.

Liu, Edward C., Andrew Nolan, and Richard M. Thompson II. CRS Report R43459. *Overview of Constitutional Challenges to NSA Collection Activities.* Washington, D.C.: Congressional Research Service.
This report provides a brief overview of the two main NSA collection activities approved by the Foreign Intelligence Surveillance Court (FISC). The first is the bulk collection of telephony metadata for domestic and international telephone calls. The second involves the interception of Internet-based communications; while targeted at foreigners outside the United States, it may also inadvertently acquire the communications of U.S. persons. The report examines the various constitutional challenges that have arisen in judicial forums with respect to each.

[1] Congressional Research Service reports are available by way of a request to your Member of Congress. You may find your House of Representatives Member at http://clerk.house.gov or your U.S. Senator at http://www.senate.gov/senators/contact.

Stevens, Gina and Charles Doyle. CRS Report 98-326. *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping.* Washington, D.C.: Congressional Research Service.
An overview of the Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA). The report includes the text of the two acts and appendices listing the citations to state statutes that correspond to various aspects of ECPA.

Theohary, Catherine A. and Edward C. Liu. CRS Report R43134. *NSA Surveillance Leaks: Background and Issues for Congress.* Washington, D.C.: Congressional Research Service.
This report clarifies the differences between two intelligence collection programs that recently received attention in the investigations into NSA surveillance and unauthorized disclosures: the program that collects phone records in bulk and the program targeting electronic communications of foreign targets overseas whose communications flow through American networks.

Thompson II, Richard M. CRS Report R43965. *Domestic Drones and Privacy: A Primer.* Washington, D.C.: Congressional Research Service.
A primer on privacy issues related to various unmanned aircraft systems (UAS) operations, both public and private, including an overview of current UAS uses, the privacy interests implicated by these operations, and various potential approaches to UAS privacy regulation. The report discusses two overarching privacy issues implicated by domestic drone flights and makes clear that understanding privacy rights vis-à-vis drones is not as simple as applying Supreme Court case law or federal and state statutes.

Thompson II, Richard. CRS Report R42701. *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses.* Washington, D.C.: Congressional Research Service.
This report provides a more in-depth look at privacy and drones. It addresses the use of drones under the Fourth Amendment right to be free from unreasonable searches and seizures. While individuals may expect substantial protections against warrantless government intrusions into their homes, the Fourth Amendment offers less robust

restrictions upon government surveillance occurring in public places, including areas immediately outside the home such as driveways or backyards.

Background and Recent History of U.S. Domestic Surveillance

Think Tanks

American Civil Liberties Union.
Available online at: [https://www.aclu.org/].
For almost 100 years, the ACLU has worked to defend and preserve the individual rights and liberties guaranteed by the Constitution and laws of the United States. The ACLU's Privacy and Technology project (available online at: [https://www.aclu.org/issues/privacy-technology]) works to expand the right to privacy, increase the control individuals have over their personal information, and ensure civil liberties are enhanced rather than compromised by technological innovation.

Center for Democracy & Technology.
Available online at: [https://cdt.org/].
The Center for Democracy & Technology (CDT) is a 501(c)(3) nonprofit organization that works to preserve the user-controlled nature of the Internet and champion freedom of expression. The CDT supports laws, corporate policies, and technology that protect the privacy of Internet users, and advocates for stronger legal controls on government surveillance.

Center on Privacy & Technology at Georgetown Law.
Available online at: [http://www.law.georgetown.edu/academics/centers-institutes/privacy-technology/].
The Center on Privacy & Technology is a think tank that aims to bridge the gap between the policy and academic worlds on privacy. It also trains Georgetown University Law students to be leaders in privacy practice, policymaking, cybersecurity law, and advocacy. Privacy issues presented by the technologies that digitize our "offline" selves, such as health apps, "wearables," and biometric identification techniques, and the

implications of Big Data techniques on civil rights and vulnerable communities are concerns of this think tank.

Liberty, Privacy & Surveillance Advocacy at the American Library Association.
Available online at: [http://www.ala.org/advocacy/privacyconfidentiality].
The American Library Association's (ALA) extensive First Amendment, liberty, and privacy principles guide the association's work in the federal legislative and policy arenas as well as at the state and local levels in order to protect personal privacy based upon a longstanding commitment to patron privacy. Advancing the library community's principles to protect patron confidentiality requires major grassroots work from the library community to promote library priorities in these environments. There are several divisions of ALA that work on these important issues: the Surveillance, Privacy, Open Government and Constitutional Rights group, the Office for Intellectual Freedom, and the Office of Government Relations.

Open Technology Institute at the New America Foundation.
Available online at: [https://www.newamerica.org/oti/].
The Open Technology Institute strengthens communities through research, technological innovation, and policy reform. It creates reforms to support open source innovations and foster open technologies and communications networks. Partnering with communities, researchers, and industry and public interest groups, they promote affordable, universal, and ubiquitous communications networks.

Sunlight Foundation.
Available online at: [http://sunlightfoundation.com/].
The Sunlight Foundation is a national, nonpartisan, nonprofit organization that uses the tools of open data, policy analysis, and journalism to make our government and politics more accountable and transparent to all. Their vision is to use technology to enable more complete, equitable, and effective democratic participation.

Background and Recent History of U.S. Domestic Surveillance

Websites

Council on Foreign Relations. 2013. "U.S. Domestic Surveillance."
Available online at: [http://www.cfr.org/intelligence/us-domestic-surveillance/p9763].
The website discusses the rise of domestic surveillance under the Bush Administration and the challenges to domestic surveillance policy today. Includes an interactive guide by *The Guardian* that attempts to explain the findings from the Snowden leaks.

