PUBLIC FORUM DEBATE
January 2021

John F. Schunk, Editor

“Resolved: The NSA should end its surveillance of U.S. citizens and lawful permanent residents.”

PRO
P01. 4th AMENDMENT PROTECTS AMERICANS’ PRIVACY
P02. INVASIONS OF PRIVACY ARE DEEPLY HARMFUL
P03. NSA SURVEILLANCE IS EXTENSIVE
P04. SECTION 215 SURVEILLANCE VIOLATES PRIVACY
P05. PRISM PROGRAM TARGETS MILLIONS OF AMERICANS
P06. SECTION 702 VIOLATES PRIVACY
P07. FISC (FISA COURT) REGULATION IS DOOMED TO FAILURE
P08. WARRANTLESS SURVEILLANCE SHOULD BE BANNED
P09. SURVEILLANCE BAN DOESN’T IMPAIR U.S. SECURITY

CON
C01. 4th AMENDMENT HAS LIMITED APPLICABILITY
C02. RIGHT TO PRIVACY IS VASTLY OVERRATED
C03. NSA SURVEILLANCE TARGETS NON-CITIZENS
C04. SECTION 215 SURVEILLANCE HAS BEEN DISCONTINUED
C05. PRISM PROGRAM SHOULD CONTINUE
C06. SECTION 702 DOES NOT VIOLATE PRIVACY
C07. FOREIGN THREATS NECESSITATE NSA SURVEILLANCE
C08. SECTION 702 PREVENTS TERRORIST ATTACKS
C09. SURVEILLANCE BAN WOULD BE A DISASTER

S-K PUBLICATIONS
PO Box 8173
Wichita KS 67208-0173
PH 316-685-3201
FAX 316-260-4976
debate@squirrelkillers.com
http://www.squirrelkillers.com

SK/P01. 4TH AMENDMENT PROTECTS AMERICANS’ PRIVACY

1. 4TH AMENDMENT PROTECTS AMERICANS FROM SURVEILLANCE

SK/P01.01) Brittany Adams [U. of Washington School of Law], WASHINGTON LAW REVIEW, March 2019, NexisUni, p. 422. The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects" by prohibiting "unreasonable searches and seizures" by the government. In the modern technological era, the Fourth Amendment has evolved from protecting only physical searches to encompassing limitations on electronic surveillance.

SK/P01.02) John F. Schifalacqua [U. of Pennsylvania Law School], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2019, NexisUni, pp. 138-139. Klayman was a successful challenge to the FISA Section 215 metadata program on unreasonableness grounds, but its implications are far reaching. "The Klayman court emphasized that one of the driving purposes behind the Fourth Amendment is to prevent the government from acquiring a significant amount of private information without a judicial determination of probable cause." This concern is equally implicated with Section 702, particularly regarding incidental "about" collection.

2. RIGHT TO PRIVACY IS DERIVED FROM 4TH AMENDMENT

SK/P01.03) Aaron Shubert [Hofstra U. School of Law], HOFSTRA LAW REVIEW, Spring 2020, NexisUni, pp. 835-836. The constitutionally-founded right to privacy has long been argued, even before the turn of the twentieth century. To this day, it remains highly-contested because while our Constitution does not explicitly state a right to privacy, the Supreme Court has repeatedly determined that variations of the right are derived from penumbras of other rights guaranteed in the Constitution.

3. LONG-TERM SURVEILLANCE IS SERIOUS INVASION OF PRIVACY

SK/P01.04) John F. Schifalacqua [U. of Pennsylvania Law School], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2019, NexisUni, p. 140. In United States v. Jones, the concurring opinions contemplate the fact that "it may be that [long-term surveillance] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy." Indeed, the surveillance data collected via the third-party doctrine is so much more intrusive in the information era than the phone records which spawned the creation of the doctrine in Smith v. Maryland. A mosaic of data points can pierce one's private life in intricate detail, even when incidentally collected.

4. FOREIGN COMMUNICATION DOESN’T FORFEIT U.S. PRIVACY RIGHT

SK/P01.05) Elizabeth Goitein [Co-Director, Liberty & National Security Program, NYU School of Law], AMERICAN CRIMINA LAW REVIEW, Winter 2018, NexisUni, p. 116. None of

the recent Section 702 decisions held that an American's expectation of privacy in her communications--as distinct from the government's obligation to obtain a warrant before intruding on that privacy--turns on the nationality or location of the other party to the communication. Indeed, the FISA Court has repeatedly acknowledged that the acquisition of international communications involving Americans raises Fourth Amendment issues. The courts reviewing Section 702 assumed as much when they performed an analysis of whether the surveillance met the Fourth Amendment's test of "reasonableness."

SK/P02. INVASIONS OF PRIVACY ARE DEEPLY HARMFUL

1. INVASIONS OF PRIVACY DESTROY HUMAN DIGNITY

SK/P02.01) Theresa E. Miedema, CROSS CURRENTS, June 2020, p. 159+, Gale Academic OneFile. I argue that privacy is important not because of privacy itself per se, but because privacy exists to protect, foster, and promote basic human dignity. This view of privacy changes how we think of our own individual privacy rights since privacy is about so much more than just my personal information. If privacy is, at its heart, about human dignity, then something is lost at a much more fundamental level when I dismiss my own privacy as irrelevant or unnecessary.

SK/P02.02) Theresa E. Miedema, CROSS CURRENTS, June 2020, p. 159+, Gale Academic OneFile. Warren and Brandeis tie privacy (in their words, "the right to be left alone") to dignitary interests where the injury suffered is a lowering of a person's esteem of others. Violations of privacy injure a person's feelings, and this type of injury is as serious, if not more so, than any kind of physical harm. When Warren and Brandeis talk about "injury to feelings", they refer to something more profound than merely a bruised ego. Indeed, Warren and Brandeis describe an invasion of privacy as a "spiritual injury" and suggest that what privacy protects is the right to "an inviolate personality".

2. INVASIONS OF PRIVACY THWART PURSUIT OF HAPPINESS

SK/P02.03) Patrick M. Garry [Professor of Law, U. of South Dakota], WAYNE LAW REVIEW, Winter 2020, NexisUni, p. 312. Robert Post views privacy in a broad context, as something seeking to safeguard certain civility norms and cultural standards. Privacy may be an important means for a society to achieve the Declaration of Independence's "pursuit of happiness." The individual "time and space to be free with their own thoughts" may be a prerequisite for the happiness that any healthy society would want for its members.

3. INVASIONS OF PRIVACY THREATEN INDIVIDUAL FREEDOM

SK/P02.04) Patrick M. Garry [Professor of Law, U. of South Dakota], WAYNE LAW REVIEW, Winter 2020, NexisUni, p. 313. Finally, privacy is very much tied to the goal of limited

government set out in the U.S. Constitution. While the constitutional principle of limited government operates on the political level (acting as a check on the power and activities of the various branches of government), privacy operates on an individual level, creating a realm in which the individual is free to live outside the encroachment of government. Privacy emanates from the individual, limiting the power of the state and further reinforcing the structural provisions of the Constitution that seek to do the same. In this respect, privacy becomes an essential tool in maintaining limited government. It becomes even more essential when we consider that recently, "the boundaries between the private and public realms have been greatly diminished, both in general and in matters concerning privacy in particular."

4. INVASIONS OF PRIVACY STIFLE DISSENT

SK/P02.05) Patrick M. Garry [Professor of Law, U. of South Dakota], WAYNE LAW REVIEW, Winter 2020, NexisUni, p. 313. Privacy also contributes to limited government insofar as privacy "is essential for political dissent," and hence an important means for individuals to resist the unwanted reach of government. Even more generally than serving the cause of limited government, privacy facilitates democratic action by "creating space for the formation and nurturing of political thought." As Professor Griffin notes, "[If] our deliberation and decisions about how to live were open to public scrutiny, our imperative for self-censorship and self-defense would come feverishly into action." Indeed, "[a]utonomy is a feature of deliberation and decision."

5. INVASIONS OF PRIVACY IMPAIR HEALTHY DEMOCRACY

SK/P02.06) Patrick M. Garry [Professor of Law, U. of South Dakota], WAYNE LAW REVIEW, Winter 2020, NexisUni, pp. 309-310. An array of justifications has been offered for a right of privacy, ranging from individual needs of autonomy, dignity, and self-actualization to privacy as an essential need for social and professional relationships and a healthy and vibrant democratic community.

6. THE “NOTHING TO HIDE” ARGUMENT IS MISGUIDED

SK/P02.07) Theresa E. Miedema, CROSS CURRENTS, June 2020, p. 159+, Gale Academic OneFile. However, as Solove argues, the "nothing to hide" argument, even in its strongest form, misses the point of privacy entirely. The core problem with this argument is that "it myopically views privacy as a form of concealment or secrecy."

SK/P03. NSA SURVEILLANCE IS EXTENSIVE

1. NSA ENGAGES IN EXTENSIVE SURVEILLANCE

SK/P03.01) Thomas A. Bass [Professor of English & Journalism, SUNY-Albany], THE

AMERICAN SCHOLAR, Autumn 2020, p. 22+, Gale Academic OneFile. The Information Surveillance Center along the Ho Chi Minh Trail has been resurrected as the Utah Data Center built along the Mormon Trail in Bluffdale, Utah. This is where the NSA, in a $2 billion facility opened in 2019, is gathering the data used by "people sniffers" to monitor everything from computer keystrokes to eyeball iris scans. A program called MYSTIC records and archives phone calls around the world. PRISM collects Internet communications. STINGRAY tracks text messages.

SK/P03.02) Thomas A. Bass [Professor of English & Journalism, SUNY-Albany], THE AMERICAN SCHOLAR, Autumn 2020, p. 22+, Gale Academic OneFile. As its computers scroll through yottabytes of data, the NSA is trying to interdict enemy forces moving along the world's electronic trails. "The U.S. government," Snowden warned, "in conspiracy with client states, chiefest among them [co-members of the Five Eyes alliance]-the United Kingdom, Canada, Australia, and New Zealand-have inflicted upon the world a system of secret, pervasive surveillance from which there is no refuge."

SK/P03.03) THE ECONOMIST, September 19, 2020, p. 78(US), Gale Academic OneFile. That America stands at the top of the list is not surprising. Its cyber-security budget for fiscal year 2020 stood at over $17 billion and the National Security Agency (NSA), its signals-intelligence (SIGINT) agency, probably gets well over $10 billion.

