# Explanation/Guide

### File Description and Tips for Debating Topicality

This file includes two topicality arguments — one for the Surveillance State Repeal Act affirmative and one for the Secure Data Act affirmative. It contains materials for both the affirmative and negative. These topicality arguments are included in the novice packet because they will introduce students to topicality and give them an opportunity to debate it. Only the topicality arguments in this file are acceptable to read in the novice division.

When negative, teams should introduce the appropriate topicality argument as an off-case position in the 1NC. The 1NC shells are included in the file. To extend topicality, students will need to prepare blocks to the affirmative’s arguments. Two additional pieces of negative evidence are also provided for each violation to assist in extending the position.

When affirmative, teams should answer the topicality argument introduced by the negative by using the appropriate 2AC frontline. Students might need to shorten the frontline so that it does not take too much time in the 2AC. The affirmative is also provided with two additional pieces of evidence that may be useful when answering topicality in the 1AR.

In the spirit of the packet, students should debate topicality as if there were not novice packet restrictions. Affirmative teams should refrain from making the argument that because of the novice packet restrictions, there are always only two topical plans. Similarly, affirmative teams should not advance the argument that the plan *must* be topical because it is included in the novice packet. While largely true, these arguments capitalize on the division’s argument limits to undermine the training value of novice topicality debates. It is better for all students if topicality is debated as if the round was taking place in a non-packet division.

### Debating Topicality vs. SSRA

The negative argues that “domestic surveillance” requires that the target of surveillance be one or more U.S. persons. They argue that the programs the plan curtails are actually *foreign* surveillance because they target non-U.S. persons. The affirmative responds that *in practice*, these foreign-targeted surveillance programs sweep up information about millions of Americans and should therefore rightly be classified as *domestic*. They will argue that the plan clearly meets the negative’s interpretation because it ends surveillance of “Americans’ electronic communications.”

### Debating Topicality vs. SDA

The negative argues that “curtail” requires a reduction in the extent or quantity of something as measured from a status quo baseline. In other words, “curtail” means to reduce from the current level. The negative contends that because there are no current programs to compel or encourage encryption backdoors, the plan only ends a hypothetical future program of domestic surveillance. In response, the affirmative argues that there *are* existing programs to compel or encourage encryption backdoors. They will further argue that because it is impossible to know for sure the exact nature of NSA programs, a better interpretation of “curtail” would be that it is about the *authority* to conduct domestic surveillance. Because the plan ends intelligence agencies’ authority to compel or encourage encryption backdoors, it is topical under this counter-interpretation.

# Topicality vs. SSRA

## Negative

### 1NC — Topicality “Domestic”

#### The first/next off-case position is Topicality *Domestic*.

#### First, “domestic surveillance” requires that the target of surveillance be a U.S. person.

Donohue 6 — Laura K. Donohue, Fellow at the Center for International Security and Cooperation at Stanford University, holds a Ph.D. in History from the University of Cambridge and a J.D. from Harvard Law School, 2006 (“Anglo-American Privacy and Surveillance,” *Journal of Criminal Law & Criminology* (96 J. Crim. L. & Criminology 1059), Spring, Available Online to Subscribing Institutions via Lexis-Nexis)

As the extent of the domestic surveillance operations emerged, Congress attempted to scale back the Executive's power while leaving some flexibility to address national security threats. n183 The legislature focused on the targets of surveillance, limiting a new law to foreign powers, and agents of foreign powers - which included groups "engaged in international terrorism or activities in preparation therefor." n184 Congress distinguished between U.S. and non-U.S. persons, creating tougher standards for the former. n185 The Foreign Intelligence Surveillance Act ("FISA") considered any "acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication," as well as other means of surveillance, such as video, to fall under the new restrictions. n186 Central to the statute's understanding of surveillance was that, by definition, consent had not been given by the target. Otherwise, the individual would have a reasonable expectation of privacy and, under ordinary circumstances, the Fourth Amendment would require a warrant. n187

Footnote n183. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, tit. 1, 102, 92 Stat. 1786 (1978) (codified as amended at 50 U.S.C. 1801-11 (2000)).

Footnote n184. 50 U.S.C. 1801(a)(4). An agent of a foreign power is anyone, other than a U.S. person who, inter alia, "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore, for or on behalf of a foreign power." Id. 1801(b)(2)(C). "International terrorism" incorporated three elements: (a) acts dangerous to human life and in violation of criminal law; (b) the intent to influence government policy or to intimidate or coerce a civilian population; and (c) acts that "occur totally outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum." Id. 1801(c)(1)-(3).

Footnote n185. The former included citizens and resident aliens, as well incorporated entities and unincorporated associations with a substantial number of U.S. persons. Non-U.S. persons qualified as an "agent of a foreign power" by virtue of membership - e.g., if they were an officer or employee of a foreign power, or if they participated in an international terrorist organization. Id. 1801(i). U.S. persons had to engage knowingly in the collection of intelligence contrary to U.S. interests, the assumption of false identity for the benefit of a foreign power, and aiding or abetting others to the same. Id. 1801(b).

Footnote n186. Id. 1801(f)(1); see also id. 1801(f)(4); Daniel Blinka, Electronic Surveillance: Commentaries and Statutes (2004).

