Harvard Model Congress
Boston 2024

NATIONAL SECURITY AGENCY OVERSIGHT

By John Cooke

INTRODUCTION

An aircraft flies into the South Tower during the 9/11 terror attacks

KQED

On September 11, 2001, the United States of America was struck by a coordinated terrorist attack orchestrated by the terror group Al-Qaeda. The attacks killed nearly 3,000 Americans, making it the deadliest coordinated terrorist attack on American soil in its history (Bergen 2023).

On October 26, 2001, in immediate response to the 9/11 attacks, President George W. Bush signed the USA PATRIOT Act into law (Rep. Sensenbrenner, *H.R.3162 - 107th Congress (2001-2002)*). The act intended to enhance the investigatory and surveillance tools of law enforcement agencies in order to prevent future attacks. However, the act emboldened many federal agencies to pursue more invasive methods of spying — often targeted toward Muslim and Arab Americans — and gave them unprecedented access to citizen communications, private records, and secret searches (ACLU, 2023).

One such law enforcement agency, the National Security Agency (NSA), quickly found itself under fire due to its invasive usage of the Patriot Act. In May 2013, Edward Snowden, a former intelligence contractor, downloaded up to 1.5 million secret and top-secret documents, resulting in about 7,000 being leaked to the public. The documents revealed that the NSA had collected telephone and email records from millions of citizens from around the world and had even **bugged** telephones belonging to foreign leaders and dignitaries (Szoldra, 2016).

The revelation of these mass spying programs has eroded public trust in the NSA and the wider American intelligence state. As members of the U.S. Senate Select Committee on Intelligence, you are entrusted with the oversight of these agencies and organizations. For the NSA to effectively and ethically carry out its mission of

President George W. Bush signs the USA PATRIOT Act into law.

The White House

national security, Congress must find ways to restore public trust in the institution and hold it accountable for its actions.

EXPLANATION OF THE ISSUE

Historical Development

Bug *– to conceal a miniature microphone in (a room or device) in order to monitor or record someone's conversations.*

The NSA originally started as the Signal Intelligence Service (SIS) in 1929 (Heiligenstein, 2014). The SIS specialized in intercepting enemy communications and decoding messages, making the organization instrumental in defeating the Japanese in World War II. After the war, President Harry Truman reorganized American signals intelligence under the National Security Agency (NSA) in 1952. Shortly after, the NSA moved to its headquarters in Fort Meade, MD, where it is still based today.

In the early days of the NSA, presidents used it to spy on political dissidents.

In its early days, the NSA was a secret organization. However, as the scope of the NSA's operations and the size of its workforce increased, denying its existence became far more difficult (Heiligenstein, 2014). The investigation during the aftermath of the 1970s Watergate scandal —where President Richard Nixon was exposed for spying on his Democratic opponents— flung the NSA into the public eye for the first time. An investigation by the U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities revealed that the NSA had been spying on the correspondence of U.S. citizens as they entered and exited the United States. The investigation also found that the NSA had spied on the communications of prominent civil rights leaders such as Martin Luther King Jr., Muhammad Ali, Jane Fonda, and even two active U.S. Senators (Heiligenstein, 2014). Although The NSA had launched this program in 1967 to monitor suspected terrorists and drug traffickers, successive presidents used it to quell uprisings and spy on political dissidents (Heiligenstein, 2014).

FISA Court *— A special federal court which approves requests from the NSA to surveil American citizens.*

The Senate Committee's findings led Congress to pass the Foreign Intelligence Surveillance Act (FISA) in 1978, which set strict guidelines for what the NSA could collect and how they could collect it (Heiligenstein, 2014). Under FISA, the NSA was no longer free to conduct warrantless surveillance on American citizens and political opponents (Heiligenstein, 2014). The organization would now have to get prior approval from a special surveillance court, known as the **FISA Court**.

In the aftermath of the USA PATRIOT Act's passage, the NSA once again found itself equipped to monitor the phone and digital correspondence of American citizens without a warrant from the intelligence court. Although President Bush formally ended the warrantless wiretap program in 2007, documents leaked by Edward Snowden found that had continued to secretly gather Internet and

Edward Snowden, the former intelligence contractor who leaked millions of classified NSA documents

NPR

telephone data from millions of Americans (Heiligenstein, 2014). He also revealed that the agency was spying on adversaries and even allies abroad, including wiretapping the private telephone of German Chancellor Angela Merkel (Szoldra, 2016). These documents also uncovered many previously unknown facts about the American intelligence apparatus, including that the United States carried out 231 offensive cyberattacks in 2011, bugged the offices of at least 38 foreign embassies, and that the NSA possessed the ability to access data directly from all major smartphones on the market, including iPhones, Androids, and BlackBerries (Szoldra, 2016). These discoveries prompted swift outrage across the United States, with many elected officials calling for increased accountability and transparency from the intelligence community.