SK/P03.04) Digital Journal, NEWSTEX BLOGS, March 30, 2020, pNA, NexisUni. Back in 2013 Snowden revealed details of secret surveillance programs that were being carried out by the National Security Agencies. After Snowden's revelations were published in both the Washington Post and the Guardian the government declassified some information about the programs and began to publish annual reports about the program but the surveillance carried on. In January of 2018 the legislation authorizing the surveillance over the Internet for national security purposes was extended.

SK/P03.05) Sunil Rajguru, PC QUEST, November 12, 2020, pNA, NexisUni. The 21st century has become the Century of Surveillance and 20 years into it, governments have picked up all the tools of the trade to spy on their citizens effectively. They are joined by big corporations, Big Tech in particular, along with various spying agencies, hackers and other bad state actors.

SK/P03.06) Jacob Knutson [Axios], NEWSTEX BLOGS, September 3, 2020, pNA, NexisUni. The ruling comes as the Trump administration, through Attorney General Bill Barr, has only pushed for more expansive digital surveillance capabilities. Europe's high court recently struck down a data pact between the EU and U.S. over concerns that Europeans' private data can't be protected from American government surveillance.

2. COVID PANDEMIC IS INCREASING SURVEILLANCE

SK/P03.07) Sunil Rajguru, PC QUEST, November 12, 2020, pNA, NexisUni. If 9/11 set the trend and China provided the tools, then what was left was the opportunity for the world to do so. That came with the Covid-19 crisis. A widespread alarmist global pandemic in the age of surveillance tech meant that governments could monitor the health and movements of all their citizens without protest.

SK/P03.08) Digital Journal, NEWSTEX BLOGS, March 30, 2020, pNA, NexisUni. Snowden made the claim at an interview with the Copenhagen International Documentary Film Festival. The US government is reported to be in talks with tech companies Google and Facebook to use anonymized location day from phones to help them in tracking the spread of COVID-19. Some commentators say this could be a helpful too for health authorities in tracking the spread of the virus but others are concerned about the potential for the data to be shared by the government. Snowden worries that government's could extend the access they have to people's personal information during a crisis but then use it to monitor their actions.

3. NSA DOES NOT OBTAIN 4TH AMENDMENT SEARCH WARRANTS

SK/P03.09) American Civil Liberties Union, STATES NEWS SERVICE, June 3, 2019, pNA, NexisUni. With the help of companies like ATandT and Verizon, the National Security Agency conducts surveillance on U.S. soil by tapping directly into the internet's backbone--the physical infrastructure that carries our emails, photos, personal chats, and web browsing. The agency then copies and searches a vast pool of internet communications flowing into and out of the United States. It does all of this without a warrant, in violation of the Fourth Amendment.

SK/P03.10) Ron Wyden [U.S. Senator], STATES NEWS SERVICE, April 30, 2019, pNA, NexisUni. "Second, the report underscores my concerns that Section 702 surveillance allows significant warrantless spying on Americans' private communications. The report shows a 28 percent increase in warrantless searches of Americans' information, not including searches by the FBI, which the government does not count.”

SK/P04. SECTION 215 SURVEILLANCE VIOLATES PRIVACY

1. SECTION 215 AUTHORIZED BULK PHONE RECORD COLLECTION

SK/P04.01) Adam Brandon [President, FreedomWorks], STATES NEWS SERVICE, December 6, 2019, pNA, NexisUni. Section 215 is the portion of the PATRIOT Act that has been used to justify the mass collection of cell phone metadata, including records on millions of Americans, as revealed by Edward Snowden in 2013. Although the NSA claims to have ceased this particular form of mass surveillance, their continuous difficulty staying within legal and constitutional due process protections highlights the need for further oversight of our government's use of surveillance authorities domestically, not a reauthorization that ignores many deeply-needed reforms.

SK/P04.02) Free Press, STATES NEWS SERVICE, September 9, 2019, pNA, NexisUni. Earlier this year, the Trump administration asked Congress to reauthorize the NSA's authority under Section 215 to gain access to the domestic communications of people across the United States. This would allow the NSA to collect metadata from hundreds of millions of phone calls and text messages.

2. SECTION 215 IS HUGE THREAT TO POLITICAL DISSENT

SK/P04.03) Free Press, STATES NEWS SERVICE, September 9, 2019, pNA, NexisUni. "The deeply problematic Patriot Act granted sweeping spying powers that no administration should have, and they're particularly dangerous in the hands of Trump," said Free Press Action Government Relations Director Sandra Fulton. "This administration's openly hostile policies are harming the most vulnerable communities in America. And over the last two years, we've seen leak after leak of documents showing the FBI targeting Black protesters fighting for racial justice. More recently we've learned that the Bureau is also spying on folks protesting inhumane immigration policies at the border. Unless House and Senate leadership work together to end the CDR and severely limit other Section 215 authorities, this disturbing trend will only worsen under Trump."

SK/P04.04) Free Press, STATES NEWS SERVICE, September 9, 2019, pNA, NexisUni. "Our millions of activists include members of the communities that the United States government has unlawfully surveilled in recent history and that the Trump administration is expressly threatening now," reads the letter, which was organized by Color Of Change, Demand Progress and Free Press Action. "We oppose any legislation that does not end the Call Detail Records (CDR) program and substantially constrain the remainder of surveillance conducted under the Patriot Act and related authorities." The NSA program permits the mapping of relationships among members of marginalized communities and distant associates of targeted individuals, even when intelligence officials don't suspect most individuals in those communities of wrongdoing.

SK/P04.05) American Civil Liberties Union, STATES NEWS SERVICE, February 6, 2019, pNA, NexisUni. Historically, government surveillance has often been used to wrongly target, and surveil communities of color. For example, media disclosures revealed that the government was using FISA to spy on prominent Muslim-American leaders during the administration of President George W. Bush. A recently leaked FBI intelligence assessment suggests the agency is targeting black activists as "extremists," and the Trump administration wants to use "extreme vetting" impacting both immigrants and non-immigrants alike.

3. NSA ADMITTED RECORDS WERE IMPROPERLY COLLECTED

SK/P04.06) American Civil Liberties Union, STATES NEWS SERVICE, June 26, 2019, pNA, NexisUni. The National Security Agency improperly collected Americans' call records in

October 2018, just four months after the agency publicly asserted it had fixed "root problems" that caused earlier failures to comply with the law, according to new government documents the American Civil Liberties Union released today. The documents also shed new light on the previous compliance violation that led to the NSA's decision in May 2018 to begin purging over 600 million phone records, including that the agency relied on improperly collected information to seek approval for spying on one or more individuals.

SK/P04.07) American Civil Liberties Union, STATES NEWS SERVICE, June 26, 2019, pNA, NexisUni. "These documents further confirm that this surveillance program is beyond redemption and a privacy and civil liberties disaster," said Patrick Toomey, staff attorney with the ACLU's National Security Project. "The NSA's collection of Americans' call records is too sweeping, the compliance problems too many, and evidence of the program's value all but nonexistent. There is no justification for leaving this surveillance power in the NSA's hands."

4. CLAIMS THAT BULK COLLECTION HAS CEASED ARE SPURIOUS

SK/P04.08) American Civil Liberties Union, STATES NEWS SERVICE, February 6, 2019, pNA, NexisUni. In 2015, Congress passed the USA Freedom Act to reform parts of the Patriot Act and make other much-needed changes to the government's surveillance activities. Perhaps most notably, the law prohibited the bulk collection of Americans' call records, internet metadata, and other private information under several statutes. It also sought to enhance transparency, so that illegal surveillance programs under these authorities would never again flourish in secrecy. Four years later, however, serious questions remain about whether these reforms have successfully halted bulk collection and other forms of overbroad surveillance.

SK/P05. PRISM PROGRAM TARGETS MILLIONS OF AMERICANS

1. SECTION 702 AUTHORIZES PRISM PROGRAM

SK/P05.01) POSTMEDIA BREAKING NEWS, December 19, 2019, pNA, NexisUni. The NSA surveillance program is sometimes called PRISM, which gathers data from tech and telecom companies under court supervision and under the authority of section 702 of the Foreign Intelligence Surveillance Act (FISA) but without individual warrants.

SK/P05.02) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, pp. 490-491. The next relevant development in surveillance policy occurred in 2008 when the FISA Act was amended to include Section 702, which granted the government (the Attorney General ("AG") and Director of National Intelligence ("DNI") in particular) surveillance authority, and permitted the collection of foreign intelligence for foreign citizens who are "reasonably believed to be located" outside of the United States. This surveillance is allowed to be conducted from inside the United States. Section 702 also gives intelligence agencies wide authority to collect foreign intelligence by sweeping United States

citizens' communications in a type of collection known as "upstream" or "PRISM" surveillance.

SK/P05.03) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, pp. 500-501. The second way data is collected through Section 702 of FISA is through PRISM, a program run by the NSA. PRISM's existence was acknowledged by the Obama Administration through DNI James Clapper in 2013. A primary function of PRISM is to allow the NSA to access "the private communications of users of nine popular Internet services providers." The service providers then provide the government with all of the communications of a targeted individual. Certain service providers even gave the NSA real-time alerts when a target logged in or sent an email. Private companies such as Google, Microsoft, and Facebook have been named in information-gathering efforts of PRISM. Despite repeated denials, reports have continuously implicated companies in sharing their information via the PRISM program.

2. PRISM COLLECTS MILLIONS OF INTERNET COMMUNICATIONS

SK/P05.04) Daniel R. Godefroi [New England Law School], NEW ENGLAND LAW REVIEW, 2017, NexisUni, p. 61. The NSA collects around 250 million Internet communications annually under the PRISM program.

SK/P05.05) Tangerine, IANS - ENGLISH, November 1, 2019, pNA, NexisUni. The most popular mass surveillance programme is 'PRISM' -- under which the US National Security Agency (NSA) collects user's personal communications from various US internet companies. 'PRISM' allegedly collects stored Internet communications based on demands made to internet companies. The NSA can use PRISM requests to target communications that were encrypted when they traveled across the internet backbone, to focus on stored data that telecommunication filtering systems discarded earlier, and to get access to data.

SK/P05.06) THAI NEWS SERVICE, September 16, 2020, pNA, NexisUni. Since 2001, US surveillance has been undertaken by the US National Security Agency (NSA) under the US-984XN project of PRISM (Planning Tool for Resource Integration, Synchronization, and Management). As an American site reported, 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.