Footnote n187. 50 U.S.C. 1801 (f)(1)-(4).

#### Second, the plan violates this interpretation — it curtails foreign surveillance.

Thompson 13 — Loren Thompson, Chief Operating Officer of the Lexington Institute—a non-profit public policy think tank, Chief Executive Officer of Source Associates—a defense consulting firm, former Deputy Director of the Security Studies Program at Georgetown University, holds a Ph.D. in Government from Georgetown University, 2013 (“Why NSA’s PRISM Program Makes Sense,” *Forbes*, June 7th, Available Online at <http://www.forbes.com/sites/lorenthompson/2013/06/07/why-nsas-prism-program-makes-sense/>, Accessed 08-14-2015)

President Obama’s firm defense of the National Security Agency’s “domestic” surveillance program on Friday should calm some of the more extravagant fears provoked by public disclosure of its existence. I put the word “domestic” in quotes because the effort to monitor Internet and other communications traffic isn’t really about listening in on Americans, or even foreign nationals living here, but rather intercepting suspicious transmissions originating overseas that just happen to be passing through the United States.

That is an eminently sensible way of keeping up with terrorists, because it is so much easier than tapping into network conduits in other countries or under the seas (not that we don’t do that). In order to grasp the logic of the NSA program, which is code-named PRISM, you have to understand how the Internet evolved. It was a purely American innovation at its inception, with most of the infrastructure concentrated in a few places like Northern Virginia.

I live a few miles from where the Internet’s first big East Coast access point was located in the parking garage of an office building near the intersection of Virginia’s Routes 7 and 123, an area that some people refer to as Internet Alley. Because the Worldwide Web grew so haphazardly in its early days, it was common until recently for Internet traffic between two European countries to pass through my neighborhood. There were only a few major nodes in the system, and packet-switching sends messages through whatever pathway is available.

The Washington Post story on PRISM today has a graphic illustrating my point about how bandwidth tends to be allocated globally. Like a modern version of ancient Rome’s Appian Way, all digital roads lead to America. It isn’t hard to see why Director of National Intelligence James R. Clapper could say on Thursday that “information collected under this program is among the most important and valuable foreign intelligence information we collect.” No kidding: PRISM generated an average of four items per day for the President’s daily intelligence briefing in 2012.

The key point to recognize, though, is that this really is foreign intelligence. The architecture of the Internet enables NSA to collect it within U.S. borders, but there is no intention to spy on U.S. citizens. A few elementary algorithms used in narrowing the analysis of traffic should be sufficient to assure that the privacy of American citizens is seldom compromised. President Obama stressed in his comments today that safeguards have been put in place to prevent the scope of NSA surveillance from expanding beyond its original purpose.

#### Finally, vote negative to maintain debatable limits. Allowing plans that curtail foreign surveillance dramatically expands the scope of the topic. Overly broad topics promote shallow and generic debates because they make it too difficult for the negative to research and prepare against each case. In-depth clash over core issues is the most important impact because it incentivizes research, promotes critical and strategic thinking, and rigorously tests content mastery.

### Extend: “Plan Not Domestic”

#### The surveillance the plan curtails is foreign intelligence collection, not domestic surveillance.

McCarthy 6 — Andrew C. McCarthy, Contributing Editor of *National Review* and Senior Fellow at the National Review Institute, former Assistant United States Attorney for the Southern District of New York where he prosecuted Sheikh Omar Abdel Rahman and eleven others for the 1993 World Trade Center bombing, 2006 (“It’s Not “Domestic Spying”; It’s Foreign Intelligence Collection,” *The Corner*—the *National Review* blog, May 15th, Available Online at <http://www.nationalreview.com/corner/122556/its-not-domestic-spying-its-foreign-intelligence-collection-andrew-c-mccarthy>, Accessed 08-14-2015)

Eggen also continues the mainstream media’s propagandistic use of the term “domestic surveillance [or 'spying'] program.” In actuality, the electronic surveillance that the NSA is doing — i.e., eavesdropping on content of conversations — is not “domestic.” A call is not considered “domestic” just because one party to it happens to be inside the U.S., just as an investigation is not “domestic” just because some of the subjects of interest happen to reside inside our country. Mohammed Atta was an agent of a foreign power, al Qaeda. Surveilling him — had we done it — would not have been “domestic spying.”

The calls NSA eavesdrops on are “international,” not “domestic.” If that were not plain enough on its face, the Supreme Court made it explicit in the Keith case (1972). There, even though it held that judicial warrants were required for wiretapping purely domestic terror organizations, the Court excluded investigations of threats posed by foreign organizations and their agents operating both within and without the U.S.

That is, the Court understood what most Americans understand but what the media, civil libertarians and many members of Congress refuse to acknowledge: if we are investigating the activities of agents of foreign powers inside the United States, that is not DOMESTIC surveillance. It is FOREIGN counter-intelligence.

That, in part, is why the statute regulating wiretaps on foreign powers operating within the U.S. — the one the media has suddenly decided it loves after bad-mouthing it for years as a rubber-stamp — is called the FOREIGN Intelligence Surveillance Act (FISA). The United States has never needed court permission to conduct wiretapping outside U.S. territory; the wiretapping it does inside U.S. territory for national security purposes is FOREIGN INTELLIGENCE COLLECTION, not “domestic surveillance.”