There has been little evidence of substantive reform in the wake of the Snowden leaks. In 2014, President Obama announced that the NSA would no longer store citizens' phone data. In 2015, Congress passed the USA FREEDOM Act, which sought to reform the intelligence agency and curb some of the NSA's most egregious mass data collection practices (Rep. Sensenbrenner, *2015*). However, the Office of the Director of National Intelligence released a report in 2016 that showed that the NSA nearly tripled the amount of phone records that it had collected before the bill's passage (Savage, 2018). Since this revelation, little information has been released concerning the NSA, and the level to which they are adhering to federal regulations is currently unknown.

Despite legislation which intended to minimize the data collected from US Citizens, the NSA collected nearly three times as much data the following year.

Scope of the Problem

When considering how to best regulate the National Security Agency, there are a variety of problems and specific issue areas that must be addressed.

Data Collection from American Citizens

President Barack Obama delivers a speech on NSA Spying reports, 2014

The Nation

Many American citizens are concerned with the NSA engaging in mass collection of private communications data. According to multiple statements from high-ranking government officials, including multiple NSA Directors and President Obama, the NSA does not directly target Americans in its data collections and communication monitoring efforts. Rather, the NSA targets select foreign nationals who are flagged by a variety of agencies as possible threats to national security (Savage, 2018). Once those individuals are flagged, the NSA will monitor all of their communications into and out of the United States, which may be conversations with American citizens.

Although this flagging process seems straightforward, there is a great deal of missing information relating to the process. First, the NSA has not revealed how many individuals are flagged or how they become flagged in the first place. If the NSA has flagged thousands

of foreign nationals, then they are most likely, by proxy, monitoring the outgoing conversations of millions of Americans.

If the NSA has flagged thousands of foreign nationals, then they are most likely, by proxy, monitoring the outgoing conversations of millions of Americans.

When attempting to limit the NSA's data gathering activities towards American citizens, Congress faces a difficult dilemma. Protecting individual constitutional rights and the right to privacy is an urgent need. The public has reacted with outrage to the disclosure of extensive surveillance operations, adding to growing concerns about government overreach. For the sake of civil freedoms and public trust, these issues must be addressed.

On the other hand, national security issues present Congress with a difficult challenge. Identifying and thwarting terrorist operations and cyberthreats are integral to not only the NSA's mission, but also to America's overall national security. Congress must consider both of these perspectives and find a solution that prioritizes privacy and security.

Collaboration with U.S. Tech Companies

To carry out its surveillance program, the NSA works closely with tech companies. The NSA collaborates with a variety of companies with reaches around the globe, such as Facebook, Google, Apple, and Microsoft (Taitz, 2023). In the NSA's PRISM program, the organization receives communications directly from these companies. The government identifies a foreign national whose accounts it wishes to monitor, and then orders the tech company to disclose all communications to and from those accounts, including communications with American citizens (Taitz, 2023).

The feud between Apple and the FBI had eduring consequences for the future of tech collaboration with the government.

Tech Crunch

Although tech companies collaborate closely with the NSA and other government agencies, the government's authority is limited when dealing with private companies. Each company has its own terms, conditions, and stance on privacy and data sharing. One well-known example of a tech company disputing government power occurred with Apple in 2016. The Federal Bureau of Investigation (FBI) wanted Apple to grant it access to an iPhone 5C that belonged to Syed Rizwan Farook, the terrorist behind the 2015 San Bernardino shooting that killed 14 people (Clark, 2021). The FBI was unable to get into the phone due to an iOS feature that would erase the phone after a certain number of failed passcode attempts. Apple refused to build a passcode bypass for the FBI, claiming that such a **backdoor** would permanently decrease the security of its phones.

Backdoor *– an undocumented method of gaining access to a computer system*

Although Apple showed defiance towards the government in this case, other tech companies have often been very forthcoming with NSA and federal requests. When considering measures to regulate the NSA's security apparatus, be sure to consider the role that private companies play in enabling —or not enabling— surveillance activities.