SK/P05.07) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, p. 501. In order to get data through PRISM, the government uses a selector and sends it to an internet service provider, who then gives the government any communications involving that particular selector. United States citizens are subject to PRISM collection whenever they correspond or communicate with a foreigner who is under surveillance. Examples of the information private companies turn over to the NSA include emails, chats, stored data, and notifications of when a target logs into that service. Furthermore, the NSA receives all the data collected by PRISM in its unminimized form. The NSA's access to

companies' data via PRISM is not unfettered, and it can be shared after a FISA request is made for that data.

SK/P05.08) Sunil Rajguru, PC QUEST, November 12, 2020, pNA, NexisUni. . The Utah Data Center is a separate township owned by the US government with its own power plant. It can store data in the form of exabytes (1 exabyte = 1 million terabytes) for private emails, mobile call records and other data related to citizens and consumers. Snowden revealed the scope of PRISM which could monitor and search the online activities of citizens in real time.

SK/P06. SECTION 702 VIOLATES PRIVACY

1. SECTION 702 ALLOWS COLLECTION OF CITIZENS' COMMUNICATIONS

SK/P06.01) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, p. 501. The NSA's warrantless surveillance program operates under Section 702, and the NSA surveilled 129,080 targets in 2017 through this program. Although primarily used to target non-United States citizens abroad, the program collects any communications of United States citizens who have spoken with the target.

SK/P06.02) POSTMEDIA BREAKING NEWS, December 19, 2019, pNA, NexisUni. The U.S. government may collect information about U.S. citizens without obtaining a warrant if the information is gathered inadvertently while legally carrying out surveillance of non-nationals abroad, a U.S. appeals court ruled on Wednesday. The 2nd U.S. Circuit Court of Appeals in New York ruled in an appeal by Agron Hasbajrami, a U.S. resident arrested in 2011 and who later pleaded guilty to a charge of attempting to provide material support to a terrorist organization. Hasbajrami challenged the charges, questioning whether the U.S. National Security Agency (NSA) had legally obtained information about him without a warrant.

2. MILLIONS OF AMERICANS' RECORDS ARE COLLECTED

SK/P06.03) American Civil Liberties Union, STATES NEWS SERVICE, February 6, 2019, pNA, NexisUni. The reforms passed in 2015 were designed to end the bulk collection programs operated by the National Security Agency and Central Intelligence Agency as well as to prevent the large-scale collection of Americans' private data under the Patriot Act going forward. But information released by the NSA suggests that these reforms may not be working as intended. For example, although civil rights groups like the ACLU urged Congress to end surveillance under Section 215 altogether, Congress instead modified that provision, replacing the mass collection of call records with a new framework permitting the government to query records held by companies using narrowly defined search terms. Yet despite the new restrictions, in 2017 alone, the government received 534 million records of Americans' phone calls based on only 40 surveillance targets. Whether the NSA considers this "bulk" collection or not, the scale is staggering.

3. NSA CAN SEARCH COLLECTED COMMUNICATIONS

SK/P06.04) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, p. 502. Once this data is collected, it is put into a database and can be searched by the NSA using search terms that are associated with United States citizens. In 2017, there were 31,196 of these searches conducted. In addition, some of the information on United States citizens collected through Section 702 has been improperly retained by the NSA "in a manner potentially inconsistent with minimization procedures."

SK/P06.05) Rachel G. Miller [U. of Notre Dame Law School], NOTRE DAME LAW REVIEW, 2020, NexisUni, p. 141. Information that has lawfully been obtained through section 702 surveillance, including information that has been incidentally collected, can later be "queried" or searched by intelligence agencies. When the government conducts queries, they are able to access the contents of 702-acquired information and may be able to use the subsequently obtained information as evidence in unrelated criminal proceedings.

SK/P06.06) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, pp. 497-498. Despite having been asked by Congress and others for the last six years, the IC [intelligence community] refuses to comment on how many United States citizens' communications are collected under Section 702 searches. Although United States citizens cannot be targeted directly under Section 702, members of the IC (namely, the Central Intelligence Agency ("CIA"), FBI, and NSA) can search through the collected Section 702 information of a United States citizen. This method gives the IC a means to bypass typical Fourth Amendment protections usually afforded to United States citizens. The Privacy and Civil Liberties Oversight Board ("PCLOB") report states that the incidental data collection of a possibly large scope of United States citizens pursuant to Section 702 is what makes the program potentially unconstitutional.

4. LAW ENFORCEMENT CAN SEARCH COLLECTED RECORDS

SK/P06.07) Brittany Adams [U. of Washington School of Law], WASHINGTON LAW REVIEW, March 2019, NexisUni, p. 416. Thus, Section 702 data acquisition is now conducted primarily by PRISM, the code name for the NSA's downstream surveillance tool. The NSA receives all communications acquired through PRISM, and the NSA, CIA, FBI, and National Counterterrorism Center (NCTC) each have access to raw PRISM-acquired data. The NSA is the only agency that receives and retains unminimized data acquired through upstream collection. All told, the FBI receives approximately 4.3% of the NSA's total collection.

SK/P06.08) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, p. 498. While numerous successes associated with the proper use of Section 702 exist, many people remain concerned about Section 702's unintended effects on United States citizens. "Back-door" searches are searches conducted by intelligence agencies

to comb through communications of United States citizens that have been collected through Section 702. A backdoor search occurs when an intelligence agency searches Section 702 data using identifiers of United States citizens. These backdoor searches are problematic because law enforcement is able to obtain Section 702 information, sometimes on crimes that are not threats to national security, without violating the Fourth Amendment.

SK/P06.09) Brittany Adams [U. of Washington School of Law], WASHINGTON LAW REVIEW, March 2019, NexisUni, p. 403. Accordingly, privacy advocates are concerned that U.S. person queries evade the Fourth Amendment by allowing the government access to U.S. person communications that would otherwise require a warrant, earning the queries the title "backdoor searches." In part, the concern arises from the FBI's ability to query data for criminal investigations, blurring the line between national security and domestic law enforcement. While the most recent reauthorization imposes a court order requirement on the FBI in certain circumstances, the requirement does not go far enough to fully address privacy concerns.

SK/P06.10) Natasha Babazadeh [U. of Virginia Law School], VIRGINIA JOURNAL OF LAW & TECHNOLOGY, Fall 2018, NexisUni, pp. 5-6. Government intelligence agencies such as the NSA will transfer information, obtained outside of domestic investigative procedures, to law enforcement agencies such as the Drug Enforcement Administration (DEA) to pursue criminal cases against U.S. citizens. The NSA's ability to transfer intelligence was most recently noted to have expanded as the Obama administration left the White House in January 2017. According to a declassified document containing intelligence sharing procedures, the NSA now enables other law enforcement agencies to "search directly through raw repositories of communications intercepted by the NSA...." Furthermore, the document revealed that if an analyst comes across any evidence implicating a U.S. citizen, the analyst can send the evidence to the Justice Department.

5. QUERIES OF COLLECTED DATA CONSTITUTE A SEARCH

SK/P06.11) POSTMEDIA BREAKING NEWS, December 19, 2019, pNA, NexisUni. The "incidental collection" of Americans' communications by NSA electronic dragnet that explicitly targets people abroad and without U.S. ties was permissible under the U.S. Constitution, the court ruled. It also said, however, that examining the content of databases of stored NSA information could violate the Constitution's Fourth Amendment protections against unreasonable searches and seizures. The court said the "vast majority" of evidence prosecutors had used against Hasbajrami was "lawfully collected," but prosecutors did not provide information to the trial court about whether investigators had "queried" NSA databases.

SK/P06.12) POSTMEDIA BREAKING NEWS, December 19, 2019, pNA, NexisUni. "While we disagree with the court's ruling that the NSA can collect Americans' international communications without a warrant ... the court rightly finds that the Fourth Amendment applies when the government searches for that sensitive information in intelligence databases," said American Civil Liberties Union lawyer Patrick Toomey, who filed a brief in the case.

6. WARRANTLESS SEARCHES OF DATA VIOLATE 4TH AMENDMENT

SK/P06.13) Rachel G. Miller [U. of Notre Dame Law School], NOTRE DAME LAW REVIEW, 2020, NexisUni, pp. 152-153. The NSA, FBI, and CIA's minimization procedures permit appropriately-trained personnel with access to section 702-acquired information to conduct queries. Queries are conducted by using an identifier, such as a phone number or email, to search through data that has already been acquired through section 702 collection. However, as alluded to by Judge Hogan, information on U.S. persons' communications obtained through this additional warrantless query can be used to prosecute Americans for crimes unrelated to terrorism. These additional queries, it is argued, are in direct violation of the Fourth Amendment as information pertaining to U.S. persons is obtained without a warrant and may be used to investigate and prosecute Americans for crimes unrelated to terrorism.

SK/P06.14) Rachel G. Miller [U. of Notre Dame Law School], NOTRE DAME LAW REVIEW, 2020, NexisUni, pp. 140-141. However, during the process of collecting information from foreign targets, it is evident that collection of U.S. persons' information--not permitted to be intentionally obtained--may still be collected if a U.S. person is in contact with the intended foreign target. Concerns regarding incidental collection of U.S. persons' communications under section 702 surveillance began to grow. Critics argued that collection of U.S. persons' communications violated the Fourth Amendment because it was a warrantless search.

SK/P06.15) John F. Schifalacqua [U. of Pennsylvania Law School], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2019, NexisUni, pp. 134-135. Second, assuming Section 702 does involve Fourth Amendment searches, there is a strong argument that such searches are unreasonable. Trends in case law involving government searches using technology imply an uneasiness with technology that can acquire large amounts of information on a person. With increased collection ability, courts are becoming concerned that the government can acquire a mosaic of information that penetrates the most private aspects of a person's life. As Section 702 collects more incidental information on U.S. persons, it surely triggers the same concerns that courts are increasingly striking down as unreasonable Fourth Amendment searches.

SK/P06.16) John F. Schifalacqua [U. of Pennsylvania Law School], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2019, NexisUni, p. 136. As to the first, it seems hard to believe that individuals do not have a recognizable expectation of privacy over the content of their communications that are increasingly swept up, and subject to review, by Section 702: “[T]he collection of foreign intelligence surveillance today involves Americans' communications at a volume and sensitivity level Congress never imagined when it enacted FISA. If the government wished to acquire the communications of a non-citizen overseas in 1978, any collection of exchanges involving Americans could plausibly be described as "incidental." Today, with international communication being a daily fact of life for large numbers of Americans, the collection of their calls and e-mails in vast numbers is an inevitable

consequence of surveillance directed at a non-citizen overseas. The volume of information collected on U.S. persons makes it difficult to characterize existing foreign intelligence programs as focused solely on foreigners and thus exempt from ordinary Fourth Amendment constraints".