\* Eggen = Dan Eggen, a *Washington Post* reporter

(CAPITALIZATION was used in the article)

#### NSA doesn’t collect Americans’ electronic communications.

DNI and NSA 13 —United States Director of National Intelligence and National Security Agency, 2013 (Joint Statement from the Office of the Director of National Intelligence and the National Security Agency, August 21st, Available Online at <https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_21_Joint_Statement_ODNI_NSA.pdf>, Accessed 08-14-2015)

Press reports based on an article published in today’s Wall Street Journal mischaracterize aspects of NSA’s data collection activities conducted under Section 702 of the Foreign Intelligence Surveillance Act. The NSA does not sift through and have unfettered access to 75% of the United States’ online communications. The following are the facts:

\* Media reports based upon the recent Wall Street Journal (WSJ) article regarding NSA’s foreign intelligence activities provide an inaccurate and misleading picture of NSA’s collection programs, but especially with respect to NSA’s use of Section 702 of the Foreign Intelligence Surveillance Act (FISA).

\* The reports leave readers with the impression that NSA is sifting through as much as 75% of the United States’ online communications, which is simply not true.

\* In its foreign intelligence mission, and using all its authorities, NSA “touches” about 1.6%, and analysts only look at 0.00004%, of the world’s internet traffic.

\* The assistance from the providers, which is compelled by the law, is the same activity that has been previously revealed as part of Section 702 collection and PRISM.

\* FISA is designed to allow the U.S. Government to acquire foreign intelligence while protecting the civil liberties and privacy of Americans.

\* Section 702 specifically prohibits the intentional acquisition of any communications when all parties are known to be inside the U.S.

\* The law specifically prohibits targeting a U.S. citizen without an individual court order based on a showing of probable cause.

\* The law only permits NSA to obtain information pursuant to Section 702 in accordance with orders and procedures approved by the Foreign Intelligence Surveillance Court.

\* When conducting 702 FISA surveillance, the only information NSA obtains results from the use of specific identifiers (for example email addresses and telephone numbers) used by non-U.S. persons overseas who are believed to possess or receive foreign intelligence information.

\* Foreign terrorists sometimes communicate with persons in the U.S. or Americans overseas. In targeting a terrorist overseas who is not a U.S. person, NSA may get both sides of a communication. If that communication involves a U.S. person, NSA must follow Attorney General and FISA Court approved “minimization procedures” to ensure the Agency protects the privacy of U.S. persons.

## Affirmative

### 2AC — Topicality “Domestic”

#### 1. We Meet — the plan curtails surveillance of “Americans’ electronic communications.” It repeals “programs under FISA and the Patriot Act that allow indiscriminate collection and access to Americans’ communications” — that’s Williams.

#### 2. Counter-Interpretation — “domestic surveillance” includes programs with foreign “targets” if those programs result in substantial collection of data from U.S. persons.

Lee 13 — Timothy B. Lee, Reporter covering technology policy for *The Washington Post*, former Reporter for *Ars Technica* and *Forbes*, former Adjunct Scholar at the Cato Institute, holds a Master’s in Computer Science from Princeton University, 2013 (“The NSA is trying to have it both ways on its domestic spying programs,” *The Washington Post*, December 22nd, Available Online at <https://www.washingtonpost.com/news/the-switch/wp/2013/12/22/the-nsa-is-trying-to-have-it-both-ways-on-its-domestic-spying-programs/>, Accessed 08-14-2015)

Traditionally, domestic surveillance powers were held by law enforcement agencies, not the NSA. And the existence of the spying powers were not secret. Everyone knows that the FBI and local police departments have the power to compel telecommunications companies to disclose their customers' communications. But first they must get a warrant, supported by probable cause, from a judge. That oversight gives Americans confidence that domestic surveillance powers won't be abused.

Things are very different when the U.S. government spies on people overseas. Obviously, U.S. intelligence agencies don't generally have the power to compel foreign telecommunications companies to cooperate with surveillance efforts. So instead of a formal legal process, they traditionally have used covert means—bribing insiders, installing bugs, tapping undersea cables, hacking into foreign networks—to intercept foreign communications. For these methods to work, the government must keep secret not only the specific surveillance targets, but the fact that the surveillance program exists at all. If the program's existence is revealed, the foreign government is likely to shut it down.

That secrecy meant that American foreign intelligence-gathering operations have not had the checks and balances that applied to domestic law enforcement surveillance. But Americans were protected by the rule that American foreign intelligence agencies were only supposed to operate overseas.

But now the Internet has made a hash of the tidy distinction between foreign and domestic surveillance. Today, citizens of France, Brazil and Nigeria routinely use Facebook, Gmail, and other American online services to communicate. Americans make calls with Skype. And much Internet traffic between two foreign countries often passes through the United States.

The NSA has reacted to this changing communications landscape by trying to claim the best of both worlds. The FISA Amendments Act, passed in 2008, gave the NSA the power to compel domestic telecommunications providers to cooperate with the NSA's surveillance programs. Yet the NSA has resisted the transparency and judicial oversight that has traditionally accompanied domestic surveillance. They've argued that disclosing the existence of these programs would compromise their effectiveness. And they've argued that because the "targets" of surveillance are overseas, only limited judicial oversight by the secretive Foreign Intelligence Surveillance Court, not individualized Fourth Amendment warrants, were required.

