January 2021 Public Forum Evidence Packet

Resolved: The National Security Agency should end its surveillance of U.S. citizens and lawful permanent residents.

Produced by the Bluegrass Debate Coalition at the University of Kentucky

BLUEGRASS DEBATE COALITION

Visit BluegrassDebate.com for additional FREE Public Forum resources

Background Information

The information in this section is designed to provide information that is useful inside and outside of the debate round to ground further discussion. Students may want to read the information in this section completely before moving on to ensure they understand the topic.

Legal Authority for Surveillance

ACLU 2020. The American Civil Liberties Union works in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. 2020. “NSA Surveillance.”
https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance

The National Security Agency’s mass surveillance has greatly expanded in the years since September 11, 2001. Disclosures have shown that, until recently, the government regularly tracked the calls of hundreds of millions of Americans. Today, it continues to spy on a vast but unknown number of Americans’ international calls, text messages, web-browsing activities, and emails.

The government’s surveillance programs have infiltrated most of the communications technologies we have come to rely on. They are largely enabled by a problematic law passed by Congress — the FISA Amendments Act (FAA), which is set to expire this year — along with Executive Order 12,333, the primary authority invoked by the NSA to conduct surveillance outside of the United States. The Patriot Act has also made it easier for the government to spy on Americans right here at home over the past 15 years. Although the Foreign Intelligence Surveillance Court oversees some of the government’s surveillance activities, it operates in near-total secrecy through one-sided procedures that heavily favor the government.

Section 702 of the FISA Amendments Act

Electronic Frontier Foundation 2020. The Electronic Frontier Foundation is the leading nonprofit defending digital privacy. 2020. “Decoding 702: What is Section 702?”

Under authority ostensibly granted by something called Section 702, the U.S. government routinely collects and searches the online communications of innocent Americans without a warrant through what are commonly called “upstream” and “PRISM” (now called “downstream”) surveillance.

Section 702 is a surveillance authority passed as part of the FISA Amendments Act in 2008. That law amended the Foreign Intelligence Surveillance Act of 1978.

Section 702 is supposed to do exactly what its name promises: collection of foreign intelligence from non-Americans located outside the United States. As the law is written, the intelligence community cannot use Section 702 programs to target Americans, who are protected by the

Fourth Amendment's prohibition on unreasonable searches and seizures. But the law gives the intelligence community space to target foreign intelligence in ways that inherently and intentionally sweep in Americans' communications.

Currently, Congress has to renew Section 702 every few years. It was last renewed in 2018 and is set to expire at the end of 2023.

The bill that was most recently passed, S. 139, endorses nearly all warrantless searches of databases containing Americans' communications collected under Section 702. It allows for the restarting of "about" collection, an invasive type of surveillance that the NSA ended in 2017 after being criticized by the Foreign Intelligence Surveillance Court for privacy violations. And it includes a six-year sunset, delaying Congress' best opportunity to debate the limits NSA surveillance.

Executive Order 12,333

ACLU 2020. The American Civil Liberties Union works in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. 2020. "NSA Surveillance."
https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance

Executive Order 12,333, signed by President Reagan in 1981 and modified many times since, is the authority primarily relied upon by the intelligence agencies to gather foreign intelligence outside of the United States. Recent disclosures indicate that the U.S. government operates a host of large-scale programs under EO 12333, many of which appear to involve the collection of vast quantities of Americans' information. These programs have included, for example, the NSA's collection of billions of cellphone location records each day; its recording of every single cellphone call into, out of, and within at least two countries; and its surreptitious interception of data from Google and Yahoo user accounts as that information travels between those companies' data centers located abroad.

Metadata Collection

Iovino 2020. Nicholas Iovino is a reporter for Courthouse News Service, a leading legal and political news wire service. 11-02-2020. "Telecoms Customers Take Fight Over NSA Spying Programs to Ninth Circuit" Courthouse News Service.
https://www.courthousenews.com/telecoms-customers-take-fight-over-nsa-spying-programs-to-ninth-circuit/

Lead plaintiff Carolyn Jewel sued the NSA in 2008, long before NSA contractor Edward Snowden leaked a trove of classified records unveiling details about the NSA's multiple warrantless spying programs in 2013.

The lawsuit claims the NSA used three programs to spy on American citizens in a way that violates the First and Fourth Amendments, the Wiretap Act, Stored Communications Act and Foreign Intelligence Surveillance Act. Those programs include the bulk collection of cellphone and landline records from phone companies, mass interception and searching of Americans'

emails and other internet communications, and collection of metadata from internet communications, such as timestamps and “to” and “from” data from emails.

The government has acknowledged the existence of those programs. It says the bulk collection of internet communications and metadata was discontinued and replaced with more targeted collection of data based on specific selection terms. The bulk collection of phone records continues. The government also maintains that revealing operational details for those programs, such as which telecom giants participated in them, would harm national security.

Section 215 of the PATRIOT Act

McKinney and Crocker 2020. India McKinney and Anderw Cooper are staff members at the Electronic Frontier Foundation, the leading nonprofit defending digital privacy. 04-16-2020. “Electronic Frontier Foundation” Courthouse News Service. https://www.eff.org/deeplinks/2020/04/yes-section-215-expired-now-what

On March 15, 2020, Section 215 of the PATRIOT Act—a surveillance law with a rich history of government overreach and abuse—expired. Along with two other PATRIOT Act provisions, Section 215 lapsed after lawmakers failed to reach an agreement on a broader set of reforms to the Foreign Intelligence Surveillance Act (FISA).

In the week before the law expired, the House of Representatives passed the USA FREEDOM Reauthorization Act, without committee markup or floor amendments, which would have extended Section 215 for three more years, along with some modest reforms.

In order for any bill to become law, the House and Senate must pass an identical bill, and the President must sign it. That didn’t happen with the USA FREEDOM Reauthorization Act. Instead, knowing the vote to proceed with the House’s bill in the Senate without debating amendments was going to fail, Senator McConnell brought a bill to the floor that would extend all the expiring provisions for another 77 days, without any reforms at all. Senator McConnell's extension passed the Senate without debate.

But the House of Representatives left town without passing Senator McConnell’s bill, at least until May 12, 2020, and possibly longer. That means that Section 215 of the USA PATRIOT Act, along with the so-called lone wolf and the roving wiretap provisions have expired, at least for a few weeks.

EFF has argued that if Congress can’t agree on real reforms to these problematic laws, they should be allowed to expire. While we are pleased that Congress didn't mechanically reauthorize Section 215, it is only one of a number of largely overlapping surveillance authorities. The loss of the current version of the law will still leave the government with a range of tools that is still incredibly powerful. These include other provisions of FISA as well as surveillance authorities used in criminal investigations, many of which can include gag orders to protect sensitive information.

In addition, the New York Times and others have noted that Section 215’s expiration clause contains an exception permitting the intelligence community to use the law for investigations

that were ongoing at the time of expiration or to investigate “offenses or potential offenses” that occurred before the sunset. Broad reliance on this exception would subvert Congress’s intent to have Section 215 truly expire, and the Foreign Intelligence Surveillance Court should carefully—and publicly—circumscribe any attempt to rely on it.

Although Section 215 and the two other provisions have expired, that doesn’t mean they’re gone forever. For example, in 2015, during the debate over the USA FREEDOM Act, these same provisions were also allowed to expire for a short period of time, and then Congress reauthorized them for another four years. While transparency is still lacking in how these programs operate, the intelligence community did not report a disruption in any of these “critical” programs at that time. If Congress chooses to reauthorize these programs in the next couple of months, it’s unlikely that this disruption will have a lasting impact.

The Senate plans to vote on a series of amendments to the House-passed USA FREEDOM Reauthorization Act in the near future. Any changes made to the bill would then have to be approved by the House and signed by the President. This means that Congress has the opportunity to discuss whether these authorities are actually needed, without the pressure of a ticking clock.

As a result, the House and the Senate should take this unique opportunity to learn more about these provisions and create additional oversight into the surveillance programs that rely on them. The expired provisions should remain expired until Congress enacts the additional, meaningful reforms we’ve been seeking.

Backdoor Searches

Greene 2017 Robyn Greene is a reporter for Politico. 06-22-2017. How the government can read your email.” Politico
https://www.politico.com/agenda/story/2017/06/22/section-702-surveillance-program-national-security-000463/

Once an American's communications have been collected, they’re no longer protected by the Fourth Amendment warrant requirement, which requires the government to show probable cause before searching your communications. The NSA, CIA and FBI are all permitted to warrantlessly search those communications using Americans’ names, phone numbers, email addresses and other identifiers. While the NSA and CIA track how often they conduct backdoor searches—and they happen a lot at those two agencies: 5,288 times in 2016 alone.

PRISM

Sottek and Kopfstein 2013 T.C. Sotteck and Janus Kopfsteim are reporters for The Verge. 07-17-2013. Everything you need to know about PRISM.” The Verge.
https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

PRISM is a tool used by the US National Security Agency (NSA) to collect private electronic data belonging to users of major internet services like Gmail, Facebook, Outlook, and others. It’s the latest evolution of the US government’s post-9/11 electronic surveillance efforts, which

began under President Bush with the Patriot Act, and expanded to include the Foreign Intelligence Surveillance Act (FISA) enacted in 2006 and 2007.

There's a lot we still don't know about how PRISM works, but the basic idea is that it allows the NSA to request data on specific people from major technology companies like Google, Yahoo, Facebook, Microsoft, Apple, and others. The US government insists that it is only allowed to collect data when given permission by the secretive Foreign Intelligence Surveillance Court.

Classified presentation slides detailing aspects of PRISM were leaked by a former NSA contractor. On June 6th, The Guardian and The Washington Post published reports based on the leaked slides, which state that the NSA has "direct access" to the servers of Google, Facebook, and others. In the days since the leak, the implicated companies have vehemently denied knowledge of and participation in PRISM, and have rejected allegations that the US government is able to directly tap into their users' data.

Both the companies and the government insist that data is only collected with court approval and for specific targets. As The Washington Post reported, PRISM is said to merely be a streamlined system — varying between companies — that allows them to expedite court-approved data collection requests. Because there are few technical details about how PRISM operates, and because of the fact that the FISA court operates in secret, critics are concerned about the extent of the program and whether it violates the constitutional rights of US citizens.

...Many crucial details on how and under what circumstances the NSA collects data are still missing. Legally speaking, surveillance programs rely on two key statutes, Section 702 of the FISA Amendments Act (FAA) and Section 215 of the Patriot Act. The former authorizes the collection of communications content under PRISM and other programs, while the latter authorizes the collection of metadata from phone companies such as Verizon and AT&T.

Evidence to Support Pro Arguments

FBI relies on NSA domestic surveillance and abuses the power

Aaronson 2019. Trevor Aaronson is a contributing writer for The Intercept and a 2020 ASU Future Security Fellow at New America. He is also executive director of the nonprofit Florida Center for Investigative Reporting 10-10-2019. "A Declassified Court Ruling Shows How The Fbi Abused Nsa Mass Surveillance Data" The Intercept. https://theintercept.com/2019/10/10/fbi-nsa-mass-surveillance-abuse/

The NSA's mass surveillance program operates as a series of technologies and authorities that allow the government to intercept communications while in transit over the internet, as well as obtain communications directly from at least eight large technology companies without the need for warrants. These authorities, created in 2008 and renewed in 2018 with some minor reforms, are the result of the expansion of the Foreign Intelligence Surveillance Act. The law created the secret FISA court to oversees its application.