Monitoring of Foreign Leaders

As previously mentioned, the Snowden leaks revealed that the NSA monitored the private communications of 35 foreign leaders for an unknown time period leading up to 2013 (Ball, 2013). After the Snowden documents were widely circulated, an investigation by German intelligence produced plausible information that Chancellor Angela Merkel's mobile phone had been targeted by the NSA. Merkel found the evidence so substantial that she called President Barack Obama to demand an explanation, according to The Guardian (Traynor et al., 2013).

President Obama and German Chancellor Angela Merkel during a visit to the White House

BBC

Such actions created deep rifts of distrust between the United States and the foreign leaders whose communications were allegedly bugged. Although surveilling adversarial foreign leaders is commonplace in the international community, surveilling the leaders of allied nations is likely to cause mistrust and complicate relations.

As the Senate Committee on Intelligence, you will have access to classified briefings and reports from the Executive Branch, which may include requests to surveil on foreign leaders, both allies and adversaries. You must consider the consequences on United States national security of such an action and decide whether to pursue a hawkish surveillance stance or forgo surveillance for the sake of diplomacy.

Congressional Action

nondisclosure order *– a court order prohibiting public entities from disclosing certain records.*

Congress' most substantive action regarding oversight of the NSA came in 2015 with the passage of HR 2048, the USA FREEDOM Act of 2015. The act sought to comprehensively reform the provisions detailed in the USA PATRIOT Act of 2001. The legislation prohibits bulk collection of all records under Section 215 of the PATRIOT Act ("USA Freedom Act", 2015). It prohibits large scale, indiscriminate collection, such as all records from an entire state, city, or zip code ("USA Freedom Act", 2015). The bill also seeks to increase open access to intelligence information by mandating that all national security **nondisclosure orders** must be based upon either a danger to national security or interference with an investigation ("USA Freedom Act", 2015). Additionally, the bill provides methods to strengthen national security, allowing the NSA to track foreign terrorists when they enter the U.S., and securing limited emergency authorities under Section 215 of the PATRIOT Act.

Pro-Snowden protestors rally outside the U.S. Capitol

RAND

Many members of Congress still believe that the USA FREEDOM Act did not go far enough in curbing the NSA's usage of Section 215, which allows the agency to collect "tangible things" (including books, records, papers, documents, and other items) for foreign intelligence information (Mann, 2014). In 2020, U.S. Senator Ron Wyden (D-OR) introduced The Safeguarding Americans' Private Records Act,

The federal courthouse in Washington, D.C. where the FISA Court meets

NPR

which would permanently end the phone surveillance program, prohibit warrantless collection of geolocation information by intelligence agencies (U.S. Senator Ron Wyden of Oregon, 2020). The bill was introduced, but no further progress has occurred.

Other Policy Action

Even though Congress has produced only two substantial pieces of legislation governing the NSA, they have been more effective on this issue than the Executive or Judicial Branch.

Most of the NSA's internal operations are authorized within Executive Order 12333, which was signed by President Ronald Reagan in 1981. It is the foundational authority by which the NSA collects, retains, analyzes, and disseminates foreign signals intelligence information. The principal application of this authority is the collection of communications by foreign persons that occur wholly outside the United States. (*EO 12333,* 1981).

The judicial branch is connected to the NSA via the aforementioned FISA Court system. These courts authorize the NSA to surveil potential national security threats on a target-by-target basis. Due to the lack of concrete action by the executive and judicial branches on the subject, this committee of Congress has an incredible opportunity to take the lead on NSA oversight.

Hawkish *– people who are hawkish believe in aggressive action to pursue national security goals.*

Dovish *– people who are dovish are more skeptical of aggressive actions for national security goals.*

IDEOLOGICAL VIEWPOINTS

Conservative View

Conservatives, on any issue, are usually more **hawkish** than their liberal counterparts and place more weight on national security and a strong national defense. This remains true with the NSA. Conservatives believe that the NSA's national security mission is very important. They are more accepting of certain practices if they know that those practices help to fight terrorism and the nation's adversaries. However, conservatives also strongly value liberty; 56% of them disapprove of NSA spying in general (*Republican Views, 2018).* Both parties agree that spying on Americans can be bad, but conservatives may be more accepting of it for national security purposes.