7. POTENTIAL FOR ABUSE IS STAGGERING

SK/P06.17) John F. Schifalacqua [U. of Pennsylvania Law School], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2019, NexisUni, pp. 98-99. The broadness of Section 702's grant of authority to surveil any foreigner abroad who might possess foreign intelligence information potentially means a large swath of people can be searched, including their communications with U.S. citizens. The American Civil Liberties Union (ACLU) warns that in the process of executing a Section 702 search, the IC collects a "vast trove of data for information specfically about Americans, even though these communications were all collected without a warrant." The concern is that the government can search incidental data at a later time "to prosecute Americans for crimes" unrelated to national security, thereby doing a "backdoor" end-run around the Fourth Amendment. And there is certainly reason to believe abuse might be widespread, at least concerning the invasion of privacy. A 2015 preliminary review found that NSA analysts "running searches on emails and other digital communications vacuumed up from undersea internet cables frequently violated Americans' privacy, albeit unintentionally."

SK/P06.18) John F. Schifalacqua [U. of Pennsylvania Law School], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2019, NexisUni, pp. 99-100. Critics paint an Orwellian picture that "broad, warrantless collection of data under Section 702 creates an understandable fear that private messages may be read or used by the government." This issue is particularly acute when activists and critics of the program feel targeted as they pursue advocacy to challenge government practices under Section 702. Intelligence collection is one thing, but law enforcement later searching data without restriction--data initially collected for intelligence purposes--is quite another.

SK/P06.19) John F. Schifalacqua [U. of Pennsylvania Law School], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2019, NexisUni, p. 99. It is hard to overstate the sheer amount of information the IC [intelligence community] can acquire under Section 702 authority. By collecting data as it runs through infrastructural switches that bring the Internet to the world--so-called "upstream backbone facility" collection--the IC can "continuously scan international internet traffic in bulk, looking for communications associated with tens of thousands of 'targets.'" Such collection only requires a surface-level system of judicial oversight. The Foreign Intelligence Surveillance Court (FISC) need only approve a reasonable set of targeting procedures and minimization standards designed to reduce the potential of surveilling Americans. As such, civil libertarians fear a process ripe for abuse.

SK/P07. FISC (FISA COURT) IS DOOMED TO FAILURE

1. FISC RUBBER STAMPS NSA REQUESTS

SK/P07.01) Masood Farivar, VOICE OF AMERICA NEWS, December 12, 2019, pNA, NexisUni. Critics say the secretive FISA court effectively serves as a government rubber stamp, routinely approving upward of 97% of applications through a "one-sided" process that leaves little room for challenging the government's evidence.

SK/P07.02) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, p. 496. In addition, under Section 702, the FISC does not review individualized applications for surveillance, nor oversee how a particular intelligence agency implements individualized surveillance programs. Section 702 also does not "require the Government to specify the nature and location of each of the particular facilities or places at which electronic surveillance will occur."

2. FISC FAILS TO EXERCISE EFFECTIVE OVERSIGHT

SK/P07.03) Center for Democracy & Technology, STATES NEWS SERVICE, April 28, 2017, pNA, NexisUni. "The ultra-secretive FISA court clearly does not offer sufficient oversight to the NSA's surveillance practices, nor are secret privacy rules enough to stop abuses of this personal data. Such private information deserves the highest standard of protection under the law. This was obviously not the case and Congress must act to align the NSA's practice with our core Fourth Amendment rights," Richardson [Deputy Director of the Freedom, Security, and Technology Project, Center for Democracy & Technology].

SK/P07.04) Andrew C. McCarthy, NATIONAL REVIEW, March 23, 2020. p. 31+, Gale Academic OneFile. The FISC has repeatedly approved collection programs only to have the Justice Department and NSA confess that communications are being collected in violation of the court's instructions--an inevitable outcome.

SK/P07.05) NEWS BITES - PRIVATE COMPANIES, September 22, 2020, pNA, NexisUni. However, US law (the Foreign Intelligence Surveillance Act) allows intelligence agencies such as the National Security Agency ("NSA") to collect large volumes of data "in bulk", without specifically targeting the collection and with little judicial oversight. Indeed, US surveillance programs are based on annual certifications that do not take into account whether or not the subjects being monitored are correctly targeted. In addition, the relevant US laws do not give data subjects any right that can be enforced against the authorities collecting their data.

SK/P07.06) Igor Bobic [The Huffington Post], NEWSTEX BLOGS, December 11, 2019, pNA, NexisUni. Top Republicans are calling for reforms to the Foreign Intelligence Surveillance Court after a Department of Justice inspector general report revealed problems with how the FBI obtained a secret warrant to surveil one of Donald Trump's campaign aides in the early months of the 2016 investigation into Russian election meddling.

SK/P07.07) Igor Bobic [The Huffington Post], NEWSTEX BLOGS, December 11, 2019,

pNA, NexisUni. Other conservatives also questioned the entire FISA application process, suggesting government surveillance may have been improperly authorized on U.S. citizens in other instances as well. How many other FISA applications were handled like this? How many other Americans were improperly spied on? How many Americans had their constitutional right trampled on with no ability to defend themselves? — John Cardillo (@johncardillo) December 11, 2019

SK/P08. WARRANTLESS SURVEILLANCE SHOULD BE BANNED

1. INCIDENTAL COLLECTION MUST BE SUBJECT TO 4TH AMENDMENT

SK/P08.01) Elizabeth Goitein [Co-Director, Liberty & National Security Program, NYU School of Law], AMERICAN CRIMINA LAW REVIEW, Winter 2018, NexisUni, pp. 119-120. If Americans have a reasonable expectation of privacy in their communications with foreigners overseas, then the "incidental overhear" cases would justify dispensing with a warrant only if they established an exception to the warrant requirement. This follows from the basic rule, articulated at the outset of this discussion, that warrantless searches and seizures are per se unreasonable unless an established exception applies.

SK/P08.02) Elizabeth Goitein [Co-Director, Liberty & National Security Program, NYU School of Law], AMERICAN CRIMINA LAW REVIEW, Winter 2018, NexisUni, p. 124. In short, the constitutional crux of Kahn, Donovan, and their progeny is that a warrant to obtain electronic communications is sufficiently particularized if it includes the facilities to be surveilled and the conversations to be seized; and, as long as reasonable procedures are in place to avoid capturing conversations that fall outside the warrant's scope, the accidental interception of a small number of such conversations does not violate the Fourth Amendment. It is not possible to read this line of cases as establishing--directly or indirectly--an exception to the warrant requirement.

SK/P08.03) Elizabeth Goitein [Co-Director, Liberty & National Security Program, NYU School of Law], AMERICAN CRIMINA LAW REVIEW, Winter 2018, NexisUni, p. 125.Once a court determines that a reasonable expectation of privacy exists and will be invaded by the government's action, a warrant is mandatory under Supreme Court jurisprudence unless an established exception applies. None of the "incidental overhear" cases suggested that they were carving out an exception to the warrant requirement; rather, they delineated the extent to which a warrant may encompass unnamed persons and pull in "innocent conversations" without running afoul of the Fourth Amendment.

SK/P08.04) Elizabeth Goitein [Co-Director, Liberty & National Security Program, NYU School of Law], AMERICAN CRIMINA LAW REVIEW, Winter 2018, NexisUni, p. 125. The courts have implicitly recognized that Americans have protected privacy interests in their communications with foreign targets. Yet they have found that the lack of Fourth Amendment

protections for the targets strips Americans of their warrant protections, as well. They have reached this conclusion by misreading the "incidental overhear" cases as indirectly establishing an exception to the warrant requirement, when in fact, the communications at issue in those cases were found to fall within the warrants the government had obtained. Read properly, the "incidental overhear" cases have no application to the warrantless collection of Americans' communications under Section 702.

2. SEARCH OF CITIZENS' COMMUNICATION MUST REQUIRE WARRANT

SK/P08.05) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, p. 506. Senators Wyden and Paul co-sponsored legislation known as the "USA Rights Act," which would have required strong oversight of intelligence agencies from an independent agency. In addition, the "USA Rights Act" would have required intelligence agencies to obtain a search warrant before reading the communications of United States citizens. The "USA Rights Act" died in 2017, having been referred to a subcommittee, where no action was taken on it. The House also voted in 2014 and 2015, with strong bipartisan support, on measures designed to close the backdoor search loophole in Section 702 surveillance. While the law surrounding backdoor searches was not changed in either instance, these legislative attempts confirm the existence of bipartisan support for amending Section 702 and closing loopholes exploited by intelligence agencies.

SK/P08.06) Brittany Adams [U. of Washington School of Law], WASHINGTON LAW REVIEW, March 2019, NexisUni, p. 403. Notwithstanding these advantages, privacy and civil liberty advocates have raised concerns that Section 702 does not adequately protect U.S. persons' privacy. Particularly, privacy advocates have challenged the use of terms identifying U.S. persons to "query," or search, the databases of Section 702 collected information. Querying raises Fourth Amendment concerns over governmental access to U.S. person information incidentally collected during authorized surveillance on non-U.S. persons. Even though U.S. persons cannot be targets of Section 702 surveillance, U.S. persons' communications may be swept up in the process. Because U.S. person information may be incidentally yet lawfully collected in Section 702 surveillance, database queries may yield U.S. person communications. Privacy advocates have recommended imposing probable cause warrant requirements on such queries.

SK/P08.07) Office of Representative Warren Davidson, STATES NEWS SERVICE, May 26, 2020, pNA, NexisUni. The Lofgren-Davidson Amendment prevents intelligence agencies from searching Americans' private search and web browsing histories without first obtaining a warrant. After the announcement, Congressman Davidson made the following statement: "For too long, Americans' most private information has been compromised by vague laws and lax privacy protections. With the vote on the Lofgren-Davidson Amendment to FISA reform this week, we take an important step toward restoring Americans' long-neglected Fourth Amendment rights. Protecting Americans' internet browser searches from warrantless surveillance is a modest, though important first step. With the amendment's adoption, I will be

voting to reauthorize the expired sections of FISA and urge my colleagues to do the same."

SK/P08.08) Office of Representative Warren Davidson, STATES NEWS SERVICE, May 26, 2020, pNA, NexisUni. The [Lofgren-Davidson] amendment which is supported by Reps. Adam Schiff, Chair of the House Permanent Select Committee on Intelligence, and Jerrold Nadler, Chair of the House Judiciary Committee is an outright prohibition: the government will not be able to use Section 215 to collect the websites that a U.S. person visits, the videos that a U.S. person watches, or the search queries that a U.S. person makes. If the government is not sure if you're a U.S. person, but you could be, the government cannot get your internet activity without a Title I FISA warrant.