Under traditional FISA authorities established in 1978, the U.S. government may intercept the communications of agents of foreign governments and terrorist organizations if the intelligence community can demonstrate legal justification to the FISA court.

The expansion of FISA authorities, known as Section 702, allows for monitoring to be approved in bulk by the court through what is essentially a recipe for mass surveillance. This surveillance cannot legally target Americans but sweeps up all communications that fit the so-called selectors — akin to search terms, as well as other data based on patterns — and can produce enormous amounts of incidentally collected information, including communications from U.S. citizens. This data is stored and can later be searched by government agencies.

The declassified FISA court ruling revealed that the FBI is the most prolific miner of data about "U.S. persons," a legal term that means any U.S. citizen or foreign national legally in the country. Queries of this data are known as "backdoor searches." In 2017, the FBI ran approximately 3.1 million searches related to U.S. persons, compared to 7,500 combined searches by the CIA and NSA during the same year.

Many of the FBI's searches were not legally justified because they did not involve a predicated criminal investigation or other proper justification for the search, as required by law, according to Boasberg's FISA court ruling.

...A type of FBI investigation known as an "assessment" is one of the primary reasons why the FBI is able to abuse mass surveillance data.

A power created after the 9/11 attacks, assessments allow the FBI to investigate anyone — for reasons as scurrilous as an anonymous tip — suspected of being a potential national security threat. Although the law doesn't establish a time limit, FBI policy generally limits assessments to 72 hours. Because assessments are de facto national security inquiries, the FBI has viewed this as authority to search mass surveillance data for Americans' communications.

The FBI refers about 10,000 investigations for prosecution every year, but at the same time, agents have queried FISA data more than 3 million times in a year while investigating Americans. That suggests agents are using assessments to justify most of its backdoor searches of Americans' communications.

Abuse of mass surveillance data collected by the NSA is common

Goitein 2020. Elizabeth Goitein codirects the Brennan Center for Justice's Liberty & National Security Program. 5-7-2020. "Warrantless Searches at the FBI." Brennan Center for Justice. https://www.brennancenter.org/our-work/analysis-opinion/warrantless-searches-fbi

Under Section 702 of FISA, enacted in 2008, the National Security Agency (NSA) collects hundreds of millions of electronic communications each year. No warrant is required for this collection because the targets of surveillance are foreigners overseas. However, massive amounts of Americans' communications are "incidentally" collected in the process.

Recognizing the inevitability of this spillover, Congress sought to protect Americans' constitutional rights by requiring the government to "minimize" the retention, use, and sharing of information about U.S. persons incidentally acquired under Section 702. Instead, as we learned through Edward Snowden's disclosures in 2013, the FBI routinely helps itself to this data, combing through communications obtained under Section 702 to find Americans' phone calls, e-mails, and text messages for use in purely domestic criminal investigations. This practice is commonly known as "backdoor searches."

When Section 702 came up for reauthorization in late 2017, civil liberties advocates pushed to end backdoor searches by requiring the government to obtain a warrant before conducting U.S. person queries. Ultimately, Congress required the FBI to obtain a warrant in only a small subset of cases — criminal investigations not relating to national security that had reached a certain stage of the investigation — and only after the query is conducted (but before reviewing the contents of any communications).

As minimal as this requirement is, the 2019 statistical transparency report reveals that the FBI has failed to comply with it in literally every relevant case. According to a table in the report, there were six instances in 2018 in which the FBI reviewed the contents of Americans' communications after conducting a backdoor search in a criminal, non-national security case. (These six instances went unreported in the 2018 transparency report because they were not detected until a Department of Justice oversight review in 2019.) The same table indicates that the FBI obtained a warrant to review the contents of those communications exactly zero times. Similarly, for 2019, the table lists one instance in which the FBI ran a backdoor search in a criminal, non-national security case and reviewed communications content, but zero instances in which it obtained a warrant.

Then there are the violations themselves. Congress chose to require a warrant in only a limited category of cases: those in which Americans' privacy and liberty interests are at their very

highest. Predicated criminal investigations are likely to result in prosecutions, and potentially in the deprivation of the target's freedoms. Additionally, because the cases in question do not implicate foreign intelligence or national security, there can be no argument that the information is subject to any exception to the Fourth Amendment's warrant requirement. And there is nothing complicated about the requirement Congress imposed; it should have been an easy matter to educate FBI agents about their new obligation. There is no imaginable excuse for a compliance rate of zero percent.

The news that the FBI violated the warrant requirement is just the latest in a remarkable series of revelations. In the last six months alone, we've learned that the FBI openly flouted the requirement Congress enacted in early 2018 to count the number of backdoor searches it performs; conducted tens of thousands of U.S. person queries without meeting the extremely low standard that applies to any query of Section 702 data (i.e., that the query must be reasonably designed to return foreign intelligence or evidence of a crime); and violated the so-called "Woods procedures" in each of 25 cases reviewed by the Justice Department's Inspector General, resulting in applications to conduct surveillance under Title I of FISA that were riddled with errors. These incidents follow a decade in which the government failed (for several years) to report the collection of purely domestic communications under Section 702, and then failed (for several more years) to comply with the procedures that the Foreign Intelligence Surveillance Court imposed to remedy the resulting Fourth Amendment violation.

Reform will not solve for misuse of data—surveilling U.S. targets must be outright banned

Goitein 2020. Elizabeth Goitein codirects the Brennan Center for Justice's Liberty & National Security Program. 5-7-2020. "Warrantless Searches at the FBI." Brennan Center for Justice. https://www.brennancenter.org/our-work/analysis-opinion/warrantless-searches-fbi

Recognizing the inevitability of this spillover, Congress sought to protect Americans' constitutional rights by requiring the government to "minimize" the retention, use, and sharing of information about U.S. persons incidentally acquired under Section 702. Instead, as we learned through Edward Snowden's disclosures in 2013, the FBI routinely helps itself to this data, combing through communications obtained under Section 702 to find Americans' phone calls, e-mails, and text messages for use in purely domestic criminal investigations. This practice is commonly known as "backdoor searches."

...The lesson should be clear. Multiple FISA authorities that enable either the direct or "incidental" collection of Americans' information rely on statutory and/or court-imposed limitations on how that data is accessed, shared, and kept. Scrupulous adherence to those limitations is necessary to safeguard Americans' privacy and, in many cases, their constitutional rights. After 12 years of repeated and systemic violations, Congress cannot continue to hand the government sweeping powers to collect Americans' most personal data on the assumption that the FBI is following the rules, or that the FISA Court's interventions will put an end to any non-compliance. Instead, in order to adequately protect Americans' rights, Congress must begin to put stricter limits on the scope of collection itself.

NSA fails to comply with restrictions; then lies to cover it up

Gerstein 2018. Josh Gerstein is Politico's Senior Legal Affairs Contributor. 1-19-2018. "NSA deleted surveillance data it pledged to preserve." Politico. https://www.politico.com/story/2018/01/19/nsa-deletes-surveillance-data-351730

The National Security Agency destroyed surveillance data it pledged to preserve in connection with pending lawsuits and apparently never took some of the steps it told a federal court it had taken to make sure the information wasn't destroyed, according to recent court filings.

...Since 2007, the NSA has been under court orders to preserve data about certain of its surveillance efforts that came under legal attack following disclosures that President George W. Bush ordered warrantless wiretapping of international communications after the 2001 terrorist attacks on the U.S. In addition, the agency has made a series of representations in court over the years about how it is complying with its duties.

However, the NSA told U.S. District Court Judge Jeffrey White in a filing on Thursday night and another little-noticed submission last year that the agency did not preserve the content of internet communications intercepted between 2001 and 2007 under the program Bush ordered. To make matters worse, backup tapes that might have mitigated the failure were erased in 2009, 2011 and 2016, the NSA said.

..."It's really disappointing," said David Greene, an attorney with the Electronic Frontier Foundation, which has been leading the prolonged litigation over the program in federal court in San Francisco. "The obligation's been in place for a really long time now. … We had a major dust-up about it just a few years ago. This is definitely something that should've been found sooner."

The last legal showdown over the issue may have actually compounded the NSA's problems. In May 2014, an NSA official known as "Miriam P." assured the court that the data were safe.

The NSA is "preserving magnetic/digital tapes of the Internet content intercepted under the [PSP] since the inception of the program," she wrote, adding that "the NSA has stored these tapes in the offices of its General Counsel."

The agency now says, "regrettably," that the statement "may have been only partially accurate when made."

The latest NSA filing says the ongoing investigation indicates that officials did a "physical inspection" in 2014 to confirm the tapes' presence in the counsel's office storage space. However, "those tapes largely concerned metadata," not the content of communications the NSA intercepted.

...Asked why the Electronic Frontier Foundation hasn't publicized the episode, Greene said his group was waiting for the NSA to turn over data that the plaintiffs in the suits have demanded

before considering next steps regarding the spy agency's failure to maintain the records it said it was keeping.

"We don't know exactly how bad it is," the lawyer said, adding: "Even if you take them at their word that this was just an honest mistake, what it shows is despite your best intention to comply with important restrictions, it can be really difficult to implement. … It shows that with the really tremendous volume of information they're vacuuming up, it is impossible to be meticulous."

Private tech companies have little incentive to deny government requests to spy

Balkin 2014. Jack Balkin is the Knight Professor of Constitutional Law and the First Amendment, Yale Law School. 06-20-2014. "Old School/New School Speech Regulation." Harvard Law Review. https://harvardlawreview.org/2014/06/old-schoolnew-school-speech-regulation/

Aiming surveillance at owners of infrastructure rather than identified persons of interest meshes with the bureaucratic, routinized character of surveillance in the National Surveillance State. The recipients of many, if not most, national security letters are large businesses. They may have little reason to challenge NSLs and gag orders, first, because they want smooth relations with the government, and second, because they probably do not want their customers to know the degree of their cooperation (compelled or not) with government surveillance.

Surveillance has a chilling effect on free speech

Waddell 2016. Waddell is a staff writer for The Atlantic. 4-5-2016. "How Surveillance Stifles Dissent on the Internet." The Atlantic https://www.theatlantic.com/technology/archive/2016/04/how-surveillance-mutes-dissent-on-the-internet/476955/

Most people behave differently when they know they're being watched, a fact that holds both in the real world and online. For many Internet users, the knowledge that their words and actions might be examined by the government leads them to self-censor opinions that they consider outside the mainstream.

That's according to new research from Elizabeth Stoycheff, a journalism professor at Wayne State University. Last week, Stoycheff published a study in Journalism & Mass Communication Quarterly examining whether users would behave differently on social media if they were primed to think about government surveillance first.

To find out, she asked about 250 people to fill out a survey about their news consumption, social-media habits, and general attitudes toward government surveillance. After filling out the survey, participants viewed a fake Facebook news post about airstrikes against ISIS, and reported how willing they'd be to share their opinions on the subject. Finally, they were asked how they thought other Americans feel about the same topic.

A random subset of the survey respondents were shown a special notice before they saw the Facebook post, reminding them that the government "monitor[s] the online activities of individual citizens."