House Speaker Kevin McCarthy delivers a press conference

Georgia Recorder

Liberal View

Liberals are much more **dovish** on national security issues than their conservative counterparts. Liberals believe in minimizing NSA surveillance of American citizens. Many liberals are concerned with the unequal treatment of Muslim and Arab Americans under the PATRIOT Act, which they say is an example of the NSA misusing its authority for problematic ends. Some even go far enough to believe

that the NSA should not involve itself in world affairs at all, as it is just another arm of the American imperialist military complex. In short, liberals believe that the NSA is in need of drastic reforms.

AREAS OF DEBATE

This section will propose and break down multiple solutions to the problems addressed so far in this briefing. It will also provide the partisan perspectives on each solution. Although this section will be comprehensive, do not feel limited by the solutions listed here. The American people need you to be as creative as possible when solving these issues, so do not hesitate to propose novel or unorthodox ideas at the conference.

President Ronald Reagan, who signed the Executive Order which defined NSA and intelligence mechanisms

NBC

Banning Warrantless Mass Collection

The most frequently proposed solution in the realm of NSA oversight is to entirely ban the mass collection of communications data without an explicit warrant from a FISA or similar court. This solution could be implemented by reforming Section 215 of the PATRIOT Act, which included a clause that mass collection of data was allowed if the either the collected data or target person was suspected of discussing matters "relevant" to national security. The benchmark for what is considered "relevant" in this case was left vague by the Act itself. Many supporters of this ban believe that the NSA used the ambiguity in the PATRIOT Act to justify targeting anyone that they desired. This solution would remove this vague language and establish that a warrant must determine national security relevance.

NSA Director Paul Nakasone. He maintains that no domestic surveillance monitors are needed for the NSA.

The Washington Post

Political Perspectives on this Solution

Since this solution would make it more difficult for the NSA to continue standard operations, most conservatives would oppose this solution. Conservatives would likely argue that the luxury of receiving a warrant should only be extended to American citizens, not foreign nationals. They would argue that such a move would jeopardize national security by introducing yet another layer of government bureaucracy, hindering America's intelligence capabilities. However, some libertarian conservatives may, in fact, support this policy, since they are in favor of putting more checks on the government's power and protecting individuals from surveillance. They would believe that upholding privacy is of the utmost importance, despite any possible national security risks.

Most liberals would likely support this policy. As previously mentioned, liberals are often laxer on military and national security issues. They stand for the human rights and dignity of all people, regardless of nationality. Liberals, especially those farther to the left,

will see this as a necessary check on the power of the intelligence and military complex. Some hawkish liberals, however, may oppose this policy for the same reasons as mainstream conservatives.

Some outside interest groups might also have heavy opposition to this policy. Both intelligence and law enforcement agencies would oppose this policy. The ramifications of adding a warrant requirement to the NSA would eventually affect them as well. Also, tech companies may show opposition because such a policy may require them to reveal sensitive data to the FISA Court, which they may not be inclined to do for privacy reasons.

Mark Zuckerberg testifies before the Senate on privacy concerns
The Washington Post

Opt-In for Data Collection

This solution would seek to provide consumers with more control over their privacy. Specifically, it would require tech companies to ask their consumers to explicitly opt-in to the possibility of their data being collected and stored by the company. In order to keep the NSA's stated mission intact, this requirement would only extend to American consumers. In terms of enforcement, each tech company may be given a blanket deadline to comply with the policy or risk losing federal funding and grants.

One major benefit of this policy would be providing citizens with much more autonomy over their data. It could inspire citizens who are unfamiliar with the NSA's practices to do research on how their data could be collected and used by government agencies. It would also clear tech companies of any liability, since all consumers have previously agreed to all necessary data collection.

The growth of social media websites has brought privacy concerns to the forefront.
Security Magazine

There are, however, many consequences to this proposal. Even if it were to pass, tech companies may require customers to either opt in or not use their services at all, defeating the purpose of the legislation. Many companies already do this. Apple, for example, includes data collection provisions in the terms and conditions that it forces users to agree to before they use their products. Also, enforcing this requirement is difficult due to the sheer number of intermediary companies with deal with consumer data. Such a policy may have to extend to phone companies, internet service providers, social media networks, and all of the companies which may handle data in between.

Political Perspectives on this Solution

Determining the supporters or opponents of this policy is complicated. While the federal government has yet to adopt comprehensive legislation on data privacy, many states have. The states that have adopted wide data privacy legislation range drastically along the political spectrum, from California and Massachusetts to Tennessee and Utah. Thus, determining a Senator's support for this legislation would come down to their

previous stances on tech issues, as well as an analysis of the lobbyists who are connected with them.