Types of Domestic Surveillance

Articles

Betts, Jennifer and Sakir Sezer. "Ethics and Privacy in National Security and Critical Infrastructure Protection." *2014 IEEE International Symposium on Ethics in Science, Technology and Engineering* (May 2014): 1-7.
This paper highlights the importance of ethical principles in the design of critical infrastructure network protection systems, focusing on privacy and data protection explanations and perspectives.

Boghosian, Heidi. "The Business of Surveillance." *Human Rights*, vol. 39, no. 3 (March 2013): 2-5, 23.
In addition to engaging in data mining, multinational companies are employing sophisticated technology, such as radio frequency identification (RFID) chips, semiconductors, and chips that can be configured to allow law enforcement "back door" access to monitor communications or that enable location-based services to track citizens' whereabouts. Under the Patriot Act, a host of personal records – from medical to magazine subscriptions – are available to the FBI if an agent claims they are sought for an "authorized investigation" related to international terrorism. Since the advent of the Total Information Awareness program, data mining has been the go-to method of domestic spying.

Cayford, Michelle, Coen van Gulijk, and P.H.A.J.M van Gelder. "When Counting is Not Enough: Limitations of NSA's Effective Assessment of Surveillance Technology." *2014 IEEE Joint Intelligence and Security Informatics Conference (JISIC)* (September 2014).
The NSA has justified its surveillance programs by citing the number of terrorist activities these programs disrupted. This paper finds this method of measuring the effectiveness of surveillance technology short-sighted, arguing that it is only one measure of effectiveness and should not be used in isolation.

Clement, Andrew. "IXmaps – Tracking Your Personal Data through the NSA's Warrantless Wiretapping Sites." *2013 IEEE International Symposium on Technology and Society (ISTAS)* (June 2013).
This paper reports on the development of the IXmaps interactive mapping application designed to show Internet users how their personal traffic may be intercepted by the NSA. It also discusses the potential for this mapping technique to serve as a tool for achieving better public understanding of surveillance in the Internet core.

Gao, George. "What Americans Think About NSA Surveillance, National Security and Privacy." (May 29, 2015).
Available online at: [http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/].
Explores government surveillance programs and opinions of Americans on security versus civil liberties.

Conti, Greg, Lisa Shay, and Woodrow Hartzog. "Deconstructing the Relationship Between Privacy and Security." *IEEE Technology and Society Magazine*, vol. 33, no. 2 (Summer 2014): 28-30.
This article explores the relationship between privacy and security and seeks to debunk the notion that privacy and security trade-offs are effective or even necessary.

Geer, Daniel E. "Personal Data and Government Surveillance." *IEEE Security Privacy*, vol. 12, no. 4 (July-August 2014): 90-96.
The author discusses data acquisition as the core issue in cybersecurity, the professionalization of cybersecurity, and personal data and the government.

Konheim, Alan G. "To Let Them Monitor or Not ... Perhaps that is *Not* the Real Question." *IEEE Technology and Society Magazine*, vol. 33, no. 3 (Fall 2014): 9-13.
We learn that the NSA may be interfering with secured Internet transactions by using a backdoor attack, "a method of bypassing normal authentication, securing illegal remote access to a computer, obtaining access to plaintext, and more while attempting to remain undetected."

McCutcheon, Chuck. "Government Surveillance: Is Government Spying on Americans Excessive?" *CQ Researcher by CQ Press*, vol. 23-30 (August 2013).
This article discusses surveillance measures, including the use of unmanned "drone" aircraft and tiny video cameras, and claims that internal safeguards – including a federal civil liberties oversight board created in 2004 – has prevented the federal government from becoming "Big Brother."

Miller, Keith W. "A Secret Sociotechnical System." *IT Professional*, vol. 15, no. 4 (July 2013): 57-59.
Sociotechnical systems and the potential implications and social outcomes of governmental metadata collection are explained.

Mulligan, Deirdre K. "The Enduring Importance of Transparency." *IEEE Security Privacy*, vol. 12, no. 3 (May-June 2014): 61-65.
The Ware report's[2] recommendation that there be no secret government system of records containing personal information about individuals has renewed urgency. The Ware report continues to hold its place as the first principle of fairness in the Code of Fair Information Practices.

Pfleeger, Shari L. "The Eyes Have It: Surveillance and How It Evolved." *IEEE Security Privacy*, vol. 12, no. 4 (July 2014): 74-79.
A brief history of surveillance, technological and otherwise, is presented. It includes a discussion of some of the issues technologists should consider when building software

[2] Dr. Willis Ware's report, "Records, Computers and the Rights of Citizens," became the foundation of the Privacy Act of 1974. The Privacy Act is the most comprehensive privacy law ever enacted in the United States.

and hardware to capture and analyze personal characteristics, habits, movements, and more.

Rash, Wayne. "Think Tank Warns U.S. Surveillance Efforts Undermine IT Industry." *eWEEK.com* (December 10, 2014).
Available online at: [http://www.eweek.com/security/think-tank-warns-u.s.-surveillance-efforts-undermine-it-industry.html].
This article discusses the effects of the current state of surveillance involving U.S. software, cloud, and hardware companies, with particular focus on the recent Microsoft case.

Sobel, Richard. "The Right to Travel and Privacy: Intersecting Fundamental Freedoms." *Journal of Information Technology & Privacy Law*, vol. 30, no. 4 (2014).
Available online at:
[http://repository.jmls.edu/cgi/viewcontent.cgi?article=1746&context=jitpl].
In a discussion of mechanisms of travel surveillance, the author argues that the requirement of official photo identification for travel, watch-list prescreening programs, and invasive airport scans and searches unreasonably burden the right to travel.