Stoycheff found that people who said they think government surveillance is justified—about two-thirds of the respondents—were likeliest to alter their behavior after they were reminded

about government surveillance. Specifically, these pro-surveillance Internet users tended to avoid sharing opinions that they believed were outside the mainstream.
One of the ways the study tested attitudes about surveillance was by asking people if they agreed with the statement, "The government can track my online behavior because I have nothing to hide." But in fact, the people who agreed that they had "nothing to hide" were the people who were most likely to censor themselves.
In real life, of course, Facebook won't show you a jarring reminder of NSA surveillance every time you post a status about a sensitive topic. But those reminders exist in the wild, Stoycheff says, in the form of news stories about surveillance, and the ubiquitous user agreements that services force you to accept before signing up—each an example of the many ways that your data is captured and used.
And the silencing effects of surveillance are especially harmful for groups of people who generally consider their opinions to be outside the majority.
...These results show that surveillance can create something of an echo chamber, amplifying widely-held opinions and weeding out other perspectives. Surveillance "changes the assumption that we've been working on this whole time, that the Internet is a safe space for deliberation, for people to share their ideas," Stoycheff said. "All of a sudden, that may not be the case."

In high-profile convictions that claimed to rely on surveillance, it wasn't necessary

Barrett 2020. Barrett is a reporter focusing on national security and law enforcement. 9-4-2020. "Surveillance program that gathered Americans' phone data was illegal, court finds." The Washington Post https://www.washingtonpost.com/national-security/phone-records-surveillance-edward-snowden/2020/09/02/97f26498-ed67-11ea-99a1-71343d03bc29_story.html

At the time, officials with the FBI and other intelligence agencies defended the Section 215 program as necessary to prevent attacks, and said it was instrumental to uncovering the case of the four Somali Americans who sent or conspired to send money to al-Shabab.
Then-FBI Deputy Director Sean Joyce told Congress that if not for the information from the phone-records program, the bureau "would not have been able to reopen" the investigation that led to the arrests.

After reviewing classified records, the court wrote in Wednesday's 59-page ruling that the phone surveillance program was not so essential to the case that the convictions should be tossed out.
"To the extent public statements of government officials created a contrary impression, that impression is inconsistent with the contents of the classified record," the judges wrote.

There is bipartisan support to end domestic surveillance

Matishak 2020. Matishak is a cybersecurity reporter. 01-25-2020. "Powerful lawmakers join effort to kill surveillance program protected by Trump administration." Politico
https://www.politico.com/news/2020/01/25/nsa-surveillance-program-congress-104023

Key House and Senate lawmakers are pushing to end a long-troubled National Security Agency surveillance program that gathers records of Americans' telephone calls and text messages in search of potential terrorist connections.

The bipartisan effort to kill what's known as the call detail records program reflects a remarkable political shift. For years, the program — which allows the country's largest intelligence organization to gain access to massive troves of Americans' domestic communications — enjoyed the support of Republicans, Democrats, the intelligence community and every administration from George W. Bush to Barack Obama to Donald Trump.

Lawmakers even voted five years ago to alter the NSA surveillance program but failed to terminate the clandestine system that Edward Snowden exposed in 2013.
But a newfound appetite for curtailing U.S. surveillance practices has emerged among Republicans who have criticized the FBI's eavesdropping of former Trump campaign adviser Carter Page, making them willing to buck the Trump administration's demands that the program be permanently extended.

And intelligence officials aren't making the case to keep to phone records program, either. They've previously admitted it has become too technically complex a burden to maintain.
..."This is a big moment for reformers," Sen. Ron Wyden (D-Ore.), a senior member of the Senate Intelligence Committee, who is looking to push for greater surveillance changes given this new climate in Congress, told POLITICO this month.

Intelligence Chairman Richard Burr (R-N.C.) and Virginia Sen. Mark Warner, the panel's top Democrat, introduced legislation that would render the program essentially inoperable while renewing the law's other surveillance authorities — predominantly used by the FBI — for another eight years.

"I plan to propose to leadership that we move, in some fashion, [our] bill," Burr said.
Senate Judiciary Chairman Lindsey Graham (R-S.C.), whose panel held a contentious public hearing with an NSA official who couldn't offer examples of the program helping in terror probes, said the proposed legislation "works" for him.

Surveillance is too expansive

Greene 2017. Robyn Greene is a reporter for Politico. 06-22-2017. "How the Government Can Read Your Email." Politico
https://www.politico.com/agenda/story/2017/06/22/section-702-surveillance-program-national-security-000463/

Government surveillance has been this big issue for 11 years, and much of the current debate boils down to one obscure-sounding but crucial corner of the law. The controversial program is called Section 702, after the section of the Foreign Intelligence Surveillance Act that allows the government to collect the communications of Americans under certain circumstances. Lawmakers are preparing to reauthorize certain provisions of the FISA law, and Section 702 has become a flash point. Opponents say it infringes on Americans' privacy; supporters see it as crucial to keeping America safe from terrorists. Proponents of reauthorization, like Senate Intelligence Committee Chairman Richard Burr and Director of National Intelligence Dan Coats, make a simple case for preserving Section 702: Intelligence agencies don't use it to target

Americans deliberately—and if any American's information is collected, it's only to protect U.S. national security. In early June, the White House's top counterterrorism official made this argument in the New York Times.

On its surface, it's a persuasive case, but these arguments are misleading. What matters isn't whether Americans were targeted—it's whether their privacy has been violated. So even if Americans are not technically targeted for surveillance under Section 702, the important part is their communications are incidentally collected just the same. More importantly, it's completely false that the government can collect Americans' communications only in cases of national security. In reality, the law is far more expansive: The National Security Agency can collect communications that are just relevant to the foreign affairs of the United States, a huge and dangerous loophole that effectively gives carte blanche to intelligence officials to spy on anyone abroad — including journalists, political and human rights activists, lawyers, scientists, students and business people.

The high rate of "incidental" and "inadvertent" spying on U.S. citizens is due to irresponsible policies and intentional searches for citizens' communications

Levinson-Waldman 2013. Rachel Levinson-Waldman serves as deputy director of the Brennan Center's Liberty & National Security Program. 10-08-2013. "What the Government Does with Americans' Data." Brennan Center for Justice
https://www.brennancenter.org/sites/default/files/publications/What%20Govt%20Does%20with%20Data%20100813.pdf

The FAA expressly contemplates that the international communications of presumptively innocent Americans will be collected. Because the true target is supposedly the non-citizen on the other end of the call or e-mail (or discussed within it), this collection of Americans' information is termed "incidental." Americans' communications are also gathered through "inadvertent" collection, which takes place when the procedures designed to ensure that only non-U.S. persons are targeted fail.

There is reason to believe that "inadvertent" collection, like "incidental" collection, is commonplace. For one, reports indicate that the NSA requires only a 51 percent certainty that its targets are foreign when conducting programmatic surveillance such as PRISM and the upstream collection described below. For another, the NSA's targeting procedures, leaked by Edward Snowden in 2013, provide that "[i]n the absence of specific information regarding whether a target is a U.S. person, a person . . . whose location is not known will be presumed to be a non-United States person." In short, while the NSA has long refused to disclose the number of presumptively innocent Americans whose communications are collected under Section 702, that number is certain to be high. (The agency has recently agreed to make some numbers available, but they appear unlikely to paint the full picture of the program's effect on Americans.) Additionally, the NSA's method of collecting targeted communications occasionally captures entire inboxes, including wholly domestic communications.

One method of collecting Internet content under Section 702 is the PRISM program that Edward Snowden revealed in June 2013. PRISM funnels communications from companies like Google, Apple, and Facebook to the NSA if the communications contain certain search terms chosen by the NSA. Another recently-revealed method of collecting Internet content is “upstream collection.” Unlike PRISM, this program gives the NSA direct access to the data packets traveling through both domestic and international fiber optic cables, also called the Internet “backbone.” Multiple programs employ upstream collection to gather and analyze reams of data. For instance, the NSA is reportedly copying all emails and text messages with one end outside of the United States in order to pull out communications that match certain “selectors” relevant to foreign intelligence, as broadly defined by the FAA. Reports also indicate that the agency has collaborated with domestic telecommunications companies to give it the ability, under certain circumstances, to directly access up to approximately 75 percent of U.S. communications.

On top of these collection authorities, a program called XKEYSCORE allows the government to search essentially any Internet activity using approved search terms. XKEYSCORE’s capabilities are vast; it stored 41 billion records — content and metadata — in a single 30-day period in 2012. Because it selects so much data, it must feed much of it to other specialized databases; these databases make XKEYSCORE the largest data repository for the NSA.

Phone log surveillance is incredibly expensive

Savage 2020. Charlie Savage is a reporter for the New York Times. 02-25-2020. “N.S.A. Phone Program Cost $100 Million, but Produced Only Two Unique Leads” New York Times..
https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html

A National Security Agency system that analyzed logs of Americans’ domestic phone calls and text messages cost $100 million from 2015 to 2019, but yielded only a single significant investigation, according to a newly declassified study.

Moreover, only twice during that four-year period did the program generate unique information that the F.B.I. did not already possess, said the study, which was produced by the Privacy and Civil Liberties Oversight Board and briefed to Congress on Tuesday.

“Based on one report, F.B.I. vetted an individual, but, after vetting, determined that no further action was warranted,” the report said. “The second report provided unique information about a telephone number, previously known to U.S. authorities, which led to the opening of a foreign intelligence investigation.”

The report did not reveal the subject matter of the one significant F.B.I. investigation that was spurred by the Freedom Act program, and it did not divulge its outcome.

Call detail surveillance did not yield valuable intelligence

Privacy and Civil Liberties Oversight Board 2020. PCLOB is working to ensure that efforts by the Executive Branch to protect the nation from terrorism appropriately safeguard privacy and civil liberties. 02-2020. “Report on the

Government's Use of the Call Detail Record Program Under the USA Freedom Act"
https://assets.documentcloud.org/documents/6786642/Privacy-and-Civil-Liberties-Oversight-Board.pdf

The Privacy and Civil Liberties Oversight Board (the "Board) presents this report to provide greater transparency and clarity about the collection of phone call detail records (" CDRs") under the USA Freedom Act. This authority is scheduled to sunset on March 15, 2020.

...USA Freedom Act CDRs were cited in 15 intelligence reports over the program's four-year operation.
Of the 15 reports USA Freedom Act CDRs, FBI received unique information from two of the intelligence reports. Based on one report, FBI vetted an individual, but, after vetting, determined that no further action was warranted. The second report provided unique information about a telephone number, previously known to US authorities,which led to the opening of a foreign intelligence investigation.

Bulk intelligence collection, which leads to incidental domestic surveillance, is not an effective way to stop terrorists

Cahall et al 2014. Bailey Cahall, Peter Bergen, David Sterman, and Emily Schneider are all staff at New America, a think tank dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals. 01-13-2013. "Do NSA's Bulk Surveillance Programs Stop Terrorists?" New America.
https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/

Rep. Mike Rogers (R-Mich.), chairman of the House Permanent Select Committee on Intelligence, said on the House floor in July that "54 times [the NSA programs] stopped and thwarted terrorist attacks both here and in Europe – saving real lives."

However, our review of the government's claims about the role that NSA "bulk" surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading. An in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda's ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance programs to these cases was minimal. Indeed, the controversial bulk collection of American telephone metadata, which includes the telephone numbers that originate and receive calls, as well as the time and date of those calls but not their content, under Section 215 of the USA PATRIOT Act, appears to have played an identifiable role in initiating, at most, 1.8 percent of these cases. NSA programs involving the surveillance of non-U.S. persons outside of the United States under Section 702 of the FISA Amendments Act played a role in 4.4 percent of the terrorism cases we examined, and NSA surveillance under an unidentified authority played a role in 1.3 percent of the cases we examined.