But the NSA programs revealed by Snowden, including PRISM and the phone records program, look more like domestic surveillance programs than foreign ones. Like conventional domestic wiretaps, they rely on compelling domestic firms to cooperate with surveillance. Like conventional wiretaps, they sweep up information about the communications of Americans on American soil. And like domestic wiretaps, information collected by the NSA is sometimes shared with domestic law enforcement agencies for prosecution of Americans.

If the NSA is going to run what amounts to a domestic surveillance program that collects the private information of Americans on American soil, it's going to face pressure to subject that program to the same kind of oversight as other domestic surveillance program. That means disclosing the general characteristics of the program—but not the specific targets—to the public. And it means requiring individualized warrants, supported by probable cause, before the government can intercept the communications of Americans on American soil.

#### 3. Prefer Our Interpretation — it is impossible to clearly differentiate foreign and domestic surveillance in the context of Internet communications. Their interpretation excludes core cases about Executive Order 12333 and Section 702 of the FISA Amendments Act like PRISM, Upstream, and X-KEYSCORE.

#### 4. Prefer Contextual Evidence — the programs the plan curtails are “domestic surveillance.” The neg’s argument is overly semantic.

Cohn et al. 14 — Cindy Cohn, Executive Director and former Legal Director and General Counsel of the Electronic Frontier Foundation, holds a J.D. from the University of Michigan Law School, et al., 2014 (Motion for Summary Judgment in *Jewel et al. v. NSA et al.*, Case Number 4:08-cv-4373-JSW in the Oakland Division of the United States District Court for the Northern District of California, July 25th, Available Online at <https://www.eff.org/files/2014/07/25/jewel_4th_a_mpsj_brief.pdf>, Accessed 08-14-2015, p. 8-9)

A. The Government Seizes And Searches Communications Flowing Through The Nation’s Internet Backbone

The information revealed by a person’s Internet activities paints an intimate and richly detailed portrait of the person’s life—often on a day-by-day or minute-by-minute basis. It is precisely this deeply personal information that the government is seizing and searching. The Washington Post recently examined a sample of 160,000 Internet communications intercepted and retained by the NSA. Even after significantly more filtering and minimization than is at issue here, the Post reported: “Many other files, described as useless by the analysts but nonetheless retained, [end page 8] have a startlingly intimate, even voyeuristic quality. They tell stories of love and heartbreak, illicit sexual liaisons, mental-health crises, political and religious conversions, financial anxieties and disappointed hopes. The daily lives of more than 10,000 account holders who were not targeted are catalogued and recorded nevertheless.” 2

The government conducts its domestic surveillance by seizing and searching Internet communications as they flow through major fiber-optic network junctions on the Internet “backbone.”3 Almost all ordinary Internet traffic travels at some point over the Internet backbone—high-capacity, long-distance fiber-optic cables controlled by major Internet providers such as AT&T. The seizures at issue here occur on the junctions between AT&T and other providers on the backbone.

#### 5. No Topic Explosion — functional limits ensure a relatively small case list even if “domestic” is interpreted broadly. Plans must still “substantially curtail,” and overly small affs will lose to core DAs because they won’t have large advantages.

#### 6. Good Is Good Enough — debatability is more important than precision. The endless search for the “best” definition distracts from topic education. Don’t vote neg unless our interpretation precludes productive debate.

### Extend: “Plan Is Domestic”

#### Prefer our evidence — the programs the plan eliminates definitely collect domestic data *even if* the “targets” are foreign.

Kayyali 14 — Nadia Kayyali, Activist at the Electronic Frontier Foundation, holds a J.D. from the University of California-Hastings, 2014 (“The Way the NSA Uses Section 702 is Deeply Troubling. Here’s Why.,” Electronic Frontier Foundation, May 8th, Available Online at <https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why>, Accessed 08-14-2015)

Section 702 has been used by the NSA to justify mass collection of phone calls and emails by collecting huge quantities of data directly from the physical infrastructure of communications providers. Here’s what you should know about the provision and why it needs to be addressed by Congress and the President:

\* Most of the discussion around the NSA has focused on the phone records surveillance program. Unlike that program, collection done under Section 702 captures content of communications. This could include content in emails, instant messages, Facebook messages, web browsing history, and more.

\* Even though it’s ostensibly used for foreign targets, Section 702 surveillance sweeps up the communications of Americans. The NSA has a twisted, and incredibly permissive, interpretation of targeting that includes communications about a target, even if the communicating parties are completely innocent. As John Oliver put it in his interview with former NSA General Keith Alexander: "No, the target is not the American people, but it seems that too often you miss the target and hit the person next to them going, 'Whoa, him!'"

\* The NSA has confirmed that it is searching Section 702 data to access American’s communications without a warrant, in what is being called the "back door search loophole." In response to questions from Senator Ron Wyden, former NSA director General Keith Alexander admitted that the NSA specifically searches Section 702 data using "U.S. person identifiers," for example email addresses associated with someone in the U.S.

\* The NSA has used Section 702 to justify programs in which the NSA can siphon off large portions of Internet traffic directly from the Internet backbone. These programs exploit the structure of the Internet, in which a significant amount of traffic from around the world flows through servers in the United States. In fact, through Section 702, the NSA has access to information stored by major Internet companies like Facebook and Google.