SK/P08.09) Office of Representative Zoe Lofgren, STATES NEWS SERVICE, January 24, 2020, pNA, NexisUni. "Congress must do its job to uphold the Constitution by reforming Section 215 to ensure it isn't misused to spy on Americans," said Rep. Lofgren. "In public hearings, the Intelligence Community made it clear that it does not believe Fourth Amendment privacy protections for personal or private information that exist for criminal investigations necessarily apply to national security investigations. That position is not only contrary to the Constitution, but also defies Congressional intent. That's why our Safeguarding Americans' Private Records Act prevents the misuse of Section 215 by clarifying that simply calling an investigation an 'intelligence investigation' cannot be used to circumvent Americans' Fourth Amendment protections."

SK/P08.10) Office of Representative Zoe Lofgren, STATES NEWS SERVICE, January 24, 2020, pNA, NexisUni. "We must stop sacrificing the civil liberties our Constitution guarantees in the name of national security. We must stop spying on our own citizens without probable cause, without legal and limited warrants, and without any transparency or accountability" said Rep. Jayapal. "By ending the unconstitutional collection of Americans' international communications and reforming Section 215 of the Patriot Act, this bipartisan bill protects the privacy and civil rights of Americans. The Safeguarding Americans' Private Records Act closes dangerous loopholes and strengthens oversight to prevent government overreach and abuse, and ends the indiscriminate collection of massive amounts of domestic communications--surveillance that disproportionately hurts communities of color. It ensures the Intelligence Community is held to important standards established under the Fourth Amendment and reinforces that we can--and must--protect our national security and our civil liberties at the same time."

SK/P09. SURVEILLANCE BAN DOESN’T IMPAIR U.S. SECURITY

1. NSA SURVEILLANCE HASN’T THWARTED ANY TERRORIST ATTACKS

SK/P09.01) Office of U.S. Representative Justin Amash, STATES NEWS SERVICE, March 28, 2019, pNA, NexisUni. "The NSA's sprawling phone records dragnet was born in secrecy, defended with lies and never stopped a single terrorist attack. Even after Congress

acted in 2015, the program collected over half a billion phone records in a single year. It's time, finally, to put a stake in the heart of this unnecessary government surveillance program and start to restore some of Americans' liberties," Wyden [U.S. Senator] said. "

SK/P09.02) Dustin Volz, NATIONALJOURNAL.COM, January 30, 2015, pNA, GALE CENGAGE LEARNING, Expanded Academic ASAP. The bipartisan Privacy and Civil Liberties Oversight Board issued a progress report Thursday charting the administration's efforts to comply with recommendations it made exactly a year ago to overhaul the NSA's surveillance apparatus. That stern review last January also deemed the bulk collection of U.S. call data illegal and ineffective at countering terrorist plots-- conclusions that prompted the board to urge its dissolution.

SK/P09.03) Sara Sorcher, THE CHRISTIAN SCIENCE MONITOR, January 16, 2015, pNA, LexisNexis Academic. After the Snowden leaks, a review board appointed by Obama found this kind of mass collection was not essential to identifying terrorist activity or suspects any more than conventional court orders, and another report from the Privacy and Civil Liberties Oversight Board last year found bulk collection was unlikely to provide significant value in safeguarding the nation in the future.

2. ANONYMITY THREAT TO U.S. SECURITY IS EXAGGERATED

SK/P09.04) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, pp. 76-77. However, there is reason to doubt that anonymity technologies will become widespread to the point where they may cause significant problems for the NSA. Anonymity tools like Tor are not simple to use and will always be rather slow because users' traffic must bounce through volunteers' proxy computers in different parts of the world.

3. THREAT OF FOREIGN ELECTION INTERFERENCE IS EXAGGERATED

SK/P09.05) Fred Guterl, NEWSWEEK, February 7, 2020, pNA, Gale Academic OneFile. Although the U.S. election system is fragmented, Iran could try to compromise voting infrastructure in key districts, spreading fear, uncertainty and doubt. Undermining Americans' faith in the legitimacy of the election could be even more destabilizing than tampering with the actual vote results. Experts say that such a tactic would be out of character for Iran, which in the past hasn't shown much interest in the U.S. political election system.

SK/P09.06) Fred Guterl, NEWSWEEK, February 7, 2020, pNA, Gale Academic OneFile. It's unlikely that Iran has the capacity for waging a cyber war that results in significant loss of life, experts say. For instance, although it could use malware to damage power plants, it would not likely be able to cause damage on enough of a scale to create a prolonged outage of the U.S. electrical grid. "A real cyber war would destroy critical infrastructure, killing potentially millions of people," says Scott Borg, director of the U.S. Cyber Consequences Unit, a non-profit

research group specializing in cyber security. "If we're totally talking about real cyber war, Iran has no capability."

SK/C01. 4TH AMENDMENT HAS LIMITED APPLICABILITY

1. 4TH AMENDMENT ONLY APPLIES TO SEARCH AND SEIZURE

SK/C01.01) David Gray [SMU Law School], SMU LAW REVIEW, Fall 2019, NexisUni, p. 629. The Fourth Amendment guarantees that “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” The threshold question in any Fourth Amendment case is whether government conduct constitutes a "search." If government conduct is a "search," then it falls within the regulatory purview of the Fourth Amendment. If not, then government agents may act at their discretion, free from Fourth Amendment restraints.

2. EXPECTATION OF PRIVACY IS CRITICAL TO DEFINING A SEARCH

SK/C01.02) Derek M. Alphran [Associate Professor, U. of District of Columbia David A. Clarke School of Law], RICHMOND PUBLIC INTEREST LAW REVIEW, Fall 2019, NexisUni, p. 100. The privacy concept also determined what constituted a search subject to the commands of the Fourth Amendment's warrant clause and its prohibition against unreasonable searches. If government action does not invade some justifiable expectation of privacy that society regards as reasonable, then it is not deemed a search under the Fourth Amendment's warrant clause or reasonableness clause.

3. 4TH AMENDMENT DOESN’T APPLY IF NO EXPECTATION OF PRIVACY

SK/C01.03) Derek M. Alphran [Associate Professor, U. of District of Columbia David A. Clarke School of Law], RICHMOND PUBLIC INTEREST LAW REVIEW, Fall 2019, NexisUni, p. 89. Although originally interpreted to protect a "zone of property" and individual security, the modern Court has viewed the Fourth Amendment to protect one's reasonable expectation of privacy.

SK/C01.04) Derek M. Alphran [Associate Professor, U. of District of Columbia David A. Clarke School of Law], RICHMOND PUBLIC INTEREST LAW REVIEW, Fall 2019, NexisUni, p. 100. Justice Harlan's two-part test requires, "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" The reasonable expectation of privacy formulation has been the "loadstar" for determining how and when the Fourth Amendment should be applied.

4. SHARING OF INFORMATION FORFEITS EXPECTATION OF PRIVACY

SK/C01.05) David Gray [SMU Law School], SMU LAW REVIEW, Fall 2019, NexisUni, p. 633. For example, the Court has held that we have no reasonable expectation of privacy in information voluntarily shared with third parties, at least where government agents access that information through those third parties. In elaborating this "third-party doctrine," the Court has held that there is no search for purposes of the Fourth Amendment when government agents look through telephone calling records, look through banking records, or try to find information by recruiting a confidential informant or undercover officer to infiltrate a group and surreptitiously record conversations by wearing a wire.

SK/C02. RIGHT TO PRIVACY IS VASTLY OVERRATED

1. THERE IS NO RIGHT TO PRIVACY IN THE U.S. CONSTITUTION

SK/C02.01) Aaron Shubert [Hofstra U. School of Law], HOFSTRA LAW REVIEW, Spring 2020, NexisUni, p. 835. While numerous decisions have been made stating implicit findings of a right to privacy within the Constitution, one would have a difficult time finding this exact terminology.

SK/C02.02) J. Lyn Entrikin [Professor of Law, U. of Arkansas, Little Rock], UNIVERSITY OF MIAMI LAW REVIEW, Spring 2020, NexisUni, p. 851. Justice Scalia concurred, joined by Justice Thomas, but they threw cold water (figuratively speaking) on the very notion that the Constitution protects informational privacy. They declared bluntly that a "federal constitutional right to 'informational privacy' does not exist."

2. EXPERTS CANNOT EVEN DEFINE WHAT PRIVACY MEANS

SK/C02.03) Patrick M. Garry [Professor of Law, U. of South Dakota], WAYNE LAW REVIEW, Winter 2020, NexisUni, p. 310. Privacy can be a subjective and ambiguous philosophical notion, with few universal rules or norms. As Judith Jarvis Thomson once noted, "[p]erhaps the most striking thing about the right to privacy is that nobody seems to have any clear idea what it is."

SK/C02.04) Susan Hazeldean [Associate Professor of Law, Brooklyn Law School], CORNELL LAW REVIEW, November 2019, NexisUni, p. 1746. Much has been written about the contradictory justifications for protecting privacy and the difficulty of even agreeing upon a definition of privacy itself. The reality is that scholars disagree passionately about how to conceptualize our legal right to privacy. As philosopher Judith Jarvis Thomson put it, "perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is." Daniel Solove argues that privacy cannot be distilled to a single unitary conception. Rather, "privacy is too complicated a concept to be boiled down to a single

essence. Attempts to find such an essence often end up being too broad and vague, with little usefulness in addressing concrete issues."

SK/C02.05) Theresa E. Miedema, CROSS CURRENTS, June 2020, p. 159+, Gale Academic OneFile. While there is considerable discussion of privacy, there is very little consensus on what privacy means or what it requires. In his review of the literature related to privacy, Lindsay observes that, "...the most notable feature of this [scholarship on privacy] has been an almost complete absence of agreement concerning both the definition of privacy and the values said to be promoted by the legal protection of privacy." For his part, Solove captures the sprawling state of scholarship and the difficulties this breadth engenders as follows: "Privacy seems to be about everything, and therefore it appears to be nothing."

SK/C03. NSA SURVEILLANCE TARGETS NON-CITIZENS

1. NSA IS ONLY PERMITTED TO TARGET NON-CITIZENS

SK/C03.01) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, p. 80. Under Section 702, the NSA may only target non-United States persons that are reasonably believed to be outside the United States.