Regular FISA warrants not issued in connection with Section 215 or Section 702, which are the traditional means for investigating foreign persons, were used in at least 48 (21 percent) of the cases we looked at, although it's unclear whether these warrants played an initiating role or were used at a later point in the investigation. (Click on the link to go to a database of all 225 individuals, complete with additional details about them and the government's investigations of these cases: http://natsec.newamerica.net/nsa/analysis).

Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group. Furthermore, our examination of the role of the database of U.S. citizens' telephone metadata in the single plot the government uses to justify the importance of the program – that of Basaaly Moalin, a San Diego cabdriver who in 2007 and 2008 provided $8,500 to al-Shabaab, al-Qaeda's affiliate in Somalia – calls into question the necessity of the Section 215 bulk collection program. According to the government, the database of American phone metadata allows intelligence authorities to quickly circumvent the traditional burden of proof associated with criminal warrants, thus allowing them to "connect the dots" faster and prevent future 9/11-scale attacks. Yet in the Moalin case, after using the NSA's phone database to link a number in Somalia to Moalin, the FBI waited two months to begin an investigation and wiretap his phone. Although it's unclear why there was a delay between the NSA tip and the FBI wiretapping, court documents show there was a two-month period in which the FBI was not monitoring Moalin's calls, despite official statements that the bureau had Moalin's phone number and had identified him. , This undercuts the government's theory that the database of Americans' telephone metadata is necessary to expedite the investigative process, since it clearly didn't expedite the process in the single case the government uses to extol its virtues.

Additionally, a careful review of three of the key terrorism cases the government has cited to defend NSA bulk surveillance programs reveals that government officials have exaggerated the role of the NSA in the cases against David Coleman Headley and Najibullah Zazi, and the significance of the threat posed by a notional plot to bomb the New York Stock Exchange.

The claim that NSA surveillance has stopped more than 50 attacks is not proven

Elliott & Meyer 2013. Justin Elliott and Theodoric Meyer are reporters with Propublica, a nonprofit newsroom that aims to produce investigative journalism in the public interest. 10-13-2013. "Claim on 'Attacks Thwarted' by NSA Spreads Despite Lack of Evidence" Propublica.
https://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence

The NSA itself has been inconsistent on how many plots it has helped prevent and what role the surveillance programs played. The agency has often made hedged statements that avoid any sweeping assertions about attacks thwarted.

A chart declassified by the agency in July, for example, says that intelligence from the programs on 54 occasions "has contributed to the [U.S. government's] understanding of terrorism activities and, in many cases, has enabled the disruption of potential terrorist events at home

and abroad" — a much different claim than asserting that the programs have been responsible for thwarting 54 attacks.

It's impossible to assess the role NSA surveillance played in the 54 cases because, while the agency has provided a full list to Congress, it remains classified.

Surveillance infringes on the work of journalism, stifling the freedom of the press

Human Rights Watch 2014. Human Rights Watch is an independent international organization that investigates and exposes abuses. 06-28-2014. "With Liberty to Monitor All." Human Rights Watch. https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and#

In an attempt to protect their sources, their data, and themselves, many journalists reported modifying their practices—their tradecraft—for investigating stories, communicating with sources, and protecting their notes. The fact that journalists are profoundly altering their tradecraft is evidence of the impact of surveillance on their profession.

Surveillance of tech companies and internet service providers are an attack on the freedom of the press

Balkin 2014. Jack Balkin is the Knight Professor of Constitutional Law and the First Amendment, Yale Law School. 06-20-2014. "Old School/New School Speech Regulation." Harvard Law Review. https://harvardlawreview.org/2014/06/old-schoolnew-school-speech-regulation/

Third, and perhaps most important, owners of private infrastructure are "the press" in the twenty-first century. The "press" in the Press Clause refers both to journalistic institutions and to technologies used to disseminate information. During the colonial period many owners of presses printed not only their own speech but also the speech of their customers. When the government aims at ISPs, broadband providers, and similar providers of digital infrastructure, it is aiming at the modern-day equivalent of "the press" in the technological sense. If one inspected only the black-letter law of the First Amendment, one would learn that prior restraints are extraordinary, legally disfavored, and must last the shortest possible time. In the National Surveillance State, by contrast, prior restraints on infrastructure companies are widespread, enjoy favored legal treatment, and potentially last forever. The prior restraint requested by the government in Pentagon Papers seemed extraordinary and riveted national attention. The prior restraints characteristic of the National Surveillance State are perfectly ordinary and have gained very little attention; they are as ubiquitous as they are invisible.

Data collected from surveillance is stored and used by private corporations, giving them too much power

Leetaru 2019. Kalev Leetaru is a Senior Fellow at the George Washington University Center for Cyber & Homeland Security and contributor to Forbes, covering AI & Big Data. 06-18-2019. "Much Of Our Government Digital

Surveillance Is Outsourced To Private Companies." Forbes. https://www.forbes.com/sites/kalevleetaru/2019/06/18/much-of-our-government-digital-surveillance-is-outsourced-to-private-companies/?sh=61acfd601799

While Hollywood typically portrays government intelligence agencies as all-powerful entities exclusively relying on government lifers, the reality is that modern digital intelligence collection relies heavily on private companies.

The datasets of greatest interest to intelligence agencies are no longer government-owned or produced. They are created and owned by private companies and must be purchased, hacked or legally compelled. Look closely at the Edward Snowden disclosures and a great deal of the NSA's global monitoring intake originates within the data centers and telecommunications networks of the world's private corporations.

Yet rather than exclusively use federal employees to acquire this content, the government relies heavily on outsourcing its collection efforts to federal contractors. These can range from quasi-employees that sit side-by-side with government employees at desks in government buildings on through staffers working in remote modern state-of-the-art office buildings compared with their colleagues in buildings that can often resemble prisons.

...The dangers as government increasingly outsources digital surveillance to private companies is that those companies may not have the same cyber investments as the government enforces at its data centers. Even if data is properly secured, these private companies are frequently granted the right to resell their software and services to others, having improved them by incorporating lessons and even data from government surveillance, such as through their machine learning models.

Putting this all together, the increasing outsourcing of the nation's digital surveillance to private companies creates newfound cyber and privacy risks. Most importantly, it increasingly commercializes the surveillance state, blending the monetization and manipulation of the digital sphere with the kinetically-enforced surveillance of the physical sphere. The future is looking ever more like 1984.

Reforms have shifted power to tech companies, which are ill-equipped to make decisions about privacy

Harvard Law Review 2018. Volume 131, No. 6. "Developments in the Law — More Data, More Problems." https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/

Facebook received 32,716 requests for information from U.S. law enforcement between January 2017 and June 2017. These requests covered 52,280 user accounts and included 19,393 search warrants and 7632 subpoenas. In the same time period, Google received 16,823 requests regarding 33,709 accounts, and Twitter received 2111 requests regarding 4594 accounts. Each company produced at least some information for about eighty percent of requests. In just six months, law enforcement agencies turned to technology companies to

gather evidence for thousands of investigations. Of the many conclusions that one might draw from these numbers, at least one thing is clear: technology companies have become major actors in the world of law enforcement and national security. In his recent article, Professor Alan Rozenshtein dubs these technology companies "surveillance intermediaries" — entities that sit between law enforcement agencies and the public's personal information, and that have the power to decide just how easy or difficult it will be for law enforcement to access that information.

Surveillance intermediaries hold extraordinary power when they decide how to respond to government requests for information — power that may or may not be to the public's benefit. While intermediaries must comply with statutory and constitutional law governing law enforcement requests for information, Rozenshtein explains that they still hold a large degree of discretion when processing those requests: discretion in how critically they evaluate the legality of requests, in slowing down the process by insisting on proceduralism, and in minimizing their capacity to respond to legal requests by implementing encryption. This discretion means that surveillance intermediaries determine, at least in part, the government's access to information about our personal relationships, professional engagements, travel patterns, financial circumstances, and much more. They also impact the government's ability to prevent terrorist attacks, solve murders, and locate missing children. In short, companies such as Facebook, Google, and Twitter are now responsible for decisions that have major consequences for our privacy, on the one hand, and our safety, on the other. This power is not the product of purposeful design — technology companies were not created in order to shield our information from, or deliver our information to, law enforcement agencies. Rather, the role of surveillance intermediary is one that technology companies happened to fall into by virtue of their omnipresence in our day-to-day lives.

The Court charged with oversight does not actually provide oversight—it approves warrants from other agencies that lack evidence

Just Security 2020. Forum on law, rights, and security based at the Reiss Center on Law and Security at New York University School of Law. Editorial Board includes former senior government officials, top civil society attorneys, and law professors. 4-27-2020. "Top Experts Analyze Inspector General Report Finding Problems in FBI Surveillance." Just Security.
https://www.justsecurity.org/69879/top-experts-analyze-inspector-general-report-finding-problems-in-fbi-surveillance/

In December 2019, Inspector General Horowitz issued a report finding serious errors and omissions in the FBI's warrants against Carter Page. Following the Office of Inspector General (OIG) report, Just Security published a series of articles by former government officials and civil society experts–including George Croner, Liza Goitein, Julian Sanchez, Andrew Weissmann–and the Reiss Center and Just Security convened a live panel event on the topic of FISA reform.

Meanwhile, the OIG continued to engage in a broader audit of FISA warrant applications to review the FBI's compliance with its "Woods Procedures"—an internal process meant to ensure,

in the absence of a traditional adversarial process, that there is supporting documentation for all of the factual assertions made in the application for a FISA warrant before the federal court.

In its March interim report, the OIG examined the Woods Files for a sample of 29 FISA applications, including both counterintelligence and counterterrorism investigations, selected from more than 700 applications from eight field offices over the period from October 2014 to September 2019. The OIG's findings were sobering: four out of the 29 FISA applications were fully missing their required Woods Files; each of the remaining 25 contained "apparent errors or inadequately supported facts," with an average of 20 errors per application. The OIG also reviewed 34 separate "accuracy review reports" conducted by the FBI and Department of Justice's National Security Division, covering the same time period and sample of field offices. Despite the deficiencies uncovered by those agency checks, the OIG found that the FBI did not act on them to "help assess the FBI's compliance with its Woods Procedures." In response, the Foreign Intelligence Surveillance Court (FISC) ordered the government to provide it with further information on the 29 applications and to assess the materiality of the discovered problems.

The NSA hoards and exploits software vulnerabilities—putting us all at risk to be hacked

Schneier 2016. Bruce Schneier is the chief technology officer of Resilient, an IBM company, a fellow at Harvard's Berkman Center, and a board member of the Electronic Frontier Foundation. 9-24-2016. "New leaks prove it: the NSA is putting us all at risk to be hacked." Vox. https://www.vox.com/2016/8/24/12615258/nsa-security-breach-hoard

The National Security Agency is lying to us. We know that because of data stolen from an NSA server was dumped on the internet. The agency is hoarding information about security vulnerabilities in the products you use, because it wants to use it to hack others' computers. Those vulnerabilities aren't being reported, and aren't getting fixed, making your computers and networks unsafe.

On August 13, a group calling itself the Shadow Brokers released 300 megabytes of NSA cyberweapon code on the internet. Near as we experts can tell, the NSA network itself wasn't hacked; what probably happened was that a "staging server" for NSA cyberweapons — that is, a server the NSA was making use of to mask its surveillance activities — was hacked in 2013.

...But what I want to talk about is the data. The sophisticated cyberweapons in the data dump include vulnerabilities and "exploit code" that can be deployed against common internet security systems. Products targeted include those made by Cisco, Fortinet, TOPSEC, Watchguard, and Juniper — systems that are used by both private and government organizations around the world. Some of these vulnerabilities have been independently discovered and fixed since 2013, and some had remained unknown until now.