Affirming Whistleblower Protection

It is important to remember that the reason the NSA is even being discussed today is because of the actions of a whistleblower. Regardless of one's views on whether Edward Snowden was justified in his actions, he is directly responsible for increased awareness and pushes for intelligence reform. However, Edward Snowden was immediately criminalized for his leaking of classified information, forcing him to find refuge in international embassies and eventually in Russia (Wiebe 2013).

Edward Snowden's Russian citizenship card
The New Yorker

In order to ensure that standards for government conduct are being upheld, people must be able to report perceived violations. Thus, some believe that whistleblowers must be allowed to publicly report violations of ethics standards going on within the United States Government. This solution would provide a route to decriminalization for whistleblowers who reveal government secrets, if the secrets are reported in order to expose misdeeds.

One advantage of this solution would be that the American people would instantly know whenever ethical violations are occurring within the government. This will force agencies to remain fully compliant with ethics standards, even behind closed doors. A possible downside to this plan would be that it would put classified information at risk. In this plan, information is leaked and then a court would determine if there were ethics violations, meaning that it is completely up to the leaker to be sure that there are violations before leaking the information.

Political Perspectives on this Solution

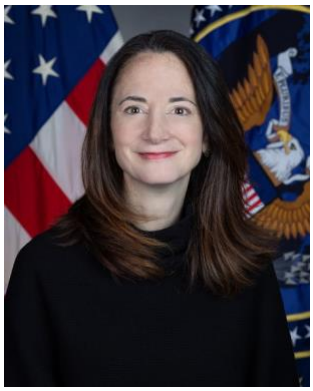
Liberals would be much more supportive of this plan than conservatives. Liberals often place adherence to ethical standards and fairness over security, while conservatives are the opposite. No matter what side of the political spectrum they lie on, opponents of this solution would point to the risk of classified information being leaked as a dealbreaker.

Regular NSA Audits

Supporters of this solution believe that for the NSA to be held accountable, transparent, and in accordance with legal and constitutional requirements, frequent audits must be implemented. These audits offer an unbiased evaluation of the NSA's data collecting procedures, assisting in the discovery of any potential abuses or invasions of privacy. Audits function as a crucial oversight mechanism by analyzing the agency's operations, data retention policies, and adherence to specified rules.

These audits would be conducted by an impartial organization; this could be either the Senate Intelligence committee itself, or professionals in privacy, civil liberties, and intelligence supervision. This committee would have the power to thoroughly examine the NSA's activities, policies, and adherence to the law. The audits should include a thorough analysis of the methods used for gathering data, the targeting standards, and how the data was handled. Additionally, they ought to assess the success of privacy protections and their overall effect on civil liberties.

Of course, one challenge in implementing regular audits is the allocation of sufficient resources, expertise, and time required to conduct thorough evaluations. Logistical difficulties and potential audit process delays would arise from establishing an impartial organization, since the public would want them to be as thorough as possible. There also may be concern regarding possible security vulnerabilities connected to audits. Confidential operational information could unintentionally give away key intelligence sources, techniques, or capabilities.



Avril Haines, the current Director of National Intelligence

Office of the DNI

Political Perspectives on this Solution

Political perspectives on this solution would be similarly mixed. Some conservatives may see regular audits as an opportunity to demonstrate that the NSA is free of violations. However, many may still be wary of the concern that audits could impede the agency's ability to swiftly respond to emerging threats. Liberals, by and large, would likely strongly support this solution.

BUDGETARY CONSIDERATIONS

The budget that goes to the NSA directly is classified. However, the budget for the entire National Intelligence Program, which includes the CIA and other intelligence agencies, totals $65.7 billion for FY 2022 (*U.S. Intelligence Budget Data, 2022*). This means that the Senate Intelligence Committee has a healthy budget with which to accomplish its initiatives.

CONCLUSION

As you can see from the information presented in this briefing, the intelligence community stands at a crossroads. The mistakes and misdeeds of its past have been exposed for all to see. The National Security Agency has been used more as an extrajudicial spying agency than one designed to keep the American people safe. It is up to the Senate Select Committee on Intelligence to find a way to effectively oversee and reform this agency. This is imperative not just

for our national security, but also to maintain our place as the nation with the most developed intelligence apparatus in the world. The American people are counting on you.