SK/C03.02) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, p. 61. Under Section 702, NSA analysts identify non-United States persons who are reasonably believed to be located outside the United States as potential targets for gathering foreign intelligence regarding a purpose that the FISC has certified. Analysts apply the NSA's targeting procedures "to make a determination regarding the assessed location and non-U.S. person status of the potential target (the foreignness determination) and whether the target possesses and/or is likely to communicate or receive foreign intelligence information authorized under an approved certification (the foreign intelligence purpose determination)."

SK/C03.03) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, p. 494. Section 702's main purpose is targeting a specific "non-U.S. person, group, or entity reasonably believed to be outside the United States." In addition, the target must "possess[] or ... is likely to communicate or receive, foreign intelligence information ... ." United States citizens abroad cannot be targeted using Section 702.

SK/C03.04) Brittany Adams [U. of Washington School of Law], WASHINGTON LAW REVIEW, March 2019, NexisUni, p. 412. Under Section 702, intelligence agencies "target" persons for intelligence collection by "tasking" specific "selectors." A selector must be a unique communications facility, such as a telephone number or email address associated with a target, and cannot be a keyword or name, such as "bomb" or "al-Baghdadi." The user of a tasked

selector is the Section 702 "target." Targets of collection may not include U.S. persons or "any person known at the time of acquisition to be located in the United States."

SK/C03.05) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, p. 497. The most recent statistics on the number of non-United States citizens currently targeted by Section 702 was 129,080 in 2017. This does not give the number of United States citizens whose data is being collected, as only the non-United States citizens are specifically targeted by Section 702 surveillance.

2. RIGOROUS PROTECTIONS ARE IN PLACE

SK/C03.06) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, p. 62. The NSA has specifically used an Internet Protocol (IP) filter with at least "upstream" collection to limit acquisition "to Internet transactions that originate and/or terminate outside the United States." If there is conflicting information regarding whether the target is located inside the United States or is a United States person, the conflict "must be resolved," and the analysts must determine that the potential target is a "non-U.S. person reasonably believed to be located outside the United States prior to targeting." In making the foreign intelligence purpose determination, NSA analysts must determine "that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory." NSA analysts must document their foreignness determinations and foreign intelligence purpose determinations, and two senior NSA analysts must approve the request before a service provider may be compelled to provide the communications associated with a tasked selector.

3. FISC (FISA COURT) HAS BEEN VERY EFFECTIVE

SK/C03.07) Masood Farivar, VOICE OF AMERICA NEWS, December 12, 2019, pNA, NexisUni. FISA grew out of public outrage over domestic intelligence abuses in the 1970s. Enacted in 1978, the statute limited electronic surveillance of U.S. citizens to national security purposes. A secret 11-member court was created to approve surveillance applications. To obtain a warrant, the FBI and the NSA must prove to the court that the intended target of their surveillance is a "foreign power" or an "agent of a foreign power," and that the surveillance is intended for intelligence-gathering purposes.

SK/C03.08) Masood Farivar, VOICE OF AMERICA NEWS, December 12, 2019, pNA, NexisUni. The FBI and the Justice Department are opposed to reforming the FISA court. Brad Wiegmann, a deputy assistant attorney general, told the Senate Judiciary Committee last month that FISA warrants already receive an "extraordinary" level of scrutiny from the court. "I think the FISA court operates really well," Wiegmann said.

4. DETECTION OF WHERE TARGET IS LOCATED IS VERY DIFFICULT

SK/C03.09) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, p. 71. Anonymity technologies may present difficulties for the NSA in conducting surveillance under Section 702 because the statute only permits the NSA to target non-United States persons that are reasonably believed to be overseas. Anonymity technologies disguise users' true IP addresses, which are critical pieces of information that can be used to identify individual's locations. The NSA may therefore have difficulty in determining whether a potential target is a United States person or non-United States person and whether the potential target is inside the United States or overseas.

5. IN THE EVENT OF ERROR, SURVEILLANCE MUST CEASE

SK/C03.10) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, p. 74. Under Verdugo-Urquidez, the Fourth Amendment does not apply to the searches of foreigners outside the United States. Thus, an individual presumed to be a non-United States person overseas does not have privacy interests protected by the Fourth Amendment. However, the individual does suffer a severe privacy intrusion that is protected under the Fourth Amendment if the individual is actually a United States person or is located inside the United States. The NSA's Section 702 procedures provide important protections that reduce this intrusiveness. If the NSA discovers that this person was actually inside the United States or was actually a United States person after targeting, the NSA must promptly detask the selectors used by the individual, which terminates the acquisition directed at those selectors.

6. THE ODDS OF SURVEILLANCE OF A CITIZEN ARE VERY LOW

SK/C03.11) Brittany Adams [U. of Washington School of Law], WASHINGTON LAW REVIEW, March 2019, NexisUni, pp. 418-419. When a person who is targeted for surveillance communicates by phone or email with another person, the second person's information is said to be "incidentally" collected. In the context of U.S. person information, incidental collection occurs when a foreign target located overseas communicates with a U.S. person. Incidental collection can also occur when two foreign targets located abroad discuss a U.S. person in the contents of their communications (e.g., two targets being surveilled under Section 702 are emailing, and the body of the email contains a passport belonging to a U.S. person). The amount of U.S. person communications acquired incidentally is unknown; however, the IC [intelligence community] targets approximately .004% of the world's internet users for Section 702 surveillance and .001% of the world's population. Therefore, the odds of acquiring any one U.S. person's communications incidentally are incredibly low.

SK/C04. SECTION 215 SURVEILLANCE HAS BEEN DISCONTINUED

1. USA FREEDOM ACT PHASED OUT SECTION 215

SK/C04.01) Masood Farivar, VOICE OF AMERICA NEWS, December 12, 2019, pNA, NexisUni. Well before the latest outcry over the Trump campaign investigation, government surveillance was the subject of controversy, fueled by the Edward Snowden revelations in 2013 that the National Security Agency had undertaken warrantless surveillance to collect data on millions of Americans in the wake of the 9/11 attacks. In 2015, Congress enacted the USA Freedom Act, limiting law enforcement agencies' ability to collect data and establishing certain civil liberties protections.

SK/C04.02) Igor Bobic [The Huffington Post], NEWSTEX BLOGS, December 11, 2019, pNA, NexisUni. Congress passed legislation in 2015 phasing out the NSA's bulk data collection programs (32 Republicans and no Democrats opposed the bill in the Senate).

2. BULK COLLECTION OF PHONE RECORDS HAS CEASED

SK/C04.03) Mihir Zaveri, THE NEW YORK TIMES, December 19, 2019, p. A6, NexisUni. Mr. Snowden has been celebrated as a whistle-blower by advocates for privacy and civil liberties but denounced as a traitor by some national security officials. His disclosure in 2013 prompted a worldwide debate about the reach of modern government-surveillance programs. It also prompted reforms. In 2015, Congress ended the N.S.A.'s collection of logs of Americans' phone records.

SK/C04.04) Ben Lovejoy [9to5Mac], NEWSTEX BLOGS, September 7, 2020, pNA, NexisUni. Wednesday's ruling 'makes plain that the NSA's bulk collection of Americans' phone records violated the Constitution. The decision also recognizes that when the government seeks to prosecute a person, it must give notice of the secret surveillance it used to gather its evidence,' Patrick Toomey, a senior staff attorney with the ACLU National Security Project [said]. The NSA was reported to have abandoned the program in 2018, informing the White House that it no longer made sense.

SK/C04.05) Adam Brandon [President, FreedomWorks], STATES NEWS SERVICE, December 6, 2019, pNA, NexisUni. The NSA began deleting these CDRs [call detail records] in 2018 because there were "irregularities" that "resulted in the production to NSA of some CDRs that NSA was not authorized to receive." The collection of phone records continued after these records were deleted. Documents released in June 2019 in response to a Freedom of Information Act (FOIA) request by the American Civil Liberties Union revealed that this continued collection, too, had violated the due process rights of thousands of innocent Americans. The NSA has since confirmed that the CDR program has ceased operation, and NSA representative Susan Morgan has recently testified that even the infrastructure to run the program has been dismantled.

SK/C05. PRISM PROGRAM SHOULD CONTINUE

1. COURTS FIND THAT PRISM DOES NOT UNDULY INVADE PRIVACY

SK/C05.01) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, p. 505. In United States v. Hasbajrami the United States District Court for the Eastern District of New York held that PRISM collection in the case was reasonable. The IC [intelligence community] gathered information that Hasbajrami had numerous communications with an individual thought to be connected with terrorist groups. These communications eventually led to Hasbajrami sending money to the individual affiliated with a terrorist group with the aim of supporting Islamic operations. In addition, Hasbajrami attempted to travel and join up with a jihadi group in Pakistan. He was arrested at John F. Kennedy International Airport in New York City as he attempted to board a flight to Turkey.

SK/C05.02) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, pp. 505-506. The interests that needed to be balanced in this case [U.S. v. Hasbajrami] were the personal privacy interests of United States citizens against the interests of the United States government in collecting "foreign intelligence information" for the purposes of protecting national security. In addition, the court held that combating terrorism and protecting national security is a "compelling government interest." Another part of the holding shows that the judge accounted for Section 702 safeguard procedures of targeting and minimization to reach his decision. The court states that these minimization procedures serve as an "additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons."

2. PRISM PROGRAM PROTECTS U.S. NATIONAL SECURITY

SK/C05.03) Daniel R. Godefroi [New England Law School], NEW ENGLAND LAW REVIEW, 2017, NexisUni, p. 61. Unlike metadata collection, "PRISM allows the NSA to collect the content of the communication." It is of the utmost importance for programs like this to be maintained and implemented. As long as these programs are no longer carried out in secrecy, they are necessary tools in keeping our country safe.

SK/C05.04) Daniel R. Godefroi [New England Law School], NEW ENGLAND LAW REVIEW, 2017, NexisUni, p. 67. Americans are not immune from another high-impact attack on home soil. With the likely probability that an attack is imminent, extreme counter-terrorism measures, such as the Section 215 and PRISM programs must be taken. Programs of this nature are necessary for ensuring the safety of American lives against extremist terrorist groups.

SK/C05.05) CNN WIRE, November 2, 2020, pNA, NexisUni. June 18, 2013 - Testifying before the House Intelligence Committee, FBI Deputy Director Sean Joyce details how the PRISM program has helped stop a number of alleged terrorist attacks.