#### NSA intercepts every American’s electronic communications without a warrant. “Targeting” is irrelevant.

Cohn et al. 14 — Cindy Cohn, Executive Director and former Legal Director and General Counsel of the Electronic Frontier Foundation, holds a J.D. from the University of Michigan Law School, et al., 2014 (Motion for Summary Judgment in *Jewel et al. v. NSA et al.*, Case Number 4:08-cv-4373-JSW in the Oakland Division of the United States District Court for the Northern District of California, July 25th, Available Online at <https://www.eff.org/files/2014/07/25/jewel_4th_a_mpsj_brief.pdf>, Accessed 08-14-2015, p. 7-8)

The eyes and ears of the government now sit on the Internet. The government indiscriminately copies and searches communications passing through the Internet’s key domestic junctions, on what is called the Internet “backbone.” By doing so, the government is operating a digital dragnet—a technological surveillance system that makes it impossible for ordinary Americans not suspected of any wrongdoing to engage in a fully private online conversation, to privately read online, or to privately access any online service. Millions of innocent Americans have their communications seized and searched as part of this dragnet even when the government is not targeting them or those with whom they communicate.

This unprecedented mass surveillance violates the core purpose of the Fourth Amendment— to protect Americans’ privacy against indiscriminate and suspicionless searches and seizures. “Indiscriminate searches and seizures conducted under the authority of ‘general warrants’ were the immediate evils that motivated the framing and adoption of the Fourth Amendment.” Payton v. New York, 445 U.S. 573, 583 (1980); accord Riley v. California, 573 U.S. \_\_, 134 S. Ct. 2473, 2494 (2014).

The government’s indiscriminate mass collection of Internet communications creates two separate Fourth Amendment violations:

First, the government unconstitutionally seizes plaintiffs’ Internet communications. Technology at plaintiffs’ Internet service provider, AT&T, automatically creates and delivers to the government a copy of plaintiffs’ online activities, along with those of millions of other innocent Americans—including email, live chat, reading and interacting with websites, Internet searching, and social networking.

Second, the government unconstitutionally searches the content of much of the communications stream it has seized. The government admits that it searches the content of the [end page 7] online communications that it has seized if it believes there is some indication that the origin or destination of the communication is outside the United States.

The Fourth Amendment prohibits the government from intercepting, copying, or searching through Americans’ communications without a warrant issued by a neutral and detached magistrate, upon probable cause, particularly describing the place to be searched and the things to be seized. The government conducts the seizures and searches at issue here without a Fourth Amendment warrant. While the government does obtain a periodic order from the Foreign Intelligence Surveillance Court (FISC) approving its general “targeting” and “minimization” procedures, those orders are simply not warrants. The FISC does not specify or limit the persons whose communications the government may seize or search, the communications facilities or accounts from which the government may seize communications, or what information the government may search for within the seized communications. The government alone determines these, without any judicial review. The FISC also does not make any determination that there is probable cause or reasonable suspicion to believe that the government’s seizures or searches will yield foreign intelligence information.

In truth, no valid warrant could authorize the government’s admitted practices here. The government’s targeting and minimization procedures are no substitute for the fundamental protections that the Constitution guarantees to all Americans. The ongoing dragnet seizure and search of innocent Americans’ Internet activities violates the Fourth Amendment.

# Topicality vs. SDA

## Negative

### 1NC — Topicality “Curtail”

#### The first/next off-case position is Topicality *Curtail*.

#### First, “curtail” means to reduce in extent or quantity by imposing a restriction on.

Oxford Dictionaries 14 — Oxford Dictionaries, 2015 (“Curtail,” Available Online at <https://www.oxforddictionaries.com/definition/english/curtail>, Accessed 08-15-2015)

Definition of curtail in English: verb

[WITH OBJECT]

1. Reduce in extent or quantity; impose a restriction on: civil liberties were further curtailed

#### Second, this requires a net reduction in domestic surveillance compared with the status quo baseline. “Curtail” does not mean to prevent a future decrease.

Howell 14 — Beryl A. Howell, United States District Judge for the United States District Court for the District of Columbia, 2014 (United States District Court Decision in *Humane Society of the United States, et al., Plaintiffs, v. Sally Jewell, Secretary of the Interior, et al., Defendants, v. State of Wisconsin et al., Intervenor–Defendants*, Westlaw Citation 2014 WL 7237702 (D.D.C. Dec. 19, 2014), Available Online at <https://www.animallaw.info/case/humane-society-united-states-v-jewell>, Accessed 08-15-2015)

\*46 Moreover, by defining “significant portion of a species' range” in the final rule as referring only to a species' “current range,” the FWS explicitly contradicts the conclusions by courts finding that “range” must include the “historical range” and the ESA's legislative history. LEG. HIST. at 742 (H. Rep. 95–1625, from Committee on Merchant Marine and Fisheries, regarding ESAA) (“The term ‘range’ [in the ESA] is used in the general sense, and refers to the historical range of the species.”); Defenders of Wildlife, 258 F.3d at 1145. It also renders meaningless the word “curtailment” in 16 U.S.C. § 1533(a)(1)(A), since it is impossible to determine the “present ... curtailment of [a species'] habitat or range” without knowing what the species' historical range was prior to being curtailed.