From now until the Senate convenes at the Conference, the chairs encourage you to find your own solutions to the issues laid out in this briefing. The conference is a forum of lively debate only thanks to the prior research and knowledge of its delegates. The chairs eagerly look forward to hearing your thoughts, discussions, and input this February.

GUIDE TO FURTHER RESEARCH

To gain further knowledge on this subject, the chairs recommend reading all of the mentioned legislation and news articles in the glossary in depth. These will provide you with the solutions that have already been proposed, as well as varying viewpoints in the realm of intelligence oversight. Useful sources include the likes of Congress.gov and ProPublica.

GLOSSARY

Bug – to conceal a miniature microphone in (a room or device) in order to monitor or record someone's conversations.

Backdoor – an undocumented method of gaining access to a computer system.

Dovish – people who are dovish are more skeptical of aggressive actions for national security goals.

FISA Court — A special federal court which approves requests from the NSA to surveil American citizens.

Hawkish – people who are hawkish believe in aggressive action to pursue national security goals.

Nondisclosure order – a court order prohibiting public entities from disclosing certain records.

BIBLIOGRAPHY

Ball, James. "NSA Monitored Calls of 35 World Leaders after US Official Handed over Contacts." *The Guardian*, 25 Oct. 2013. *The Guardian*,

https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.

Bipartisan, Bicameral Coalition Roll Out New Bill To Reform NSA Surveillance and Protect Americans' Rights | U.S. Senator Ron Wyden of Oregon. https://www.wyden.senate.gov/news/press-releases/bipartisan-bicameral-coalition-roll-out-new-bill-to-reform-nsa-surveillance-and-protect-americans-rights. Accessed 12 June 2023.

Clark, Mitchell. "Here's How the FBI Managed to Get into the San Bernardino Shooter's IPhone." *The Verge*, 14 Apr. 2021, https://www.theverge.com/2021/4/14/22383957/fbi-san-bernadino-iphone-hack-shooting-investigation.

Heiligenstein, Michael X. "A Brief History of the NSA: From 1917 to 2014." *The Saturday Evening Post*, 17 Apr. 2014, https://www.saturdayeveningpost.com/2014/04/a-brief-history-of-the-nsa/.

Mann, Scott F. *Fact Sheet: Section 215 of the USA PATRIOT Act*. Feb. 2014. *www.csis.org*, https://www.csis.org/analysis/fact-sheet-section-215-usa-patriot-act.

National Security Agency/Central Security Service > Signals Intelligence > EO 12333. https://www.nsa.gov/Signals-Intelligence/EO-12333/. Accessed 12 June 2023.

Rep. Sensenbrenner, F. James. *H.R.3162 - 107th Congress (2001-2002): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*. 26 Oct. 2001, http://www.congress.gov/bill/107th-congress/house-bill/3162. 2001-10-23.

---. *Text - H.R.2048 - 114th Congress (2015-2016): USA FREEDOM Act of 2015*. 2 June 2015, http://www.congress.gov/bill/114th-congress/house-bill/2048/text/pl. 2015-04-28.

Republican Views On Domestic Surveillance | Republican Views. 31 Dec. 2018, https://www.republicanviews.org/republican-views-on-domestic-surveillance/.

Savage, Charlie. "N.S.A. Triples Collection of Data From U.S. Phone Companies." *The New York Times*, 4 May 2018. *NYTimes.com*, https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html.

"Surveillance Under the USA/PATRIOT Act." *American Civil Liberties Union*, https://www.aclu.org/other/surveillance-under-usapatriot-act. Accessed 6 June 2023.

Szoldra, Paul. "This Is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks." *Business Insider*, https://www.businessinsider.com/snowden-leaks-timeline-2016-9. Accessed 6 June 2023.

Taitz, Sarah. "Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress | ACLU." *American Civil Liberties Union*, 11 Apr. 2023, https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress.

Traynor, Ian, et al. "Angela Merkel's Call to Obama: Are You Bugging My Mobile Phone?" *The Guardian*, 24 Oct. 2013. *The Guardian*, https://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german.

U.S. Intelligence Budget Data. https://irp.fas.org/budget/. Accessed 18 June 2023.

"USA Freedom Act." *House Judiciary Committee Republicans*, 22 Apr. 2015, http://judiciary.house.gov/usa-freedom-act.