Types of Domestic Surveillance

Books

Bellaby, Ross. *Ethics and Intelligence Collection: A New Framework*. New York, NY: Routledge, 2014.
This book discusses types of intelligence and ethical frameworks for intelligence gathering.

Boon, Kristen and Douglas C. Lovelace. *The Drone Wars of the 21st Century: Costs and Benefits*. Oxford, UK: Oxford University Press, 2014.
Covers how drones are beginning to be used domestically for law enforcement purposes.

Clarke, Richard A., Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter P. Swire. *The NSA Report: Liberty and Security in a Changing World*. Princeton, NJ:

Princeton University Press, 2014.
The authors examine the extent of NSA surveillance programs and call for dozens of urgent and practical reforms. The result is a blueprint showing how the government can reaffirm its commitment to privacy and civil liberties – without compromising national security.

Cohen, Elliot D. *Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance*. New York, NY: Palgrave Macmillan, 2014.
This book offers a systematic analysis of mass surveillance in America, along with policy changes and software developments necessary to establish an Internet-based, global forum for transparency affecting legal and technological change.

Deibert, Ronald, Canadian Defence and Foreign Affairs Institute, and Canadian International Council. *Shutting the Backdoor: The Perils of National Security and Digital Surveillance Programs.* Toronto, Canada: Canadian Defence and Foreign Affairs Institute, 2013.
Available online at: [http://opencanada.org/wp-content/uploads/SL13CIC018-SSWGP-Deibert-v3.pdf].
As governments have sought to monitor digital communications for security purposes, the "backdoor" paradigm has become the predominant approach. The "backdoor" concept is used to describe the way in which governments compel or get the cooperation of private sector companies to provide access to the data they control.

Engdahl, Sylvia. *Domestic Wiretapping*. Farmington Hills, MI: Greenhaven Press, 2008.
Describes how wiretapping works and explores the various controversies surrounding it.

Engelhardt, Tom. *Shadow Government: Surveillance, Secret Wars, and a Global Security State in a Single Superpower World*. Chicago, IL: Haymarket Books, 2014.
This book discusses how national security concerns of the past have morphed into global security issues.

Kirchner, Richard. *Surveillance and Threat Detection Prevention Versus Mitigation*. Waltham, MA: Butterworth-Heinemann, 2014.
Available online at: [http://www.books24x7.com/marc.asp?bookid=62201].

Terrorists and criminals often rely on pre-attack and pre-operational planning and surveillance activities that can last a period of weeks, months, or even years. This book discusses how identifying and disrupting this surveillance is key to preventing attacks.

Kraft, Michael and Edward Marks. *U.S. Government Counterterrorism: A Guide to Who Does What*. Boca Raton, FL: CRC Press, 2012.
This is a guide to the many U.S. government agencies, bureau offices, and programs involved in all aspects of countering terrorism domestically and overseas.

Kreitner, Richard. *Surveillance Nation: Critical Reflections on Privacy and its Threats: Articles from the Nation, 1931 – the Present.* New York, NY: The Nation, 2014.
A collection of writings on the rise of the surveillance state in the U.S. since post-WWI is presented.

Segrave, Kerry. *Wiretapping and Electronic Surveillance in America, 1862-1920.* Jefferson, NC: McFarland & Company, Inc. Publishers, 2014.
Available online at: [http://public.eblib.com/choice/PublicFullRecord.aspx?p=1774278].
Following Edward Snowden's revelations in 2013, Americans have come to realize that they may be under surveillance at any time. It all started 150 years ago on the battlefields of the Civil War, where each side tapped the other's telegraph lines. The history of surveillance through 1920 is discussed.

Thompson, Tamara. *Domestic Surveillance*. Farmington Hills, MI: Greenhaven Press, 2015.
The author presents a collection of writings on types of domestic surveillance and essays on its effects on privacy, the economy, and government transparency.

Types of Domestic Surveillance

Government Reports

U.S. Government Accountability Office. 2014. GAO Report 14-796T. *Secure Flight: Additional Actions Needed to Determine Program Effectiveness and Strengthen Privacy*

Oversight Mechanisms. Washington, D.C.: U.S. Government Accountability Office.
Available online at: [http://www.gao.gov/products/GAO-14-796T].
This article discusses and critiques the Transportation Security Administration's (TSA) Secure Flight program and processes in place to implement Secure Flight screening determinations.

U.S. Government Accountability Office. 2012. GAO Report 12-981. *Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System.* Washington, D.C.: U.S. Government Accountability Office.
Available online at: [http://www.gao.gov/products/GAO-12-981].
This report discusses the status of obstacles identified in GAO's 2008 report to integrate unmanned aircraft systems (UAS) into the national airspace system, the FAA's progress in meeting its congressional requirements for UAS, and emerging issues.

U.S. Government Accountability Office. 2012. GAO Report 12-889T. *Unmanned Aircraft Systems: Use in the National Airspace System and the Role of the Department of Homeland Security*. Washington, D.C.: U.S. Government Accountability Office.
Available online at: [http://www.gao.gov/products/GAO-12-889T].
This report discusses obstacles identified in GAO's previous report on the safe and routine integration of UAS into the national airspace, and DHS's role in the domestic use of these systems.

Types of Domestic Surveillance

Think Tanks

Digital Due Process.
Available online at: [http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163].
Digital Due Process is a diverse coalition of privacy advocates, major companies, and think tanks, working together to provide stronger privacy protections in communications.

Electronic Frontier Foundation (EFF).
Available online at: [https://www.eff.org/].
Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development.

EPIC - Electronic Privacy Information Center.
Available online at: [https://www.epic.org/].
EPIC works to protect privacy, freedom of expression, and democratic values, and to promote the public's voice in decisions concerning the future of the Internet.