All of them are examples of the NSA — despite what it and other representatives of the US government say — prioritizing its ability to conduct surveillance over our security. Here's one example. Security researcher Mustafa al-Bassam found an attack tool codenamed BENIGHCERTAIN that tricks certain Cisco firewalls into exposing some of their memory,

including their authentication passwords. Those passwords can then be used to decrypt virtual private network, or VPN, traffic, completely bypassing the firewalls' security. Cisco hasn't sold these firewalls since 2009, but they're still in use today.

Vulnerabilities like that one could have, and should have, been fixed years ago. And they would have been, if the NSA had made good on its word to alert American companies and organizations when it had identified security holes.

The Obama administration’s pledge to notify companies about flaws in common software
Over the past few years, different parts of the US government have repeatedly assured us that the NSA does not hoard "zero days" — the term used by security experts for vulnerabilities unknown to software venders. After we learned from the Snowden documents that the NSA purchases zero-day vulnerabilities from cyberweapons arms manufacturers, the Obama administration announced, in early 2014, that the NSA must disclose flaws in common software so they can be patched (unless there is "a clear national security or law enforcement" use).

Later that year, National Security Council cybersecurity coordinator and special adviser to the president on cybersecurity issues Michael Daniel insisted that US doesn't stockpile zero days (except for the same narrow exemption). An official statement from the White House in 2014 said the same thing.

The Shadow Brokers data shows this is not true. The NSA hoards vulnerabilities.

Hoarding zero-day vulnerabilities is a bad idea. It means that we're all less secure. When Edward Snowden exposed many of the NSA's surveillance programs, there was considerable discussion about what the agency does with vulnerabilities in common software products that it finds. Inside the US government, the system of figuring out what to do with individual vulnerabilities is called the Vulnerabilities Equities Process (VEP). It's an inter-agency process, and it's complicated.

There is a fundamental tension between attack and defense. The NSA can keep the vulnerability secret and use it to attack other networks. In such a case, we are all at risk of someone else finding and using the same vulnerability. Alternatively, the NSA can disclose the vulnerability to the product vendor and see it gets fixed. In this case, we are all secure against whoever might be using the vulnerability, but the NSA can't use it to attack other systems.

There are probably some overly pedantic word games going on. Last year, the NSA said that it discloses 91 percent of the vulnerabilities it finds. Leaving aside the question of whether that remaining 9 percent represents 1, 10, or 1,000 vulnerabilities, there's the bigger question of what qualifies in the NSA’s eyes as a "vulnerability."

Not all vulnerabilities can be turned into exploit code. The NSA loses no attack capabilities by disclosing the vulnerabilities it can’t use, and doing so gets its numbers up; it’s good PR. The

vulnerabilities we care about are the ones in the Shadow Brokers data dump. We care about them because those are the ones whose existence leaves us all vulnerable.

Because everyone uses the same software, hardware, and networking protocols, there is no way to simultaneously secure our systems while attacking their systems — whoever "they" are. Either everyone is more secure, or everyone is more vulnerable.

“Back Door” surveillance puts us all at higher risk for cyber attack

Perlroth et al 2013 Nicole Perlroth, Jeff Larson and Scott Shane are reporters for the New York Times. 09-05-2013. “N.S.A. Able to Foil Basic Safeguards of Privacy on Web.” New York Times. https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0

The National Security Agency is winning its long-running secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age, according to newly disclosed documents.

The agency has circumvented or cracked much of the encryption, or digital scrambling, that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and automatically secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world, the documents show.

Many users assume — or have been assured by Internet companies — that their data is safe from prying eyes, including those of the government, and the N.S.A. wants to keep it that way. The agency treats its recent successes in deciphering protected information as among its most closely guarded secrets, restricted to those cleared for a highly classified program code-named Bullrun, according to the documents, provided by Edward J. Snowden, the former N.S.A. contractor.

Beginning in 2000, as encryption tools were gradually blanketing the Web, the N.S.A. invested billions of dollars in a clandestine campaign to preserve its ability to eavesdrop. Having lost a public battle in the 1990s to insert its own “back door” in all encryption, it set out to accomplish the same goal by stealth.

The agency, according to the documents and interviews with industry officials, deployed custom-built, superfast computers to break codes, and began collaborating with technology companies in the United States and abroad to build entry points into their products. The documents do not identify which companies have participated.

The N.S.A. hacked into target computers to snare messages before they were encrypted. In some cases, companies say they were coerced by the government into handing over their master encryption keys or building in a back door. And the agency used its influence as the world’s most experienced code maker to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world.

...But some experts say the N.S.A.'s campaign to bypass and weaken communications security may have serious unintended consequences. They say the agency is working at cross-purposes with its other major mission, apart from eavesdropping: ensuring the security of American communications.

Some of the agency's most intensive efforts have focused on the encryption in universal use in the United States, including Secure Sockets Layer, or SSL; virtual private networks, or VPNs; and the protection used on fourth-generation, or 4G, smartphones. Many Americans, often without realizing it, rely on such protection every time they send an e-mail, buy something online, consult with colleagues via their company's computer network, or use a phone or a tablet on a 4G network.

For at least three years, one document says, GCHQ, almost certainly in collaboration with the N.S.A., has been looking for ways into protected traffic of popular Internet companies: Google, Yahoo, Facebook and Microsoft's Hotmail. By 2012, GCHQ had developed "new access opportunities" into Google's systems, according to the document. (Google denied giving any government access and said it had no evidence its systems had been breached).

"The risk is that when you build a back door into systems, you're not the only one to exploit it," said Matthew D. Green, a cryptography researcher at Johns Hopkins University. "Those back doors could work against U.S. communications, too."

NSA relies on racial profiling

Greenwald and Hussain 2014. Glen Greewald and Murtaza Hussain are writers for the Intercept. 07-08-2014. "Meet the Muslim-American Leaders the FBI and NSA have Been Spying on." The Intercept. https://theintercept.com/2014/07/09/under-surveillance/

According to documents provided by NSA whistleblower Edward Snowden, the list of Americans monitored by their own government includes:
Faisal Gill, a longtime Republican Party operative and one-time candidate for public office who held a top-secret security clearance and served in the Department of Homeland Security under President George W. Bush;
Asim Ghafoor, a prominent attorney who has represented clients in terrorism-related cases;
Hooshang Amirahmadi, an Iranian-American professor of international relations at Rutgers University;
Agha Saeed, a former political science professor at California State University who champions Muslim civil liberties and Palestinian rights;
Nihad Awad, the executive director of the Council on American-Islamic Relations (CAIR), the largest Muslim civil rights organization in the country.
Given that the government's justifications for subjecting Gill and the other U.S. citizens to surveillance remain classified, it is impossible to know why their emails were monitored, or the extent of the surveillance. It is also unclear under what legal authority it was conducted, whether the men were formally targeted under FISA warrants, and what, if anything, authorities found that permitted them to continue spying on the men for prolonged periods of time. But the five

individuals share one thing in common: Like many if not most of the people listed in the NSA spreadsheet, they are of Muslim heritage.

Evidence to Support Neg Arguments

Domestic metadata surveillance stops terrorism with limited privacy invasion

Hines 2013. Pierre Hines is a Defense Council member of the Truman National Security Project. After graduating from West Point, Pierre served as an Army intelligence officer before attending Georgetown Law. 6-9-2013. "Here's How Metadata on Billions of Phone Calls Prevents Terrorist Attacks." Truman Center for National Policy. http://trumancenter.org/doctrine-blog/heres-how-metadata-on-billions-of-phone-calls-predicts-terrorist-attacks/

Yesterday, when NSA Director General Keith Alexander testified before the House Committee on Intelligence, he declared that the NSA's surveillance programs have provided "critical leads to help prevent over 50 potential terrorist events." FBI Deputy Director Sean Boyce elaborated by describing four instances when the NSA's surveillance programs have had an impact: (1) when an intercepted email from a terrorist in Pakistan led to foiling a plan to bomb of the New York subway system; (2) when NSA's programs helped prevent a plot to bomb the New York Stock Exchange; (3) when intelligence led to the arrest of a U.S. citizen who planned to bomb the Danish Newspaper office that published cartoon depictions of the Prophet Muhammad; and (4) when the NSA's programs triggered reopening the 9/11 investigation.

So what are the practical applications of internet and phone records gathered from two NSA programs? And how can "metadata" actually prevent terrorist attacks?

Metadata does not give the NSA and intelligence community access to the content of internet and phone communications. Instead, metadata is more like the transactional information cell phone customers would normally see on their billing statements—metadata can indicate when a call, email, or online chat began and how long the communication lasted. Section 215 of the Patriot Act provides the legal authority to obtain "business records" from phone companies. Meanwhile, the NSA uses Section 702 of the Foreign Intelligence Surveillance Act to authorize its PRISM program. According the figures provided by Gen. Alexander, intelligence gathered based on Section 702 authority contributed in over 90% of the 50 cases.

One of major benefits of metadata is that it provides hindsight—it gives intelligence analysts a retrospective view of a sequence of events. As Deputy Director Boyce discussed, the ability to analyze previous communications allowed the FBI to reopen the 9/11 investigation and determine who was linked to that attack. It is important to recognize that terrorist attacks are not orchestrated overnight; they take months or years to plan. Therefore, if the intelligence community only catches wind of an attack halfway into the terrorists' planning cycle, or even after a terrorist attack has taken place, metadata might be the only source of information that captures the sequence of events leading up to an attack. Once a terrorist suspect has been identified or once an attack has taken place, intelligence analysts can use powerful software to sift through metadata to determine which numbers, IP addresses, or individuals are associated with the suspect. Moreover, phone numbers and IP addresses sometimes serve as a proxy for the general location of where the planning has taken place. This ability to narrow down the location of terrorists can help determine whether the intelligence community is dealing with a domestic or international threat.

Even more useful than hindsight is a crystal ball that gives the intelligence community a look into the future. Simply knowing how many individuals are in a chat room, how many individuals have contacted a particular phone user, or how many individuals are on an email chain could serve as an indicator of how many terrorists are involved in a plot. Furthermore, knowing when a suspect communicates can help identify his patterns of behavior. For instance, metadata can help establish whether a suspect communicates sporadically or on a set pattern (e.g., making a call every Saturday at 2 p.m.). Any deviation from that pattern could indicate that the plan changed at a certain point; any phone number or email address used consistently and then not at all could indicate that a suspect has stopped communicating with an associate. Additionally, a rapid increase in communication could indicate that an attack is about to happen.

Metadata can provide all of this information without ever exposing the content of a phone call or email. If the metadata reveals the suspect is engaged in terrorist activities, then obtaining a warrant would allow intelligence officials to actually monitor the content of the suspect's communication.

In Gen. Alexander's words, "These programs have protected our country and allies . . . [t]hese programs have been approved by the administration, Congress, and the courts." Now, Americans will have to decide whether they agree.

Surveillance has stopped terrorist attacks—examples

Savage 2013. Charlie Savage is a reporter for the New York Times. 06-18-2013. "N.S.A. Chief Says Surveillance Has Stopped Dozens of Plots." The New York Times.
https://www.nytimes.com/2013/06/19/us/politics/nsa-chief-says-surveillance-has-stopped-dozens-of-plots.html

Top national security officials on Tuesday promoted two newly declassified examples of what they portrayed as "potential terrorist events" disrupted by government surveillance. The cases were made public as Congress and the Obama administration stepped up a campaign to explain and defend programs unveiled by recent leaks from a former intelligence contractor.