#### Third, the plan violates this interpretation — NSA is not currently authorized to insert encryption backdoors.

Kravets 15 — David Kravets, Senior Editor for *Ars Technica*, former Senior Staff Writer at *Wired*, former Legal Affairs Writer for the *Associated* Press, holds an M.A. in Political Science from California State University-Fullerton, 2015 (“This is the most outrageous government tirade against iOS 8 encryption,” *Ars Technica*, July 9th, Available Online at <http://arstechnica.com/tech-policy/2015/07/this-is-the-most-outrageous-government-tirade-against-ios-8-encryption/>, Accessed 08-15-2015)

As it now stands, nobody in Congress has actually proposed a law mandating these backdoors. Instead, politicians are trying to guilt the tech sector into complying. And President Barack Obama's administration is mulling an encryption policy and could ask Congress for backdoor legislation in the coming months.

For now, US-based companies are not required to provide the government with backdoors into their wares. The law surrounding this issue is the Communications Assistance for Law Enforcement Act of 1994. CALEA requires telcos to make their phone networks amenable to wiretaps, but it doesn't apply to phone hardware or most other communication services.

#### Finally, vote negative to maintain debatable limits. Allowing plans that curtail future surveillance substantially increases the scope of the topic because there are many hypothetical surveillance programs that should not be implemented. This also hurts negative ground because it allows the affirmative to curtail worst-case theoretical examples of domestic surveillance. Overly broad topics promote shallow and generic debates because they make it too difficult for the negative to research and prepare against each case. In-depth clash over core issues is the most important impact because it incentivizes research, promotes critical and strategic thinking, and rigorously tests content mastery.

### Extend: “No Current Programs”

#### There is no chance of legislation requiring encryption backdoors — that plan ends a hypothetical program.

Nakashima and Gellman 15 — Ellen Nakashima, National Security Reporter covering intelligence, technology, and civil liberties for *The Washington Post*, and Barton Gellman, National Correspondent for *The Washington Post*, Senior Fellow at the Century Foundation, Visiting Lecturer and Author in Residence at the Woodrow Wilson School of Public and International Affairs at Princeton University, recipient of a Pulitzer Prize for National Reporting for his coverage of the September 11 attacks, a Pulitzer Prize for National Reporting for his coverage of the Dick Cheney’s influence on Bush Administration foreign policy, and a Pulitzer Prize for Public Service for his coverage of the Snowden leaks, holds an M.A. in Politics from University College, Oxford, 2015 (“As encryption spreads, U.S. grapples with clash between privacy, security,” *The Washington Post*, April 10th, Available Online at <https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html>, Accessed 08-15-2015)

The odds of passing a new law appear slim, given a divided Congress and the increased attention to privacy in the aftermath of leaks by former NSA contractor Edward Snowden. There are bills pending to ban government back doors into communications devices. So far, there is no legislation proposed by the government or lawmakers to require Internet and tech firms to make their services and devices wiretap-ready.

“There is zero chance of any domestic restrictions on encryption absent a catastrophic event which clearly could have been stopped if the government had been able to break some encryption,” said Michael Vatis, a senior Justice Department cyber-official in the Clinton administration and a partner at Steptoe and Johnson. “That is the only way I could even imagine any restriction on encryption being passed by Congress.”

#### The RSA backdoor their evidence cites didn’t actually happen — RSA denies it.

Arthur 13 — Charles Arthur, Technology Editor at *The Guardian*, 2013 (“Security company RSA denies knowingly installing NSA 'back door',” *The Guardian*, December 23rd, Available Online at <http://www.theguardian.com/technology/2013/dec/23/security-company-rsa-denies-installing-nsa-back-door>, Accessed 08-15-2015)

The security company RSA has denied that it knowingly weakened the encryption it used in its products as part of a secret contract with the US's National Security Agency.

A report from the Reuters news agency on Friday alleged that RSA arranged a $10m contract to use a mathematically weaker formula in a number of its products, which would in effect have created a "back door" for cracking encrypted messages or communications.

RSA initially declined to respond to the reports. But in a blogpost on its site posted Sunday, the company now says: "Recent press coverage has asserted that RSA entered into a 'secret contract' with the NSA to incorporate a known flawed random number generator into its BSAFE encryption libraries. We categorically deny this allegation."

It adds that "We have worked with the NSA, both as a vendor and an active member of the security community. We have never kept this relationship a secret and in fact have openly publicized it. Our explicit goal has always been to strengthen commercial and government security."

## Affirmative

### 2AC — Topicality “Curtail”

#### 1. We Meet — the plan eliminates current programs. “The Patriot Act made such acts lawful, validating the use of programs” that insert encryption backdoors — that’s Mukunth.