Future of Privacy.
Available online at: [http://www.futureofprivacy.org/].
The Future of Privacy Forum (FPF) is a Washington, D.C.-based think tank that seeks to advance responsible data practices.

Global Commission on Internet Governance.
Available online at: [https://www.ourinternet.org/].
The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance.

Progress and Freedom Foundation.
Available online at: [http://www.pff.org/].
The Progress and Freedom Foundation is a market-oriented think tank that studies the digital revolution and its implications for public policy.

Types of Domestic Surveillance

Websites

Currier, Cora, Justin Elliott, and Theodoric Meyer. 2013. "Mass Surveillance in America: A Timeline of Loosening Laws and Practices." ProPublica.
Available online at: [https://projects.propublica.org/graphics/surveillance-timeline].
Includes a list of surveillance activities from a patchwork of official statements, classified documents, and anonymously sourced news stories.

Democracy Now! "Domestic Surveillance."
Available online at: [http://www.democracynow.org/topics/domestic_surveillance].
Democracy Now! (a national daily independent news program) provides stories, posts, and pages that relate to domestic surveillance.

Electronic Frontier Foundation. "How the NSA's Domestic Spying Program Works."
Available online at: [https://www.eff.org/nsa-spying/how-it-works].
Background on NSA's domestic spying program, known in official government documents as the "President's Surveillance Program."

Stray, Jonathan. 2013. "FAQ: What You Need to Know about the NSA's Surveillance Programs." ProPublica.
Available online at: [http://www.propublica.org/article/nsa-data-collection-faq].
This online story contains a list of several secret NSA collection programs that have been revealed.

Legislation and Case Law

Statutes

Foreign Intelligence Surveillance Act, Public Law No. 95-511, 92 Stat. 1783 (1978).
Available online at: [http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf].
Enacted in response to congressional Church Committee[3] investigations of federal surveillance activities, FISA permitted the President, acting through the Attorney General, to authorize electronic surveillance for foreign intelligence purposes without a court order in certain circumstances. The act established a court of review for surveillance applications, and specified the terms of the *ex parte* orders. The Attorney

[3] The Church Committee was the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, chaired by Senator Frank Church (D-ID) in 1975. A precursor to the U.S. Senate Select Committee on Intelligence, the committee investigated intelligence gathering for illegality by the Central Intelligence Agency, National Security Agency, and Federal Bureau of Investigation after certain activities had been revealed by the Watergate affair.

General was required to report instances of such applications, with a Report to Congress on its implementation. Additionally, the statute provided for both penalties to unauthorized persons conducting surveillance and civil liability to aggrieved persons.

Electronic Communications Privacy Act, Public Law No. 99-508, 100 Stat. 1848 (1986). Available online at: [http://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf].
Introduced by Rep. Kastenmeier, the enacted legislation extended the prohibition against unauthorized interception of communications to include specific types of electronic communication. Prohibited access to stored communications (see Public Law No. 99-508 below) and the installation or use of a pen register or a trap and trace device without a court order. Imposed criminal penalties for violations.

Stored Communications Act, Public Law No. 99-508, Title II, 100 Stat. 1860 (1986). Available online at: [http://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf].
A provision of the ECPA, Title II, explicitly prohibited access to stored communications without authorization and the disclosure of such content. It prescribed the terms under which governmental entities could require the disclosure, for communication in storage for 180 days or less. Without notifying the customer, a governmental entity could require a service provider to create a backup for its use. Customers could challenge such action within 14 days after notice. Notification could be delayed up to a period not to exceed 90 days if it was determined that the notice would result in adverse results.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Public Law No. 107-56, 115 Stat. 272 (2001).
Available online at: [http://www.gpo.gov/fdsys/pkg/STATUTE-115/pdf/STATUTE-115-Pg272.pdf].
Introduced by Rep. Sensenbrenner, the USA PATRIOT Act, “To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes,” was enacted in response to 9/11. The Act authorized measures for enhancing domestic security and surveillance procedures and

increased northern border protection. Provisions addressed certain obstacles to investigating terrorism, providing aid to terrorism victims and their families, expanding regional networks to share information related to terrorism attacks, strengthening criminal law provisions, and recommending measures to improve intelligence gathering.

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Public Law No. 110-261, 122 Stat. 2436 (2008).
Available online at: [http://www.gpo.gov/fdsys/pkg/PLAW-110publ261/pdf/PLAW-110publ261.pdf].
Introduced by Rep. Reyes, the FISA of 1978 Amendments Act of 2008 amended FISA by authorizing, "for periods up to one year, the targeting (electronic surveillance) of persons located outside the United States in order to acquire foreign intelligence information, under specified limitations." The act prohibited federal or civil actions against any person (including an electronic communication service provider or a landlord or custodian) providing surveillance assistance to an intelligence community member if certified by the Attorney General, under certain conditions.

Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA FREEDOM) Act of 2015, Public Law No. 114-23, 129 Stat. 268 (2015).
Available online at: [https://www.congress.gov/bill/114th-congress/house-bill/2048/text].
Introduced by Rep. Sensenbrenner, the USA FREEDOM Act amends FISA by establishing privacy protections for section 215 business records orders, requiring the Department of Justice Inspector General and the intelligence community to conduct audits and submit implantation reports. The Act requires that court orders for pen registers or trap and trace devices include specific selection terms, clarifies acquisition targeting outside the U.S., reforms the Foreign Intelligence Surveillance Courts, and ensures that National Security Letters are not used in bulk collection.