One case involved a group of men in San Diego convicted of sending money to an extremist group in Somalia. The other was presented as a nascent plan to bomb the New York Stock Exchange, although its participants were not charged with any such plot. Both were described by Sean Joyce, deputy director of the Federal Bureau of Investigation, at a rare public oversight hearing by the House Intelligence Committee.

At the same hearing, Gen. Keith B. Alexander, the head of the National Security Agency, said that American surveillance had helped prevent "potential terrorist events over 50 times since 9/11," including at least 10 "homeland-based threats." But he said that a vast majority of the others must remain secret.

"In the 12 years since the attacks on Sept. 11, we have lived in relative safety and security as a nation," General Alexander said. "That security is a direct result of the intelligence community's

quiet efforts to better connect the dots and learn from the mistakes that permitted those attacks to occur on 9/11."

The hearing was aimed at bolstering public support for surveillance programs after leaks by Edward J. Snowden, a former N.S.A. contractor who was one of about 1,000 systems administrators who ran the agency's networks. Its title: "How Disclosed N.S.A. Programs Protect Americans, and Why Disclosure Aids Our Adversaries."

The Republican chairman of the committee, Representative Mike Rogers of Michigan, and the top Democrat, Representative C. A. Dutch Ruppersberger of Maryland, both defended the surveillance programs revealed by Mr. Snowden and expressed anger over his leaks.

"It is at times like these where our enemies within become almost as damaging as our enemies on the outside," Mr. Rogers said.

As an example of how the domestic calling log database has been used, Mr. Joyce cited the case of several men convicted by a jury in February of raising and sending about $8,500 to Al Shabab, a terrorist group in Somalia. The N.S.A. had flagged the calling activities of one of the men as suspicious, he said.

Representative Mac Thornberry, Republican of Texas, pressed Mr. Joyce to say more, asking, "But there was some connection to suicide bombings that they were talking about, correct?"

Mr. Joyce replied, "Not in the example that I'm citing right here."

Speaking of the calling log program, the deputy director of the N.S.A., John C. Inglis, said that "only 20 analysts at N.S.A. and their two managers, for a total of 22 people, are authorized to approve numbers that may be used to query this database." The N.S.A. has said that it searched for links to fewer than 300 numbers in 2012.

Representative Adam B. Schiff, Democrat of California, pressed General Alexander to explain why the F.B.I. could not simply get the relevant logs of calls linked to a suspicious number without keeping a database of all domestic calls.

General Alexander said he was open to discussing doing it that way, but added, "The concern is speed in crisis."

As a newly disclosed example of how the FISA Amendments Act surveillance authority has been used, Mr. Joyce described a case in which he said the authorities had discovered and disrupted a plot to bomb the New York Stock Exchange.

Monitoring a terrorist in Yemen, the N.S.A. discovered that he was talking to a man named Khalid Ouazzani in Kansas City, Mo. After applying for a separate warrant for Mr. Ouazzani's

communications, they identified two additional conspirators and discovered they were “in the very initial stages” of the stock exchange bomb plot, he said.

Mr. Ouazzani pleaded guilty in 2010 to sending money to Al Qaeda but was not charged with any domestic plots. Later on Tuesday, law enforcement officials said Mr. Joyce had been referring to Sabirhan Hasanoff and Wesam El-Hanafi, two Brooklyn men who pleaded guilty to providing material support to terrorism.

A sentencing memorandum filed by prosecutors contends that in 2008, “at the direction of a senior terrorist leader,” Mr. Hasanoff conducted surveillance of the New York Stock Exchange and sent the leader a one-page report on it.

“The report was rudimentary and of limited use” for any terrorist operation, the memo acknowledges, while nevertheless contending that Mr. Hasanoff’s willingness to conduct such surveillance bolstered the case for giving him a 20-year sentence.

At the hearing, Mr. Thornberry asked Mr. Joyce whether the stock exchange attack was a “serious plot” or just “something that they kind of dreamed about.” Mr. Joyce replied, “I think the jury considered it serious, since they were all convicted.”

Tech Companies serve as a powerful check on NSA surveillance

Rozenshtein 2018. Alan Rozenshtein is a Visiting Assistant Professor of Law at the University of Minnesota Law School and former attorney advisor in the Office of Law and Policy, National Security Division, U.S. Department of Justice. 01-2018. “Surveillance Intermediaries.” Stanford Law Review. https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/01/70-Stan.-L.-Rev.-99.pdf

This vast corporate power would do little to constrain government surveillance if surveillance intermediaries saw their interests as aligned with those of government spies and investigators. But they don’t. Today’s intermediaries have powerful incentives to resist government surveillance. In this regard the 2013 Snowden disclosures were a major inflection point. The massive leaks of classified information revealed a broad surveillance system— and, worse, implicated major Silicon Valley companies as collaborators, causing blowback from domestic civil liberties groups and overseas customers. Although the disclosures motivated some legislative and policy changes, they didn’t alter the core of U.S. surveillance. They did, however, as Julian Sanchez notes, “transform the incentives of the technology companies that maintain [the] architectures” that permit surveillance. This, so far, has been Edward Snowden’s main victory: to increase the incentives for surveillance intermediaries to resist the government.

These incentives fall into two categories. The first is financial. Companies have always had the incentive to lower compliance costs by resisting government surveillance (as long as the costs of such resistance were themselves not too great). But the Snowden disclosures have turned such resistance into an opportunity for product differentiation. For example, when Apple publicly touts how its business model doesn’t need to access user data, part of what it’s doing is jabbing at companies like Google and Facebook, which rely on scanning user data to sell advertisements. Resisting U.S. government surveillance can also improve a company’s global

competitiveness—specifically, its ability to sell its products and services abroad. This is particularly important because the international market provides the bulk of sales for modern technology companies (unlike for the phone companies and retail banks that made up the earlier generation of surveillance intermediaries). For example, Facebook has over two billion active monthly users, of which the vast majority are outside the United States; similarly, over half of the company's ad revenues come from abroad. Given such globally distributed revenue streams, along with the ability to move their key asset—data—instantaneously around the world, today's surveillance intermediaries come as close as we've ever seen to the Platonic ideal of the multinational corporation.

Domestic surveillance is often incidental, and banning it would threaten national security

Bossert 2017. Thomas P. Bossert is the former homeland security and counterterrorism adviser to President Trump. 06-07-2017. "Congress Must Reauthorize Foreign Surveillance" The New York Times. https://www.nytimes.com/2017/06/07/opinion/congress-reauthorize-foreign-surveillance.html

The most important section under consideration, Section 702, allows a federal court to approve and supervise, under specific conditions, the collection of information on foreign persons, in foreign countries, who happen to use American communications services and internet technology. The authority has existed and Congress has reauthorized it under two administrations.

Congress created Section 702 authority to address an intelligence-collection gap that resulted from the evolution of technology in the years after FISA became law in 1978. This gap allowed foreign terrorists to benefit from the legal protections enjoyed by American citizens…

While there are many examples of the value of this tool, they are likely to remain classified for years to preserve our national security. But in one instance that is public, intelligence collected under Section 702 helped prevent Al Qaeda's Najibullah Zazi from conducting a suicide bombing on the New York City subway. Simply put, the use of this authority has helped save lives.

Yet there are two serious misconceptions about what Section 702 permits the government to do that threaten the reauthorization.
First, it does not permit the targeting of Americans. The authority expressly forbids intentional targeting of a United States person for surveillance. Electronic surveillance of Americans, or even foreigners inside the United States, requires an individual court order supported by probable cause.

Second, it does not permit backdoor targeting of Americans, whose communications with foreign persons can be incidentally captured in the process. National security officials may use

search terms or identifiers associated with Americans, such as an email address, to query the information lawfully acquired using Section 702 authority.

...Under President Barack Obama, the National Security Agency used the authority more broadly to acquire internet communications about foreign intelligence targets. Under President Trump's leadership, we have refined the application of this authority to target only those internet communications sent directly to or from a lawful foreign intelligence target. This smart choice will reduce incidental collection on Americans without sacrificing our security. We proposed, and the Foreign Intelligence Surveillance Court approved, the new procedures, which achieve this goal and protect Americans' privacy.

Cabinet officials and security professionals from different agencies will testify on this matter on Wednesday. President Trump stands with them 100 percent on the need for permanent reauthorization of Section 702. Officials from the past two administrations also agree that we cannot have a blind spot in our defenses simply because a foreign terrorist on foreign land chooses an American email provider.

Incidental surveillance of U.S. persons is accidental and corrected once discovered

Levy 2014. Steven Levy is a reporter for Wired. 01-07-2014. "How the NSA Almost Killed the Internet" Wired. https://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/

I am introduced to general counsel Rajesh De; Anne Neuberger, the NSA's point person for partnerships with the private sector; and Rick Ledgett, a deputy director who heads the agency's Media Leaks Task Force, a position created last summer for Snowden damage control.

...The officials paint a picture, though, of a system that fundamentally works. They describe a rigorous training process. They tell me that respect for boundaries is drilled into the psyche of NSA employees from the day they are hired. (As for one embarrassing incident, in which employees tracked their romantic partners, the officials emphasize its rarity—and point out that the abuses were caught by the NSA's own system of frequent polygraph tests.) Ledgett provides an example of what happens when someone's information is mistakenly analyzed. The agency, he says, had tracked a high-value target in South Asia for over a decade before learning that he had once applied for a green card—making him, under NSA rules, a "US person." "As soon we discovered that," Ledgett says, "we dropped collection on him under our Executive Order 12333 authority and canceled 14 years of reports."

The NSA helps to identify key software flaws that could be exploited by adversaries

Nakashima 2020. Ellen Nakashima is a national security reporter for The Washington Post. She covers cybersecurity counterterrorism and intelligence issues. 02-06-2020. "The Cybersecurity 202: Here's why NSA rushed to expose a dangerous computer bug" The Washington Post. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/02/06/the-cybersecurity-202-here-s-why-nsa-rushed-to-expose-a-dangerous-computer-bug/5e3b0f41602ff15f8279a52e/

The National Security Agency is known for keeping secrets. But a bug it recently discovered in Microsoft's operating system was so potentially catastrophic that it fast-tracked a lengthy decision-making process to alert the company and the public as quickly as possible.

The quick disclosure marks a big pivot for the agency, which has historically been eager to hold onto hackable computer bugs that it can use to spy on U.S. adversaries — at least temporarily — before sharing them with companies and has been loath to advertise its role in uncovering them.

It also underscores the havoc the Microsoft flaw could have caused if it was discovered and exploited by U.S. adversaries in Russia, Iran or elsewhere who could have compromised millions of computers for surveillance or sabotage.

“Internally the decision was clear” to disclose, said a government official, who like others interviewed spoke on the condition of anonymity to describe internal discussions. “It was a no-brainer.”

Officials across the government typically convene when they discover dangerous computer bugs to weigh whether it’s better to disclose or hold onto them — an exercise known as the “vulnerabilities equities process” or VEP. The meetings are chaired by the White House's senior director for cybersecurity policy, Grant Schneider.

Yet NSA officials in this case worried that if malicious hackers detected the bug, it could be turned into a weapon to use against Americans and others and wreak havoc before Microsoft had a chance to patch it. The longer they held it, the greater the danger it would be discovered by others. “That's not in anybody's interest,” the official said.