#### 2. Prefer Our Evidence — proof that NSA is compelling and encouraging backdoors is overwhelming.

Leinster 14 — Tom Leinster, Chancellor's Fellow and Reader in Mathematics at the University of Edinburgh, has held postdoctoral positions at the University of Cambridge and the Institut des Hautes Études Scientifiques (France) and held an EPSRC Advanced Research Fellowship at the University of Glasgow, holds a Ph.D. in Mathematics from the University of Cambridge, 2014 (“New Evidence of the NSA Deliberately Weakening Encryption,” *The n-Category Café*—a group blog on math, physics, and philosophy, October 17th, Available Online at <https://golem.ph.utexas.edu/category/2014/10/new_evidence_of_nsa_weakening.html>, Accessed 08-14-2015)

One of the most high-profile ways in which mathematicians are implicated in mass surveillance is in the intelligence agencies’ deliberate weakening of commercially available encryption systems — the same systems that we rely on to protect ourselves from fraud, and, if we wish, to ensure our basic human privacy.

We already knew quite a lot about what they’ve been doing. The NSA’s 2013 budget request asked for funding to “insert vulnerabilities into commercial encryption systems”. Many people now know the story of the Dual Elliptic Curve pseudorandom number generator, used for online encryption, which the NSA aggressively and successfully pushed to become the industry standard, and which has weaknesses that are widely agreed by experts to be a back door. Reuters reported last year that the NSA arranged a secret $10 million contract with the influential American security company RSA (yes, that RSA), who became the most important distributor of that compromised algorithm.

In the August Notices of the AMS, longtime NSA employee Richard George tried to suggest that this was baseless innuendo. But new evidence published in The Intercept makes that even harder to believe than it already was. For instance, we now know about the top secret programme Sentry Raven, which

works with specific US commercial entities … to modify US manufactured encryption systems to make them exploitable for SIGINT [signals intelligence].

(page 9 of this 2004 NSA document).

The Intercept article begins with a dramatic NSA-drawn diagram of the hierarchy of secrecy levels. Each level is colour-coded. Top secret is red, and above top secret (these guys really give it 110%) are the “core secrets” — which, as you’d probably guess, are in black. From the article:

the NSA’s “core secrets” include the fact that the agency works with US and foreign companies to weaken their encryption systems.

(The source documents themselves are linked at the bottom of the article.)

It’s noted that there is “a long history of overt NSA involvement with American companies, especially telecommunications and technology firms”. Few of us, I imagine, would regard that as a bad thing in itself. It’s the nature of the involvement that’s worrying. The aim is not just to crack the encrypted messages of particular criminal suspects, but the wholesale compromise of all widely used encryption methods:

The description of Sentry Raven, which focuses on encryption, provides additional confirmation that American companies have helped the NSA by secretly weakening encryption products to make them vulnerable to the agency.

The documents also appear to suggest that NSA staff are planted inside American security, technology or telecomms companies without the employer’s knowledge. Chris Soghoian, principal technologist at the ACLU, notes that “As more and more communications become encrypted, the attraction for intelligence agencies of stealing an encryption key becomes irresistible … It’s such a juicy target.”

Unsurprisingly, the newly-revealed documents don’t say anything specific about the role played by mathematicians in weakening digital encryption. But they do make it that bit harder for defenders of the intelligence agencies to maintain that their cryptographic efforts are solely directed against the “bad guys” (a facile distinction, but one that gets made).

In other words, there is now extremely strong documentary evidence that the NSA and its partners make strenuous efforts to compromise, undermine, degrade and weaken all commonly-used encryption software. As the Reuters article puts it:

The RSA deal shows one way the NSA carried out what Snowden’s documents describe as a key strategy for enhancing surveillance: the systematic erosion of security tools.

The more or less explicit aim is that no human being is able to send a message to any other human being that the NSA cannot read.

Let that sink in for a while. There is less hyperbole than there might seem when people say that the NSA’s goal is the wholesale elimination of privacy.

#### 3. Counter-Interpretation — curtail means to decrease authority. The plan meets because it decreases intelligence agencies’ authority to compel or encourage backdoors.

Merriam-Webster 15 — Merriam-Webster Dictionary, 2015 (“Curtail,” Available Online at <http://www.merriam-webster.com/dictionary/curtail>, Accessed 08-15-2015)

Full Definition of CURTAIL

transitive verb

: to make less by or as if by cutting off or away some part <curtail the power of the executive branch> <curtail inflation>

Examples of CURTAIL

The new laws are an effort to curtail illegal drug use.

School activities are being curtailed due to a lack of funds.

#### 4. Prefer Our Interpretation — it is impossible to know the full extent of NSA activities because their operations are secret, but authority is clearly codified in law. Their interpretation excludes core cases based on the Snowden archive because NSA has not confirmed that those programs still exist.

#### 5. Prefer Contextual Evidence — the plan curtails one of the three major NSA surveillance programs.

Schneier 14 — Bruce Schneier, Chief Technology Officer for Counterpane Internet Security, Fellow at the Berkman Center for Internet and Society at Harvard Law School, Program Fellow at the New America Foundation's Open Technology Institute, Board Member of the Electronic Frontier Foundation, Advisory Board Member of the Electronic Privacy Information Center, interviewed by Rob Price, 2014 (“It's time to break up the NSA,” *CNN*, February 20th, Available Online at http://www.cnn.com/2014/02/20/opinion/schneier-nsa-too-big/index.html, Accessed 07-20-2015)

Broadly speaking, three types of NSA surveillance programs were exposed by the documents released by Edward Snowden. And while the media tends to lump them together, understanding their differences is critical to understanding how to divide up the NSA's missions.

The first is targeted surveillance.