Legislation and Case Law

Bills/Legislative Activity

Email Privacy Act (H.R. 699, 114th Congress).
Available online at: [https://www.congress.gov/bill/114th-congress/house-bill/699].
Introduced by Rep. Yoder, the bill proposes amendments to the Electronic Communications Privacy Act prohibiting providers from disclosing contents to a governmental entity, with certain exceptions. The Act requires the government to obtain warrants regardless of the length of storage and nature of electronic communication. It also directs the Comptroller General to report to Congress regarding such disclosures and requires the government to provide such customers with a notification and copy of the warrant disclosing their communications.

Drone Aircraft Privacy and Transparency Act (S.635, 114th Congress).
Available online at: [https://www.congress.gov/bill/114th-congress/senate-bill/635] and its counterpart, the Drone Aircraft Privacy and Transparency Act (H.R. 1229, 114th Congress).
Available online at: [https://www.congress.gov/bill/114th-congress/house-bill/1229].
Both legislative proposals amend the FAA Modernization Reform Act of 2012 which would prohibit the FAA from issuing any certificate, license, or other grant of authority to operate a drone system unless it meets certain data transparency requirements. Certain exceptions would be granted in "exigent circumstances" involving the belief of "imminent danger of death or serious physical injury" or "high risk of an imminent terrorist attack by a specific individual or organization."

Location Privacy Protection Act of 2014 (S.2171, 113th Congress; introduced 3/27/2014).
Available online at: [https://www.congress.gov/bill/113th-congress/senate-bill/2171].
Introduced by Senator Franken, the legislation proposed prohibiting non-government individuals or entities from knowingly collecting or disclosing geolocation information from an electronic communications device. Covered entities would be required to notify individuals and make public information details available if collecting geolocations from more than 1,000 devices. The bill would require the Attorney General to issue regulations

to implement these requirements. The bill prohibited usage and disclosure in aid of domestic violence or stalking, in addition to establishing an Anti-Stalking Fund.

Location Privacy Protection Act of 2012 (S.1223, 112th Congress; introduced 6/16/2011).
Available online at: [https://www.congress.gov/bill/112th-congress/senate-bill/1223/text].
Introduced in 2011 by Senator Franken, the bill proposed amending the federal criminal code with certain protections and exceptions on the collection or disclosure of geolocation information to or by nongovernmental entities.

U.S. Congress. House Committee on the Judiciary. *Constitutional Limitations on Domestic Surveillance: Hearing before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the Committee on the Judiciary, House of Representatives*. 110th Congress, 1st Session, Thursday, June 7, Serial No. 110-45. Washington, D.C.: GPO, 2007.
Available online at: [http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg35861/pdf/CHRG-110hhrg35861.pdf].
The hearing examined the constitutional and statutory restrictions on domestic surveillance, the Bush administration's NSA terrorist surveillance program, the President's constitutional authority as chief executive and commander-in-chief, and the Foreign Intelligence Surveillance Act (FISA) requirements. Five witnesses provided overviews of FISA activities from a variety of perspectives (U.S. Department of Justice, Office of Legal Counsel, attorneys, Library of Congress, and the American Civil Liberties Union).

U.S. Congress. House Committee on the Judiciary. *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA FREEDOM) Act of 2015: Report [To Accompany H.R. 2048]*. 114th Congress, 1st Session, May 8, 2015. H.Rept. 114-109. Washington, D.C.: GPO, 2015.
Available online at: [https://www.congress.gov/114/crpt/hrpt109/CRPT-114hrpt109-pt1.pdf].
Part of the legislative history of Public Law No. 114-23 and its related bill H.R. 2048, the

report of the Committee explains the background and need of the legislation, including a section-by-section analysis.

Legislation and Case Law

Case Law

ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).
The U.S. Court of Appeals for the Second Circuit held that Section 215 of the USA PATRIOT Act of 2001, as amended, did not authorize the National Security Agency's bulk telephony metadata collection program. The court held that the program, which "requires that the phone companies turn over records on an 'ongoing daily basis' – with no foreseeable end point, no requirement of relevance to any particular set of facts, and no limitations as to subject matter or individuals covered" – did not meet the statute's requirement of being "relevant to an authorized investigation." Because the court found that the program was not authorized by the statute, it did not evaluate its constitutionality under the Fourth Amendment. This decision vacated a lower-court decision, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

In re Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008).
The Foreign Intelligence Surveillance Court of Review held that the government's task of "protecting an interest of utmost significance to the nation – the safety and security of its people" – justified "a foreign intelligence exception to the Fourth Amendment's warrant requirement ... when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States." "For one thing, the purpose ... goes well beyond any garden-variety law enforcement objective."

Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013). *Appeal Argued,* No. 14-5004 (D.C. Cir. Nov. 4, 2014). (*Appeal pending as of publication date).*
The U.S. District Court for the District of Columbia ruled that the Fourth Amendment

prohibited a National Security Agency counterterrorism program that collected and stored telephone call records in bulk without warrants. The court held that the bulk metadata collection program invaded reasonable expectations of privacy. The court went on to find that the program was not justified under "special needs" precedents for suspicionless and warrantless searches and seizures, and that the limited record before the court did not demonstrate that the program was any faster or more effective than other investigative techniques.

Riley v. California, 134 S. Ct. 2473 (2014).
The Supreme Court unanimously held that the Fourth Amendment generally prohibits a warrantless search for digital information on a cell phone seized from an arrestee. The "search incident to arrest" doctrine allows police to search the person arrested to protect officer safety and prevent the destruction or concealment of evidence. "[N]either of [these] rationales has much force with respect to digital content on cell phones." Moreover, among "several interrelated consequences for privacy," "[t]he sum of an individual's private life can be reconstructed" due to modern cell phones' "immense storage capacity." "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple – get a warrant."