SK/C06. SECTION 702 DOES NOT VIOLATE PRIVACY

1. SECTION 702 HAS MANY SAFEGUARDS TO PROTECT PRIVACY

SK/C06.01) Rachel G. Miller [U. of Notre Dame Law School], NOTRE DAME LAW REVIEW, 2020, NexisUni, p. 141. Importantly, however, section 702 includes many comprehensive safeguards protecting the privacy interests of U.S. persons. Likewise, the Privacy and Civil Liberties Oversight Board ("PCLOB")--a bipartisan oversight agency within the executive branch--found that section 702 is subject to extensive oversight and further concluded there was "no evidence of intentional abuse."

SK/C06.02) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, p. 495. Any data acquired through Section 702 is handled according to minimization procedures, which include enforcing restrictions on the handling of non-publicly available information on United States citizens acquired via Section 702 methods. The minimization procedures of each agency under Section 702 are approved by the United States Attorney General ("AG") and also reviewed by FISC when FISC is certifying agencies to collect intelligence under Section 702. Each agency's certification must be renewed with an annual application, submitted by the Government to FISC. These minimization procedures are meant to ensure the protection of any government-collected information that pertains to United States citizens.

SK/C06.03) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, p. 98. The NSA already employs minimization procedures that dictate how the agency limits the accessibility, retention, and dissemination of "nonpublicly available information concerning unconsenting United States persons" who are not the target of the surveillance. These minimization procedures help protect United States persons' privacy interests and diminish the intrusiveness of incidental or inadvertent collection.

SK/C06.04) Brittany Adams [U. of Washington School of Law], WASHINGTON LAW REVIEW, March 2019, NexisUni, p. 418. Incidentally collected U.S. person information - information obtained when a U.S. person is communicating with a foreign target or when a foreign target's communications contain U.S. person information - may be retained and used subject to minimization. Inadvertently (or accidentally) collected U.S. person information, however, must generally be destroyed.

2. QUERIES OF COLLECTED DATA HAVE STRICT PROTECTIONS

SK/C06.05) Brittany Adams [U. of Washington School of Law], WASHINGTON LAW REVIEW, March 2019, NexisUni, p. 421. NSA analysts may also get approval for a U.S. person identifier query by making a showing to the Office of the General Counsel that the identifier is reasonably likely to yield foreign intelligence information. The NSA conducts significantly fewer content queries using U.S. person identifiers than metadata queries. To ensure compliance, the

NSA conducts periodic spot checks of queries.

SK/C06.06) Brittany Adams [U. of Washington School of Law], WASHINGTON LAW REVIEW, March 2019, NexisUni, p. 420. All queries, involving U.S. persons or otherwise, must be reasonably likely to return foreign intelligence information or evidence of a crime and must be sufficiently tailored. U.S. person queries are subject to additional limitations. The most recent reauthorization of Section 702 requires the AG and DNI to adopt "procedures consistent with the requirements of the fourth amendment" to govern queries. These procedures are subject to review by the FISC, and agencies must keep a record of U.S. person query terms used. These limitations aim to reduce the probability of returning non-pertinent U.S. person information.

3. QUERIES OF COLLECTED DATA ARE NOT 4TH AMENDMENT SEARCHES

SK/C06.07) Rachel G. Miller [U. of Notre Dame Law School], NOTRE DAME LAW REVIEW, 2020, NexisUni, pp. 154-155. Querying databases containing section 702 information does not result in any new acquisition of data; it is instead only an examination or reexamination of previously acquired information. Therefore, queries are not separate searches for Fourth Amendment purposes. In similar database collections, such as DNA databases, courts have held that subsequent analyses of information previously collected do not rise to the level of a search under the Fourth Amendment, and thus can be used in unrelated criminal prosecutions.

SK/C06.08) Brittany Adams [U. of Washington School of Law], WASHINGTON LAW REVIEW, March 2019, NexisUni, p. 404. Additionally, queries do not result in any new intelligence collection but allow access only to communications that have already been collected lawfully under Section 702 surveillance procedures subject to significant internal and external oversight.

SK/C06.09) Brittany Adams [U. of Washington School of Law], WASHINGTON LAW REVIEW, March 2019, NexisUni, p. 450. However, privacy advocates strongly criticize Section 702, particularly over the use of U.S. person queries. Nevertheless, U.S. person queries are reasonable searches that fall into the foreign intelligence exception to the Fourth Amendment warrant requirement. Their reasonableness is defined by both how the queries are conducted, including minimization, and the narrow scope of U.S. person information revealed by U.S. person queries.

SK/C06.10) Brittany Adams [U. of Washington School of Law], WASHINGTON LAW REVIEW, March 2019, NexisUni, pp. 419-420. Querying is used to access data already in the government's possession more quickly and efficiently; rather than examining single, discrete communications, analysts may query databases to retrieve information readily. In this context, a "query" is a search of Section 702 acquired data using specific terms - such as keywords or phrases, names, email addresses, or phone numbers - to access previously collected information. Such terms may be identifiers associated with U.S. persons. Agencies may use U.S. person identifiers "as the first step in evaluating and detecting potential threats to the

homeland." For example, the NSA may query a database with the name of a government official traveling abroad to identify threats by foreign adversaries, or the name of a U.S. citizen who is held hostage abroad to pinpoint terrorist communications indicating the location or condition of the hostage.

4. NSA IS COMPLYING WITH PRIVACY PROCEDURES

SK/C06.11) Deborah Samuel Sills [Intelligence Community Fellow, Georgetown U. Law Center], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2017, NexisUni, pp. 4-5. Importantly, comprehensive safeguards are built into the FAA [Foreign Intelligence Surveillance Act (FISA) Amendments Act], particularly into Section 702, that protect the privacy interests of United States persons. Equally significant, the executive branch has established a history of compliance with the statutory requirements of Section 702 that preserve such privacy interests. For example, the Senate Select Committee on Intelligence found, based upon its numerous hearings and briefings since the enactment of Section 702, that Section 702 "has been implemented with attention to protecting the privacy and civil liberties of U.S. persons, and has been the subject of extensive oversight" by all three branches of the government.

SK/C06.12) Deborah Samuel Sills [Intelligence Community Fellow, Georgetown U. Law Center], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2017, NexisUni, pp. 80-81. The misuse of intelligence authorities of the 1960s and 1970s as documented by the Church and Pike Committees has been addressed. The executive branch has an established history of compliance with the statutory requirements of Section 702. Reports by the PCLOB, Attorney General, and Director of National Intelligence consistently show that the executive branch is fulfilling its statutory and procedural obligations. Moreover, in reauthorizing the FAA, including Section 702, the Senate Select Committee on Intelligence found that the statutory provisions have been implemented in a manner that protects the privacy and civil liberties of United States persons and is subject to extensive oversight by all three branches of our government.

SK/C06.13) Center for Democracy & Technology, STATES NEWS SERVICE, April 28, 2017, pNA, NexisUni. As reported in the New York Times, the National Security Agency (NSA) is stopping a controversial part of its warrantless surveillance conducted under Section 702 of the Foreign Intelligence Surveillance Act (FISA), which permits the targeting of non-U.S. persons outside the U.S. It reportedly abandoned the practice of collecting communications that merely mention an identifier associated with a target, such as an email address or telephone number.

5. OVERSIGHT HAS DETECTED NO EVIDENCE OF ABUSE

SK/C06.14) Deborah Samuel Sills [Intelligence Community Fellow, Georgetown U. Law Center], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2017, NexisUni, p. 5. Likewise, the Privacy and Civil Liberties Oversight Board (PCLOB), a bipartisan oversight

agency within the executive branch, found that the implementation of the Section 702 program has been subject to extensive oversight and concluded that there was "no evidence of intentional abuse."

SK/C06.15) Deborah Samuel Sills [Intelligence Community Fellow, Georgetown U. Law Center], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2017, NexisUni, pp. 5-6. Moreover, reports by the Attorney General (AG) and Director of National Intelligence (DNI) indicate that the National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Central Intelligence Agency (CIA) implemented procedures related to Section 702 in a manner that reflects a "focused and concerted effort" by the Intelligence Community to comply with the requirements of Section 702. Reviews have uniformly determined that the executive branch has not intentionally misused any of its authorities under Section 702 or intentionally violated any of the procedural safeguards that protect United States privacy interests.

SK/C06.16) Rachel G. Miller [U. of Notre Dame Law School], NOTRE DAME LAW REVIEW, 2020, NexisUni, pp. 153-154. Additionally, information acquired under a section 702 query may not be introduced as evidence against that person in any criminal proceedings except with the approval of the Attorney General, and in criminal cases with national security implications or certain other serious crimes. The 2017 FAA amendments additionally require the FBI to report on the number of instances in which they opened a criminal investigation of a U.S. person, who is not considered a threat to national security, based wholly or in part on section 702 acquired information. As reported in the DNI Transparency Report, in 2017 and subsequently in 2018, there were zero instances in which the FBI opened a criminal investigation of a U.S. person who was not considered a threat to national security, based wholly or in part on section 702-acquired information.

6. SECTION 702 ACHIEVES A BALANCE BETWEEN PRIVACY & SECURITY

SK/C06.17) Deborah Samuel Sills [Intelligence Community Fellow, Georgetown U. Law Center], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2017, NexisUni, pp. 81-82. Multiple layers of protections currently exist for the querying of Section 702 data and the executive branch has a record of complying with these procedural safeguards. As stated in United States v. Hasbajrami, "in this era there are individuals and groups dedicated to inflicting grave harm on our nation," and the government's intelligence tools "are a critical component of our government's efforts to protect us from harm." Our government "has a duty to respect and protect our constitutional rights while simultaneously ensuring the nation's security."

SK/C06.18) Igor Bobic [The Huffington Post], NEWSTEX BLOGS, December 11, 2019, pNA, NexisUni. Support for the controversial Section 702 of FISA, which deals primarily with non-U.S. citizens but can involve communications of citizens, has historically been bipartisan.

SK/C07. FOREIGN THREATS NECESSITATE NSA SURVEILLANCE

1. U.S. FACES SIGNIFICANT FOREIGN INTELLIGENCE THREATS

a. CHINA IS A THREAT

SK/C07.01) Jamil N. Jaffer [Executive Direcftor, National Security Institute, George Mason U.], NEWSWEEK, October 30, 2020, pNA, Gale Academic OneFile. Standing alone, cyber-enabled economic warfare conducted by China drains the American private sector of billions of dollars a year, with total damages estimated in the trillions. Former NSA Director Gen. Keith B. Alexander described this concerted effort as "the greatest transfer of wealth in human history," and former House Intelligence Committee Chairman Mike Rogers (R-MI)--nearly a decade ago--called out the ongoing cyber economic war.