This is best illustrated by the work of the NSA's Tailored Access Operations (TAO) group, including its catalog of hardware and software "implants" designed to be surreptitiously installed onto the enemy's computers. This sort of thing represents the best of the NSA and is exactly what we want it to do. That the United States has these capabilities, as scary as they might be, is cause for gratification.

The second is bulk surveillance, the NSA's collection of everything it can obtain on every communications channel to which it can get access. This includes things such as the NSA's bulk collection of call records, location data, e-mail messages and text messages.

This is where the NSA overreaches: collecting data on innocent Americans either incidentally or deliberately, and data on foreign citizens indiscriminately. It doesn't make us any safer, and it is liable to be abused. Even the director of national intelligence, James Clapper, acknowledged that the collection and storage of data was kept a secret for too long.

The third is the deliberate sabotaging of security. The primary example we have of this is the NSA's BULLRUN program, which tries to "insert vulnerabilities into commercial encryption systems, IT systems, networks and endpoint communication devices." This is the worst of the NSA's excesses, because it destroys our trust in the Internet, weakens the security all of us rely on and makes us more vulnerable to attackers worldwide.

#### 6. No Topic Explosion — “worst-case hypothetical” cases aren’t viable because they aren’t “substantial” and don’t have credible advantages.

#### 7. Good Is Good Enough — debatability is more important than precision. The endless search for the “best” definition distracts from topic education. Don’t vote neg unless our interpretation precludes productive debate.

### Extend: “Plan Ends Current Programs”

#### Recent documents prove NSA is working with companies to weaken encryption.

Maass and Poitras 14 — Peter Maass, Senior Editor at *The Intercept*, and Laura Poitras, documentary filmmaker who worked with Edward Snowden and produced *Citizenfour*—a documentary that won the Oscar for Best Documentary, currently suing the U.S. government for harassment, 2014 (“Core Secrets: NSA Saboteurs In China and Germany,” *The Intercept*, October 10th, Available Online at <https://firstlook.org/theintercept/2014/10/10/core-secrets/>, Accessed 08-14-2015)

The description of Sentry Raven, which focuses on encryption, provides additional confirmation that American companies have helped the NSA by secretly weakening encryption products to make them vulnerable to the agency. The briefing sheet states the NSA “works with specific U.S. commercial entities…to modify U.S manufactured encryption systems to make them exploitable for SIGINT.” It doesn’t name the commercial entities or the encryption tools they modified, but it appears to encompass a type of activity that Reuters revealed last year—that the NSA paid $10 million to the security firm RSA to use a weak random number generator in one of its encryption programs.

#### NSA is inserting backdoors in commercial hard drives now — this is a clear example of a program the plan curtails.

Levine 15 — Greg Levine, Digital News Editor at *Al Jazeera America*, 2015 (“Is the NSA your backdoor man?,” *The Scrutineer*—an *Al Jazeera America* blog, February 17th, Available Online at <http://america.aljazeera.com/blogs/scrutineer/2015/2/17/is-the-nsa-your-backdoor-man.html>, Accessed 08-14-2015)

Kaspersky Lab, a Moscow-based cybersecurity firm, says spy software has been embedded in the hard drives produced by many of the world’s largest computer hardware manufacturers, opening a backdoor to a western surveillance agency.

That agency is widely believed to be the U.S. National Security Agency. Though Kaspersky does not directly name the NSA, the firm does say the code infecting the firmware on the drives is closely related to the Stuxnet virus, the malicious code developed by the U.S. and Israel that caused widespread damage to the Iranian uranium enrichment program.

Though no one is disputing the point anymore, it is still proper at this point to say that the US has never officially admitted involvement with Stuxnet.

A former NSA employee and another former intelligence “operative” confirmed to Reuters that the NSA had developed the ability to hide a surveillance portal on commercial hard drives. Concealing the code in the drive’s firmware is particularly useful because the computer essentially re-infects itself every time it starts up the hard drive.

The proprietary source code on drives is a closely guarded trade secret for hardware manufacturers. Kaspersky said there was zero chance that someone could rewrite drive operating systems based solely on public information, though it is not clear how a government intelligence agency gained access to the code. One drive manufacturer, Western Digital, told Reuters it had “not provided its source code to government agencies”; other manufacturers wouldn’t say if they had cooperated with the NSA on this matter.

The revelation by Kaspersky comes on the heels of last week’s Silicon Valley standoff between tech executives and President Barack Obama. The chief executives of Facebook, Google and Yahoo declined a sit-down with Obama, reportedly to express their displeasure with some aspects of government surveillance and the administration’s latest cybersecurity plan.

The tech sector objects to the government’s behavior in a couple of crucial areas: the intelligence community’s fight against certain kinds of data encryption and/or their insistence on a pass key for government agencies, and the NSA’s hording of so-called “zero-day flaws,” bugs that allow spies or hackers to access supposedly secure computer systems.

Exploiting a zero-day flaw is one possible way in which the NSA gained access to hard drive source code.

In the eyes of U.S. tech companies, continued revelations about the vulnerability of their systems — from the Snowden leaks through today’s Kaspersky report — mean a direct assault not only on their integrity, but on their bottom line. Governments and foreign businesses, alike, have no interest in good ol’ American know how if it means good ol’ Uncle Sam has access to their data and operating systems.