United States v. Jones, 132 S. Ct. 945 (2012).
The Supreme Court unanimously held that installing a GPS tracking device on a drug suspect's vehicle and using it to track the vehicle's movements for 28 days was a "search" under the Fourth Amendment, and therefore required a warrant. Five justices held that a "search" occurred because "the Government obtain[ed] information by physically intruding on a constitutionally protected area." Four concurring justices would have reached the same result solely on grounds that the suspect's "reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." The majority and concurring opinions sharply disagreed on whether the correct test for a "search" is (or should be) based on physical trespass alone, reasonable expectation of privacy alone, or some combination.

United States v. United States District Court, 407 U.S. 297 (1972).
The Supreme Court held that the Fourth Amendment requires the government to obtain a warrant from a neutral and disinterested magistrate before using electronic surveillance in a domestic national-security case. "[U]nreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." The Court emphasized it was not addressing surveillance "with respect to the activities of foreign powers, within or without this country."

Domestic Surveillance

Advantages

Articles

Atkinson, L. Rush. "The Fourth Amendment's National Security Exception: Its History and Limits." *Vanderbilt Law Review*, vol. 66, no. 5 (October 2013): 1344-1405.
This article provides an overview of what national security investigations actually are, and compares and contrasts them to traditional criminal investigations, (see pages 1348-51). The article focuses on the historical precedents of modern-day national security investigations, dating back to 1797.

Lowry, Rich. "Patriot Hysteria: The Zacarias Moussaoui Protection Act." *National Review Online* (August 28, 2003).
Available online at: [http://www.nationalreview.com/article/207877/patriot-hysteria-rich-lowry].
The author argues that no civil liberties have actually been violated under the USA PATRIOT Act, despite the "hysteria" surrounding it and the importance of "aggressive, preemptive law enforcement."

Yoo, John. "The Legality of the National Security Agency's Bulk Data Surveillance Programs." *Harvard Journal of Law & Public Policy,* vol. 37, no. 3 (Summer 2014): 901-930.
Argues that the Foreign Intelligence Surveillance Act blends "criminal and wartime

information gathering schemes," and "does not reflect a general attitude against government surveillance." Defends the legality and constitutionality of the National Security Agency's programs to collect bulk telephone metadata ("the magnitude of harm that the government seeks to prevent exceeds by several orders that of regular crime") and electronic communications data between non-U.S. persons outside the United States ("the Fourth Amendment does not provide rights outside the United States except to citizens or those with sufficient connections to the nation, such as permanent resident aliens").

Domestic Surveillance

Advantages

Books

Ashcroft, John D. 2006. *Never Again: Securing America and Restoring Justice*. New York, NY: Center Street, 2006.
Former Attorney General John Ashcroft provides examples where the use of electronic surveillance may have prevented terrorist attacks. In chapter 10, he argues that the USA PATRIOT Act allowed the "fight against terror" to use surveillance techniques already available in other areas of law enforcement.

Carroll, Jamuna, ed. *Privacy*. Farmington Hills, MI: Greenhaven Press, 2006.
This title is part of the *Opposing Viewpoints Series*. Chapter 1, titled "Do Counterterrorism Measures Infringe on Privacy Rights?" includes two essays on surveillance under the Patriot Act, one arguing that such surveillance violates privacy and one arguing that it protects Americans.

Huang, Lee-Sean and Nicholas DiBiase, eds. *Freedom vs. Security: The Struggle for Balance*. New York, NY: International Debate Education Association, 2010.
This title is part of the *International Debate Education Association (IDEA) Contemporary Controversies Series*. Part 4, titled "On Surveillance," includes essays that examine the conflict between privacy and safety.

Miller, Debra A., ed. *Homeland Security*. Farmington Hills, MI: Greenhaven Press, 2009. This title is part of the *Current Controversies Series*. Chapter 4, titled "Do Efforts to Enhance Homeland Security Threaten Civil Liberties?" includes essays that examine the interplay between homeland security and the protection of civil liberties.

Office of the Director of National Intelligence, Office of General Counsel. *Intelligence Community Legal Reference Book*. Washington, D.C.: GPO, 2012.
Available online at: [http://www.dni.gov/ogc].
From the book's introduction: "The Intelligence Community draws much of its authority and guidance from the body of law contained in this collection ... expanded and updated ... to reflect legal developments since the previous edition was published in 2009 and in response to comments received from the Intelligence Community to that edition."

Domestic Surveillance

Advantages

Think Tanks

"The Patriot Act and Related Provisions: The Heritage Foundation's Research." Washington, D.C.: The Heritage Foundation, 2004.

Available online at: [http://www.heritage.org/research/reports/2004/11/the-patriot-act-and-related-provisions-the-heritage-foundations-research].
A compilation of Heritage Foundation research on the USA PATRIOT Act.

Domestic Surveillance

Advantages

Websites

U.S. Department of Justice. "Preserving Life and Liberty."
Available online at: [http://www.justice.gov/archive/ll/highlights.htm].

This Department of Justice website provides a range of information on the USA PATRIOT Act. "Highlights" of the Act can be found in the section entitled "What is the Patriot Act?" The website also includes sections that link to testimony and congressional remarks, and a section entitled "Dispelling the Myths."

Domestic Surveillance

Disadvantages

Articles

Dahl, Erik. "Domestic Intelligence Today: More Security but Less Liberty?" *Homeland Security Affairs*, vol. 7, no. 2 (2011).
This article discusses the restructuring and growth of the U.S. intelligence system since September 11, 2001, and the debate over the creation of a domestic intelligence agency. The author argues that the balance between security and liberty in the United States has shifted "in the direction of more security, but less liberty."