Agency officials notified Schneider of the urgent nature of the case, noting that the VEP charter has a specific exemption allowing an agency to expedite a decision to disclose a flaw in such circumstances without having to convene an interagency meeting. “Since the default position was to release there was no need to go through the whole interagency process and risk something going wrong,” the official said.

The White House agreed the immediate disclosure was the right thing to do.

Before alerting Microsoft, however, the agency conducted its own robust internal discussion in which some argued to keep news of the flaw secret so that NSA hackers could exploit it to gain intelligence overseas. All the agency's senior leaders, however, insisted the bug was too critical to withhold — even temporarily.

The NSA even took the rare step of publicly acknowledging its role in finding the bug and announcing its decision to disclose it — a move that won plaudits for the agency, which has

struggled to present a positive face since former agency contractor Edward Snowden revealed in 2013 a broad surveillance program that scooped up Americans' phone metadata logs.

NSA Cybersecurity Directorate Head Anne Neuberger last month gave two reasons for why the agency did it. "First, we recognized that our partnership is really built on trust," she said, and "a part of building trust is sharing data." Second, she said, "we knew we wanted to lean forward and raise awareness" so that Microsoft could devise a patch. NSA wanted to "ensure that we could be very transparent about that."

Surveillance of U.S. citizens will persist even if NSA isn't doing it

MacAskill et al 2013. Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball are reporters for The Guardian. 06-21-2013. "GCHQ taps fibre-optic cables for secret access to world's communications." The Guardian. https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Britain's spy agency GCHQ has secretly gained access to the network of cables which carry the world's phone calls and internet traffic and has started to process vast streams of sensitive personal information which it is sharing with its American partner, the National Security Agency (NSA).

The sheer scale of the agency's ambition is reflected in the titles of its two principal components: Mastering the Internet and Global Telecoms Exploitation, aimed at scooping up as much online and telephone traffic as possible. This is all being carried out without any form of public acknowledgement or debate.

One key innovation has been GCHQ's ability to tap into and store huge volumes of data drawn from fibre-optic cables for up to 30 days so that it can be sifted and analysed. That operation, codenamed Tempora, has been running for some 18 months.

GCHQ and the NSA are consequently able to access and process vast quantities of communications between entirely innocent people, as well as targeted suspects.

This includes recordings of phone calls, the content of email messages, entries on Facebook and the history of any internet user's access to websites – all of which is deemed legal, even though the warrant system was supposed to limit interception to a specified range of targets.

The existence of the programme has been disclosed in documents shown to the Guardian by the NSA whistleblower Edward Snowden as part of his attempt to expose what he has called "the largest programme of suspicionless surveillance in human history".

...When it came to judging the necessity and proportionality of what they were allowed to look for, would-be American users were told it was "your call".

The Guardian understands that a total of 850,000 NSA employees and US private contractors with top secret clearance had access to GCHQ databases.

Five Eyes Partnership allows circumvention of a congressional ban on domestic surveillance—reform is more necessary

Indrajit et al 2017. Sneha Indrajit, Celia Louie, and Julia Summers are International Policy Institute Cybersecurity Policy Fellows. Jessica Beyer is is a lecturer and research scientist in the Jackson School of International Studies. 10-25-2017. "FISA's Section 702 & the Privacy Conundrum: Surveillance in the U.S and Globally." The Henry M. Jackson School of International Studies at the University of Washington. https://jsis.washington.edu/news/controversy-comparisons-data-collection-fisas-section-702/

For instance, Snowden's data illustrated that the so-called "Five Eyes" (U.S., U.K., Canada, Australia, New Zealand) all engage in upstream data collection. These countries then share data on each other's citizens, circumventing strict national laws around this type of surveillance. The need to use such tactics to evade national law is because the Five Eyes' are all liberal democracies. In contrast, citizens in countries such as China and Russia have no expectations that they are not being surveilled. Thus, upstream collection there would not be considered noteworthy – except to geopolitical adversaries that might object to the practice.

NSA has a unique technical capability to fight cybercrime with targeted surveillance operations

Bojarski 2015. Kamil Bojarski is a LLM candidate at Nicolaus Copernicus University, Torun, Poland. He is president of the Student Scientific Group of ICT Law at Nicolaus Copernicus University and author of a blog dedicated to legal aspects of network security lawsec.net. 2015. "Dealer, Hacker, Lawyer, Spy: Modern Techniques and Legal Boundaries of Counter-cybercrime Operations." The European Review of Organised Crime 2(2), 2015, 25-50. https://standinggroups.ecpr.eu/sgoc/wp-content/uploads/sites/51/2020/01/bojarski.pdf

The analysis of documents released by Edward Snowden provides great insight into the technical means available to signal intelligence and enables a comparison against methods used by civilian law enforcement. Asymmetric capabilities is best described in these terms: law enforcement routinely use traditional investigative techniques, while counter-cybercrime operations require involvement of cybersecurity experts; SIGINT agencies routinely engage in extremely advanced surveillance methods, while targeted operations involve methods beyond capabilities and resources of any civilian law enforcement agency.

Programs which gained most popularity in media were mass surveillance programs such as PRISM or TEMPORA. However in terms of counter-cybercrime operations the capability of targeted attacks is significantly more important. Mass surveillance programs relied on massive storage capabilities and legal authority to coerce service providers to cooperate with intelligence agencies. On the other hand, targeted operations present the cutting-edge technology and evident technological superiority available to SIGINT.

One of the operational units exposed during NSA document leaks was the Office of Tailored Access Operations (TAO). Active since 1998 aimed at infiltrating, monitoring and gathering intelligence from computer networks. Effectiveness of TAO relied on obtaining data from upstream collection, a term used by the NSA to describe interception of data from "internet backbone"—major internet routers, cables, and switches. One famous example of upstream

collection is Room 641A, a telecommunication interception facility where the NSA tapped directly into fibre optic cables of telecommunication services provider AT&T. This type of data interception was conducted under program XKEYSCORE. TAO has developed 'fingerprints' of specific hardware-software configurations which then could be correlated with data obtained by upstream collection. Due to the global nature of the internet, even tapping US based fibre cables provided targets from all over the world (Gallagher and Greenwald, 2014). To perform successful remote operations and remain undetected TAO employed the QUANTUMSQUIRREL program, which enabled masquerading as any routable IP address in the world (a technique commonly known as "spoofing"). Unfortunately, no documents regarding the technical side of QUANTUMSQUIRREL were leaked. What is known however, is that the whole suite of penetration facilitating tools was developed under the umbrella term "QUANTUM" (NSA, 2010). These tools provided multiple capabilities; most prominent was QUANTUMINSERT, which was able to mimic whole services such as YouTube or Yahoo. After capturing enough data about a target's online behaviour, the tool was able to redirect traffic from the subject's computer to NSA servers without any noticeable change on victim's side (Schneier, 2013b). In reality however, after accessing a particular service, QUANTUM launched tailored exploits enabling access to targeted machines (NSA, 2010). This type of attack is available exclusively to government agencies, as it requires access to the internet backbone. This is because an attacker requires a privileged position on the network in order to win race condition and therefore responds to the request of the user before the legitimate server does. Another important tool is FoxAcid. Described in NSA presentations as an "exploit orchestrator." The purpose of FoxAcid was to launch targeted attacks at specific machines. FoxAcid ran on publicly accessible servers, which waited for so-called FoxAcid tags (Schneier, 2013b). A tag being a specially prepared URL (Uniform Resource Locator), which commanded FoxAcid to launch an attack against a computer. TAO was tricking victims into using tagged URLs through a variety of methods including injection and phishing attacks. Frameworks were also equipped with several payloads, updated on regular basis by TAO. To remain effective for a considerable period of time FoxAcid used a sophisticated detection prevention mechanism, able to deceive commercial anti-virus software and modify operating systems in order to survive reboot. The type of attack was based on an assessment made by FoxAcid: in case of well-secured systems, it could launch zero day exploit, or even decide not to attack at all. As, by definition, it is only possible to use zero-day exploit once FoxAcid may however, decide that using it would be wasteful. Because of how automated this process of exploitation is, some researchers criticised the system claiming that it provides enormous power to employees who do not fully comprehend the gravity of their actions (Schneier, 2013a). Furthermore, these methods are not overly different from those used by cybercrime groups, as they rely on massive propagation of malware, similar to i.e. spread of botnet[1].

NSA domestic surveillance was essential to shutting down SilkRoad, a cornerstone of the Dark Web

Bojarski 2015. Kamil Bojarski is a LLM candidate at Nicolaus Copernicus University, Torun, Poland. He is president of the Student Scientific Group of ICT Law at Nicolaus Copernicus University and author of a blog dedicated to legal aspects of network security lawsec.net. 2015. "Dealer, Hacker, Lawyer, Spy: Modern Techniques and Legal Boundaries of Counter-cybercrime Operations." The European Review of Organised Crime 2(2), 2015, 25-50. https://standinggroups.ecpr.eu/sgoc/wp-content/uploads/sites/51/2020/01/bojarski.pdf

Launched in February 2011 and shut down in October 2013, SilkRoad became a flagship Tor drug marketplace. Its administrator, Ross Ulbricht, also known as Dread Pirate Roberts, was charged with drug trafficking conspiracy, computer hacking conspiracy, and money laundering conspiracy (United States of America v. Ross Ulbricht, Sealed Complaint, 13 MAG 2328). Ultimately, in January 2015, Ulbicht was convicted on all charges laid in relation to SilkRoad. Due to substantial evidence gathered during investigation, which includes Ulbricht's personal journal describing details of his criminal activity, the chance of a successful appeal or retrial is low (Greenberg, 2015; McCoy, 2015). The case of Ross Ulbricht is an example of how tracking down criminals who use modern encryption solutions relies on performing technically complex operations combined with exploiting negligent behaviour of perpetrators. The SilkRoad service looked and worked like an ordinary e-commerce platform. Users had to make individual accounts in order to enter buy or sell products. Offers were catalogued into categories and users were able to comment on the quality of service after each transaction. Also an escrow service was available in order to ensure safety of transactions and prevent frauds (Christin, 2012). Furthermore, Silk Road administration provided guidelines on how to ensure the safety of transactions. Guidelines also covered technological aspects with instructions relating to the usage of Tor browser, cryptography, and system configuration (United States of America v. Ross Ulbricht, Sealed Complaint, 13 MAG 2328). Customer service, similar to those used by legitimate e-commerce platforms, was also implemented to deal with technical problems.

Two major safeguards secured SilkRoad's servers location and the identity of its owner. First, the use of the Tor network—SilkRoad was available only as a hidden service. Tor is a software which enables obscuring Internet Protocol (IP) addresses of its users by utilising so-called "onion routing". Traffic in Tor network is sent through a number of relays voluntarily hosted by users around the world. Relays are computers used to transmit data to its destination. The term onion refers to layers of encryption used—data, including IP address, is encrypted and send through a circuit of relays, each of them adding another layer of encryption (Dingledine et al., 2004). The point is that each relay decrypts only the data required to establish another circuit (or to reach the destination, in case of final relay). As a result, an individual relay does not know about the origin of traffic and as a result, traffic cannot be traced back to the original user.