Etzioni, Amitai. "NSA: National Security vs. Individual Rights." *Intelligence & National Security*, vol. 30, no. 1 (February 2015): 100-136.
This article provides analysis of the bulk phone records collection and PRISM programs of the National Security Agency to examine their effectiveness, and the relationship between the threats to national security and justifications for these programs. The author endeavors to address the scope of possible privacy violations, the legality and constitutionality of the programs, and their accountability and oversight, including concerns of abuse.

Richards, Neil M. "The Dangers of Surveillance." *Harvard Law Review,* vol. 126, no. 7 (2012): 1934-1965.
The author draws on law, history, literature, and the work of scholars in surveillance studies to address the significance of privacy rights and civil liberties in the context of government surveillance. He proposes principles for future surveillance law, including examinations of transparency, oversight, and the "harmfulness" of surveillance.

Setty, Sudha. "Surveillance, Secrecy, and the Search for Meaningful Accountability." *Stanford Journal of International Law*, vol. 51, no. 1 (2015): 69-103.
This article discusses the growth of the surveillance infrastructure in the United States since September 11, 2001, in the context of secrecy, transparency, and oversight. The author provides comparisons to surveillance-related powers and accountability measures in the United Kingdom and India to advance the discussion of the efficacy, accountability, and transparency of intelligence programs created and expanded to address the threat of terrorism.

Vagle, Jeffrey L. "Furtive Encryption: Power, Trusts, and the Constitutional Cost of Collective Surveillance." *Indiana Law Journal,* vol. 90, no. 1 (Winter 2015): 101-150.
This article discusses a provision of the Foreign Intelligence Surveillance Act of 1978 that allows the United States National Security Agency (NSA) to keep indefinitely any encrypted information collected from domestic communications, regardless of the purpose of encryption. The authors discuss the constitutionality of the collection of all electronic communications from U.S. citizens that are hidden or obscured through encryption, and argue that this is in conflict with the Fourth Amendment, as a form of "suspicionless search and seizure."

Domestic Surveillance

Disadvantages

Books

Landau, Susan Eva. *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*. Cambridge, MA: MIT Press, 2010.
Examines the history of surveillance and security in the United States, including the histories of communication technology, policy, and law, with a focus on information and data in the modern world. The author discusses the effect of surveillance policies on privacy and government transparency, and offers advice on future policy and actions to address these issues.

Lind, Nancy S. and Erik Rankin. *Privacy in the Digital Age: 21st-Century Challenges to the Fourth Amendment.* Santa Barbara, CA: Praeger, 2015.
This two-volume set discusses the impact of surveillance and data collection on privacy, as defined in the Fourth Amendment to the U.S. Constitution. It examines the "erosion of privacy rights engendered by the ability of digital technology to intercept, mine, and store personal data, most often without the knowledge of those being monitored," and examines "the possible impact of the widespread gathering of such data by law enforcement, security agencies, and private corporations." It includes essays on the history and intent of the Fourth Amendment as it relates to recent court cases on privacy.

Solove, Daniel J. *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven, CT: Yale University Press, 2011.
The book endeavors to counter the argument that privacy must be sacrificed for security through an examination of the history of this debate, the laws protecting privacy, and concerns about new technologies. The author discusses concerns with current surveillance policies and proposes alternatives, including changes to oversight and regulations.

Domestic Surveillance

Disadvantages

Think Tanks

Bendix, William and Paul J. Quirk. *Secrecy and Negligence: How Congress Lost Control of Domestic Surveillance*. Washington, D.C.: Brookings Institution, March 2015.
Available online at:
[http://www.brookings.edu/~/media/research/files/papers/2015/03/02-secrecy-negligence-congres-surveillance-bendix-quirk/ctibendixquirksecrecyv3.pdf].
This paper examines the role of the executive and legislative branches of government in oversight and control of domestic surveillance programs in the United States. The authors contend the United States Congress yielded oversight of surveillance programs to the

executive branch by “repeatedly reauthoriz[ing] intelligence-gathering activities on the basis of false and misleading accounts of their scope.” The authors suggest reforms for Congressional involvement and oversight of classified surveillance programs.

SUBJECT BIBLIOGRAPHY

This section of the bibliography was compiled by the U. S. Government Publishing Office Library Services and Content Management.

These resources are available for purchase at the GPO bookstore at http://bookstore.gpo.gov/

"Resolved: The United States Federal Government Should Substantially Curtail Its Domestic Surveillance"

Annual Open Hearing on Current and Projected National Security Threats to the United States, Hearing, January 29, 2014

Publisher: Select Committee on Intelligence of the Senate

Year/Pages: 2015: 68 p.

Price: $7.50

Code of Federal Regulations, Title 32, National Defense, Pt. 191–399. Revised as of July 1, 2014

Publisher: National Archives and Records Administration, Office of the Federal Register

Year/Pages: 2014: 1147 p.

Price: $69.00

Studies in Intelligence, Journal of the American Intelligence Professional, V. 58, No. 2 (Unclassified Articles from June 2014)

Publisher: Central Intelligence Agency, Center for the Study of Intelligence

Year/Pages: 2014: 94 p.; ill.

Price: $9.00

Constitutional Limitations on Domestic Surveillance, Hearing, June 7, 2007

Publisher: Committee on the Judiciary of the House of Representatives

Year/Pages: 2013: 156 p.

Price: $20.00

Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace, Hearing, November 17, 2009

Publisher: Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security of the Senate

Year/Pages: 2010: 184 p.

Price: $16.00

Cybersecurity: The Evolving Nature of Cyber Threats Facing the Private Sector, Hearing, March 18, 2015

Publisher: Subcommittee on Information Technology of the Committee on Oversight and Government Reform of the House

Year/Pages: 2015: 109 p.

Price: $12.00

Do-Not-Track Legislation: Is Now the Right Time? Hearing, December 2, 2010

Publisher: Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection of the U.S. House of Representatives

Year/Pages: 2013: 158 p.

Price: $15.00

2014 The FBI Story

Publisher: Justice Department, Federal Bureau of Investigation

Year/Pages: 2014: 115 p.; ill.

Price: $22.00

How Data Mining Threatens Student Privacy, Joint Hearing, June 25, 2014

Publisher: Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies and Committee on Education and the Workforce of the House

Year/Pages: 2015: 61 p.

Price: $7.00

Industry Perspectives on the President's Cybersecurity Information Sharing Proposal, Hearing, March 4, 2015

Publisher: Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies and Committee on Education and the Workforce of the House

Year/Pages: 2015: 57 p.

Price: $7.00

Striking the Right Balance: Protecting Our Nation's Critical Infrastructure from Cyber Attack and Ensuring Privacy and Civil Liberties, Hearing, April 25, 2013

Publisher: Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the House

Year/Pages: 2013: 42 p.

Price: $5.25

A number of additional resources on this topic are freely available on GPO's Federal Digital System at http://www.gpo.gov/fdsys/search/home.action

Constitutional Limitations on Domestic Surveillance, Hearing Before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the Committee on the Judiciary House of Representatives, One Hundred Tenth Congress, First Session, June 7, 2007, Serial No. 110–45
http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg35861/pdf/CHRG-110hhrg35861.pdf

S. RES. 350, One Hundred Ninth Congress, Second Session, January 20, 2006
Expressing the sense of the Senate that Senate Joint Resolution 23 (107th Congress), as adopted by the Senate on September 14, 2001, and subsequently enacted as the Authorization for Use of Military Force does not authorize warrantless domestic surveillance of United States citizens.
http://www.gpo.gov/fdsys/pkg/BILLS-109sres350is/pdf/BILLS-109sres350is.pdf

S. 1215 (IS)—FISA Accountability and Privacy Protection Act of 2013, One Hundred Thirteenth Congress, First Session, June 24, 2013
http://www.gpo.gov/fdsys/pkg/BILLS-113s1215is/pdf/BILLS-113s1215is.pdf

S. 436 (IS)—Domestic Surveillance Oversight Act of 2003, One Hundred and Eighth Congress, First Session, February 25, 2003
http://www.gpo.gov/fdsys/pkg/BILLS-108s436is/pdf/BILLS-108s436is.pdf

156 Congressional Record S2108—Expiring Domestic Surveillance Provisions, Congressional Record—Senate, March 25, 2010
http://www.gpo.gov/fdsys/pkg/CREC-2010-03-25/pdf/CREC-2010-03-25-pt1-PgS2108.pdf

H.R. 11 (IH)—NSA Oversight Act, One Hundred Tenth Congress, First Session, January 4, 2007
http://www.gpo.gov/fdsys/pkg/BILLS-110hr11ih/pdf/BILLS-110hr11ih.pdf

H.R. 4976 (IH)—NSA Oversight Act, One Hundred Ninth Congress, Second Session, March 16, 2006
http://www.gpo.gov/fdsys/pkg/BILLS-109hr4976ih/pdf/BILLS-109hr4976ih.pdf

H.R. 5371 (IH)—Lawful Intelligence and Surveillance of Terrorists in an Emergency by NSA Act, One Hundred Ninth Congress, Second Session, May 11, 2006
http://www.gpo.gov/fdsys/pkg/BILLS-109hr5371ih/pdf/BILLS-109hr5371ih.pdf

151 Congressional Record H12145—Domestic Surveillance, Congressional Record—House, December 17, 2005
http://www.gpo.gov/fdsys/pkg/CREC-2005-12-17/pdf/CREC-2005-12-17-pt1-PgH12145-2.pdf

House Report 109–680 Electronic Surveillance Modernization Act Part 1, One Hundred Ninth Congress, Second Session, September 25, 2006
http://www.gpo.gov/fdsys/pkg/CRPT-109hrpt680/pdf/CRPT-109hrpt680-pt1.pdf

House Report 109–680 Electronic Surveillance Modernization Act Part 2, One Hundred Ninth Congress, Second Session, September 25, 2006
http://www.gpo.gov/fdsys/pkg/CRPT-109hrpt680/pdf/CRPT-109hrpt680-pt2.pdf

House Report 110–373, Part 1—Responsible Electronic Surveillance that is Overseen, Reviewed, and Effective Act of 2007 or Restore act of 2007, One Hundred Tenth Congress, First Session, October 12, 2007
http://www.gpo.gov/fdsys/pkg/CRPT-110hrpt373/pdf/CRPT-110hrpt373-pt1.pdf

House Report 110–373, Part 2—Responsible Electronic Surveillance that is Overseen, Reviewed, and Effective Act of 2007 or Restore act of 2007, One Hundred Tenth Congress, First Session, October 12, 2007
http://www.gpo.gov/fdsys/pkg/CRPT-110hrpt373/pdf/CRPT-110hrpt373-pt2.pdf

Senate Hearing 113–50—The Future of Drones in America: Law Enforcement and Privacy Considerations, One Hundred Thirteenth Congress, First Session, March 20, 2013
http://www.gpo.gov/fdsys/pkg/CHRG-113shrg81775/pdf/CHRG-113shrg81775.pdf

House Report 109–696—Providing for Consideration of H.R. 5825, Electronic Surveillance Modernization Act, One Hundred Ninth Congress, Second Session, September 28, 2006
http://www.gpo.gov/fdsys/pkg/CRPT-109hrpt696/pdf/CRPT-109hrpt696.pdf

○