...The deanonymisation of Tor users ranks high on the list of priorities of targeted operations (NSA, 2013b). In fact, the agency developed an entire program for identifying machines within Tor network, using the functionality of QUANTUM (NSA, 2007). Using upstream collection of data, the NSA created a database of Tor users – which is easy to achieve, as by design all Tor clients should look the same. To distinguish individual users QUANTUM analysed each system it detected, and produced software-hardware 'fingerprints' of system configuration. Gathered patterns were automatically processed and matched with possible FoxAcid attacks for further exploitation. According to presentations on project EGOISTICALGOAT/EGOISTICALGIRAFFE, the NSA tried to attack specific Tor users by targeting the Firefox browser included as a part of the Tor bundle (NSA, 2007). Similarities between this proposition and FBI operations "Magento" and "Torpedo" show that in the case of Tor, identification tools used by the agencies are different but the ultimate method of attack remains similar. Furthermore, the NSA admits that it

is impossible to deanonymise a significant portion of network (NSA, 2012), and that Tor remains the best online anonymity tool available (NSA, 2013c). Targeting Tor is also becoming part of official operations. In December 2014, British Prime Minister David Cameron officially announced that GCHQ would cooperate with the National Crime Agency to tackle child pornography groups in dark net (gov.uk, 2014).

High rates of approval from FISA courts show the agency's ability to self-regulate

Frits 2014. Clara Fritts and Scott F. Mann are research associates with the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.. 2-27-2014. "Fact Sheet: The Foreign Intelligence Surveillance Court." Center for Strategic and International Studies. https://www.csis.org/analysis/fact-sheet-foreign-intelligence-surveillance-court

While there are merits to strengthening the FISC, the criticisms lack insight into the workings of the Court. The high rate of approvals by the FISC is due to an intensive vetting process by the Justice Department (DOJ) and the legal departments of the IC. What follows an application for a warrant is an iterative process between the federal government and the Court, whereby the court provides comments and Justice amends the application until it is ready for approval. In a three month period during the summer of 2013 Judge Walton, "observed that 24.4% of matters submitted ultimately involved substantive changes to the information provided by the government or to the authorities granted as a result of Court inquiry or action."

The ex parte nature of proceedings before the FISC is fundamentally sound and has worked well for decades in adjudicating the Government's applications for authority to conduct electronic surveillance or physical searches in the national security context under FISA.

Domestic surveillance is necessary to protect against cyber attacks

Goldsmith 2013. Jack Goldsmith is a contributing editor for the New Republic, teaches at Harvard Law School and is a member of the Hoover Institution Task Force on National Security and Law. 10-09-2013. "We Need an Invasive NSA." The New Republic. https://newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks

The Times editorial board is quite right about the seriousness of the cyber- threat and the federal government's responsibility to redress it. What it does not appear to realize is the connection between the domestic NSA surveillance it detests and the governmental assistance with cybersecurity it cherishes. To keep our computer and telecommunication networks secure, the government will eventually need to monitor and collect intelligence on those networks using techniques similar to ones the Times and many others find reprehensible when done for counterterrorism ends.

The fate of domestic surveillance is today being fought around the topic of whether it is needed to stop Al Qaeda from blowing things up. But the fight tomorrow, and the more important fight, will be about whether it is necessary to protect our ways of life embedded in computer networks.

Anyone anywhere with a connection to the Internet can engage in cyber-operations within the United States. Most truly harmful cyber-operations, however, require group effort and significant skill. The attacking group or nation must have clever hackers, significant computing power, and

the sophisticated software—known as “malware”—that enables the monitoring, exfiltration, or destruction of information inside a computer. The supply of all of these resources has been growing fast for many years—in governmental labs devoted to developing these tools and on sprawling black markets on the Internet.

Telecommunication networks are the channels through which malware typically travels, often anonymized or encrypted, and buried in the billions of communications that traverse the globe each day. The targets are the communications networks themselves as well as the computers they connect—things like the Times’ servers, the computer systems that monitor nuclear plants, classified documents on computers in the Pentagon, the nasdaq exchange, your local bank, and your social-network providers.

To keep these computers and networks secure, the government needs powerful intelligence capabilities abroad so that it can learn about planned cyber-intrusions. It also needs to raise defenses at home. An important first step is to correct the market failures that plague cybersecurity. Through law or regulation, the government must improve incentives for individuals to use security software, for private firms to harden their defenses and share information with one another, and for Internet service providers to crack down on the botnets—networks of compromised zombie computers—that underlie many cyber-attacks. More, too, must be done to prevent insider threats like Edward Snowden’s, and to control the stealth introduction of vulnerabilities during the manufacture of computer components—vulnerabilities that can later be used as windows for cyber-attacks.

And yet that’s still not enough. The U.S. government can fully monitor air, space, and sea for potential attacks from abroad. But it has limited access to the channels of cyber-attack and cyber-theft, because they are owned by private telecommunication firms, and because Congress strictly limits government access to private communications. “I can’t defend the country until I’m into all the networks,” General Alexander reportedly told senior government officials a few months ago.

For Alexander, being in the network means having government computers scan the content and metadata of Internet communications in the United States and store some of these communications for extended periods. Such access, he thinks, will give the government a fighting chance to find the needle of known malware in the haystack of communications so that it can block or degrade the attack or exploitation. It will also allow it to discern patterns of malicious activity in the swarm of communications, even when it doesn’t possess the malware’s signature. And it will better enable the government to trace back an attack’s trajectory so that it can discover the identity and geographical origin of the threat.

Incidental collection of U.S. persons’ communications is limited in scope and impossible to separate from an essential foreign surveillance

American Bar Association Homeland Security Law Institute 2017. The ABA hosted a panel featuring experts Elisabeth Collins, board member of the Privacy and Civil Liberties Oversight Board; Stuart J. Evans, deputy assistant attorney general at the National Security Division, U.S. Department of Justice; Glenn Gerstell, NSA general counsel;

and Caroline Lynch, founder and owner of Copper Hill Strategies public policy shop. The following is a summary of those experts' opinions 09-29-2017. "FISA reauthorization necessary to keep homeland safe, panel concludes." The American Bar Association. https://www.americanbar.org/news/abanews/aba-news-archives/2017/09/fisa_reauth/

Section 702 of the FISA Amendments Act of 2008 allows the National Security Agency to tap into the communications of "non-U.S. persons" outside the United States. However, FISA warrants require investigators to demonstrate to a FISA court that there is probable cause to believe the target may be acting as an unlawful foreign agent.

Many in the intelligence community want Congress to not just renew the act, which expires on Dec. 31, but to make it permanent law.

A panel of experts at the 2017 ABA Homeland Security Law Institute gathered to discuss how the act is used to keep Americans safe and if it should be renewed.

The reauthorization of Section 702 is the No. 1 priority of the intelligence community and the Department of Justice, said Stuart J. Evans, deputy assistant attorney general at the National Security Division, U.S. Department of Justice.

Glenn Gerstell, general counsel of the NSA, agrees, saying that it's hard to overstate the importance of Section 702 authority. "It's arguably the single most important operational statute that the intelligence agencies have," he said. It is used by the NSA, CIA, FBI and the National Counterterrorism Center to inform us on counterterrorism, weapons of mass destruction and proliferation, protection of our troops and our cybersecurity efforts. It has strong oversight by all three branches of government and is critically important to our intelligence agencies, Gerstell said.

The act authorizes the electronic surveillance only of foreign citizens on foreign soil, Evans said. "No Americans, either here or abroad, can be targeted for surveillance."

That said, section 702 of the FISA does allow the NSA to listen in on American citizens caught up "incidentally" without a warrant, troubling some. Incidental collection occurs when a person is in contact with a surveillance target. If the NSA believes the information collected contains evidence of a crime, the NSA can share those communications with law enforcement or other relevant agencies.

Under one aspect of the NSA's warrantless surveillance program, telecommunications companies like AT&T and Verizon give copies of emails that cross the international border and contain a search term that identifies foreigners overseas whom the government has targeted for surveillance; email addresses are one example. The agency calls this "upstream" collection. Until 2013, it was not publicly known that the equipment installed on network switches was systematically sifting all cross-border internet traffic and sending to the NSA messages containing such a targeted email address anywhere—not just emails to or from targets, but also between other people who talk about the targets. This practice, so-called "abouts" collection,

was discovered amid the fallout from the leaks by the former intelligence contractor Edward J. Snowden.

Gerstell said it's impossible to know exactly how many Americans are caught up in incidental collections, but estimated numbers are low and have been reported to Congress. He added that the only time an American could be caught in incidental collection is if that American is in direct contact with a foreign intelligence target.

Panelist Elisabeth Collins, board member of the Privacy and Civil Liberties Oversight Board, an independent, bipartisan agency within the executive branch, said that after studying the law for a year, the board recommended changes to Section 702 to strengthen privacy protections and restrictions, and all of the recommendations have been implemented.

Oversight is more important than restricting data access

Rosenzweig 2013. Paul Rosenzweig is founder of homeland security consulting company Red Branch Consulting and senior adviser to The Chertoff Group. Rosenzweig formerly served as deputy assistant secretary for policy in the Department of Homeland Security. 10-29-2013. "The NSA Doesn't Need Wholesale Reform, Just Greater Oversight." The New Republic. https://newrepublic.com/article/115392/nsa-reform-not-essential-congressional-oversight

First, we can't with one breath condemn government access to vast quantities of data about individuals as a return of "Big Brother," and at the same time criticize the government for its failure to "connect the dots" (as we did, for example, during the Christmas 2009 bomb plot attempted by Umar Farouk Abdulmutallab).

More to the point—large scale data analytical tools of the type the NSA is apparently using are of such great utility that governments will expand their use, as will the private sector. Old rules about collection and use limitations are no longer technologically relevant. If we value privacy at all, these ineffective protections must be replaced with new constructs. The goal then is the identification of a suitable legal and policy regime to regulate and manage the use of mass quantities of personal data.

We should therefore favor those reforms that create delegated or calibrated transparency (enough to enable oversight without eliminating essential capabilities) and respond to the new paradigm of data analytics and privacy (by controlling use rather than collection).

...Phone Company Data Retention: Some have suggested that, instead of NSA collecting and retaining telephone call metadata, Congress should amend the law and impose a data retention requirement on phone companies and ISPs, requiring them to retain metadata for a fixed period of time, say five years. NSA and the FBI would, in turn, only be able to access this data set after a FISC court had passed on the validity of the request and determined that it met some evidentiary threshold, say, of relevance.

While the idea is attractive it is, in the end, more problematic than beneficial. To begin with, the FISC pre-access review would be more privacy protective–but it would achieve this protection in

the old fashioned way of limiting access to the underlying data. More effective ways that focus on managing end uses rather than collection are to be preferred.

...To my mind the system of delegated transparency, where Congress stands in for the general public, has worked reasonably well–allowing us to use intelligence capabilities while minimizing the risks of abuse of law. Today, however, thanks to the Snowden disclosures, that system is under assault. Most who challenge the system do so from the best of motives. But there are some whose calls for transparency mask the intention of diminishing American capabilities.

And that means that in this post-Snowden era, this House Intelligence Committee (and its Senate counterpart) bear a great responsibility. To them falls the task of defending the integrity of our current system of intelligence oversight. While we have discussed possible reforms to the NSA's programs, both legislative and structural, the critical insight is that, despite the hue and cry, the system is not badly broken. In can be improved, but in the main it has produced a reasonably effective system of oversight that, if the public record is an accurate reflection, resulted in precious little abuse of the sort we ought to fear.

Congress should be proud of that record and of your role in creating it. Can the Intelligence Committees, perhaps, do a better job of oversight? No doubt. But in the end, notwithstanding the calls for reform and the many plausible reforms you might consider, this Committee should defend the essential structure of our current system. And that, in the end, means rejecting most calls for wholesale reform and complete transparency, and, instead, defending the role of graduated or delegated oversight