SK/C07.02) Jamil N. Jaffer [Executive Direcftor, National Security Institute, George Mason U.], NEWSWEEK, October 30, 2020, pNA, Gale Academic OneFile. During the same testimony, the DNI [Director of National Intelligence] noted that "China has the ability to launch cyber attacks [in the U.S.] that [could] cause...disruption of a natural gas pipeline for days to weeks."

b. IRAN IS A THREAT

SK/C07.03) Jamil N. Jaffer [Executive Direcftor, National Security Institute, George Mason U.], NEWSWEEK, October 30, 2020, pNA, Gale Academic OneFile. Just last year, then-Director of National Intelligence (DNI) Dan Coats told Congress that Iran is actively "preparing for cyber attacks against the United States and our allies" and is "capable of...disrupting a large company's corporate networks for days to weeks."

SK/C07.04) Fred Guterl, NEWSWEEK, February 7, 2020, pNA, Gale Academic OneFile. The most worrying cyber threat from Iran are those that could result in a loss of life. In this respect, Iran is capable of using hackers to support some kind of conventional military action, such as a bombing or the assassination of an individual or a kidnapping. It could also use cyber espionage or data collection techniques to monitor the movement of troops, ships or planes in the Middle east and target them for attack.

c. RUSSIA IS A THREAT

SK/C07.05) Jamil N. Jaffer [Executive Direcftor, National Security Institute, George Mason U.], NEWSWEEK, October 30, 2020, pNA, Gale Academic OneFile. Of course, we all know about Russia's wildly successful covert influence campaign that has undermined public confidence in our elections and rule of law institutions. While the Russian activities are likely to go down in history as among the most effective covert influence operations ever, what sometimes goes missed in all the election talk is the DNI's assessment that Russia is also actively "mapping our critical infrastructure with the long-term goal of being able to cause

substantial damage," including by "disrupting an electrical distribution network for at least a few hours."

2. NSA SURVEILLANCE IS VITAL FOR COUNTERINTELLIGENCE

SK/C07.06) Andrew C. McCarthy, NATIONAL REVIEW, March 23, 2020. p. 31+, Gale Academic OneFile. The "necessity of procuring good intelligence is apparent and need not be further urged," remarked General George Washington while commanding the Continental Army. "Upon Secrecy, Success depends in Most Enterprises... and for want of it, they are generally defeated." The acquisition of intelligence is and has always been a security imperative.

SK/C07.07) Andrew C. McCarthy, NATIONAL REVIEW, March 23, 2020. p. 31+, Gale Academic OneFile. Since national security is a duty of the executive, not the judiciary, it's only natural that the court would defer to the intelligence professionals on the matter of foreign threats. If the agents responsible for protecting the country have sketchy but frightening intelligence that, say, al-Qaeda is plotting a mass-murder attack, what judge would want to risk thwarting their investigation? The vast majority of the time, when there is some evidence of foreign threats, the judges should green-light surveillance.

SK/C07.08) Eric Manpearl [Sr. Graduate Fellow, Robert S. Strauss Center for International Security & Law], FLORIDA JOURNAL OF INTERNATIONAL LAW, 2018, NexisUni, p. 356. The Intelligence Community's routine collection of political intelligence is critical to ensuring that U.S. policymakers are informed and can make the best decisions regarding U.S. foreign policy actions. The limitation on the Intelligence Community's ability to collect political intelligence will result in the decreased effectiveness in obtaining critical information about foreign governments that could help U.S. policymakers in crafting their decisions.

SK/C07.09) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, p. 56. Finally, as Section 702 becomes less useful in the future, the Intelligence Community must improve collection under Executive Order 12333 to ensure that the government continues to acquire vital intelligence to protect United States national security interests. The National Security Agency (NSA) must continue to invest resources in being able to decrypt communications and acquiring unencrypted communications.

SK/C08. SECTION 702 PREVENTS TERRORIST ATTACKS

1. TERRORIST THREATS NECESSITATE NSA SURVEILLANCE

SK/C08.01) Deborah Samuel Sills [Intelligence Community Fellow, Georgetown U. Law Center], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2017, NexisUni, pp. 1-2. The rising globalization of terrorist organizations and their ever more sophisticated abilities

to reach people throughout the world has deepened the threat of terrorist activities both in the United States and abroad. Recent events show that terrorist groups overseas have influenced homegrown terrorist acts in the United States. Many of these same overseas terrorist organizations are recruiting thousands of new members from Western countries, including hundreds from the United States. In light of these growing threats, the United States must ensure that our country has the necessary legal authorities to anticipate and counter them. One such vehicle for providing the United States with these critical legal tools is through strengthening Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA).

SK/C08.02) Deborah Samuel Sills [Intelligence Community Fellow, Georgetown U. Law Center], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2017, NexisUni, pp. 2-3. Information collected pursuant to the FAA [Foreign Intelligence Surveillance Act (FISA) Amendments Act] Section 702 provides foreign intelligence information that is critical to the protection of the United States against terrorist threats. Members of the Intelligence Community believe that Section 702 collection offers valuable insights into the plans, objectives, and operations of terrorist organizations. For example, the NSA considers information acquired under Section 702 as the "most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world."

SK/C08.03) Deborah Samuel Sills [Intelligence Community Fellow, Georgetown U. Law Center], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2017, NexisUni, p. 3. Likewise, the former director of the National Counterterrorism Center (NCTC), Mathew G. Olsen, testified that "Section 702 collection was instrumental to our efforts to discern the intentions and capabilities of our terrorist adversaries, contributing both to our strategic judgments and tactical insights." Congress also recognizes that the intelligence obtained under Section 702 is essential to our national security, observing that this information is "often unique, unavailable from any other source, and regularly provides critically important insights and operationally actionable intelligence on terrorists and foreign intelligence targets around the world."

SK/C08.04) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, p. 120. Section 702 was a critical intelligence collection reform that addressed technological developments to enable the Intelligence Community to acquire vital foreign intelligence to protect United States national security interests and inform policymakers. Section 702 enables the Intelligence Community to collect intelligence on non-United States persons that are reasonably believed to be overseas when the Intelligence Community reasonably believes it will likely acquire foreign intelligence from surveilling these individuals without having to undergo the significant step of establishing probable cause that the target is an agent of a foreign power, probable cause that each facility is being used or is about to be used by a foreign power or agent of a foreign power, and that the information could not be reasonably obtained by normal investigative methods.

2. NSA SURVEILLANCE HAS THWARTED TERRORIST ATTACKS

SK/C08.05) Deborah Samuel Sills [Intelligence Community Fellow, Georgetown U. Law Center], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2017, NexisUni, pp. 3-4. Information acquired from Section 702 has aided the government's efforts in preventing potential terrorist attacks. For example, in September 2009, information acquired pursuant to Section 702 was instrumental in disrupting a terrorist attack on the New York City subway system. Using this information, the FBI identified and ultimately arrested Najibullah Zazi, a United States citizen living in the United States, for his role in an al-Qaeda plot to carry out suicide attacks on the New York City subway system.

SK/C08.06) Deborah Samuel Sills [Intelligence Community Fellow, Georgetown U. Law Center], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2017, NexisUni, p. 4. As another example, in 2008, information collected under Section 702 was used to uncover an al-Qaeda cell in Kansas City, Missouri that was in the initial stages of planning an attack on the New York Stock Exchange. Further, information obtained under Section 702 supported the arrest of David Coleman Headley, who had plotted to attack a Danish newspaper that had printed cartoons of the Prophet Muhammad and who had helped plan the 2008 Mumbai terrorist attacks.

SK/C08.07) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, pp. 496-497. Section 702 allows the "government to obtain the communications of foreigners outside the United States, including foreign terrorist threats." Section 702 has been instrumental in gathering foreign intelligence to protect United States national security interests, even within the country's borders. One example is the foiling of a plot to bomb the subway system in Manhattan. In 2009, Najibullah Zazi was arrested by authorities in connection with the plot, and he pleaded guilty to his crimes in 2010. The DNI confirmed that Section 702 data was critical in identifying Zazi and arresting him before he carried out his attack. Another example of Section 702's success was the tracking and killing of Hajji Iman, a United States citizen turned terrorist, who at one point became the second-in-command of the Islamic State of Iraq and Syria ("ISIS"). The DNI and other IC [intelligence community] agencies utilized Section 702 to gain information that led to an apprehension attempt that resulted in Iman's death.

SK/C08.08) Stephen Gemar [U. of South Dakota School of Law], SOUTH DAKOTA LAW REVIEW, 2020, NexisUni, p. 497. In recent years, there have been additional successes from Section 702. Using Section 702, the NSA was able to identify and become familiar with certain cybersecurity information relating to a hostile foreign government and individuals working for it as well as become familiar with the tactics employed by this government. Section 702 was also instrumental in helping the NSA gain first-hand knowledge of a target who was providing support to a "leading terrorist" in the Middle East. Through Section 702 data collection, the target was removed by a successful military operation.

SK/C08.09) Rachel G. Miller [U. of Notre Dame Law School], NOTRE DAME LAW

REVIEW, 2020, NexisUni, p. 140. Additionally, section 702 has proven commendable as a vast number of terrorist plots have been foiled through use of information obtained under section 702. For example, information obtained under section 702 led to the arrest of Najibullah Zazi, a U.S. citizen living in the United States, for his role in an al-Qaeda plot to carry out suicide attacks on the New York City subway system.

SK/C08.10) POSTMEDIA BREAKING NEWS, December 19, 2019, pNA, NexisUni. The case of Hasbajrami, arrested at New York's John F. Kennedy International Airport as he attempted to board a flight to Turkey, was returned to the trial court for a determination about whether evidence against him was lawfully collected and admissible under the Fourth Amendment. Prosecutors said Hasbajrami communicated by email with a non-American overseas, who he believed was associated with a terrorist organization.

3. ENDING SECTION 702 SURVEILLANCE LEAVES U.S. VULNERABLE

SK/C08.11) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, pp. 54-55. Section 702 of the FAA [FISA Amendments Act of 2008] is likely the most important statutory tool for intelligence collection, especially against terrorism, and is vital for protecting United States national security. In 2018, there were more than 164,000 Section 702 targets. The Intelligence Community would simply not be able to maintain nearly the same level of intelligence collection without Section 702. Further, Section 702 allows for collection to occur in a stable and safe domestic environment and can yield intact copies of the entirety of communications. This has been an extraordinary success story for United States signals intelligence (SIGINT) and developed as a response to changing technology and a new threat landscape.

SK/C08.12) John F. Schifalacqua [U. of Pennsylvania Law School], AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF, 2019, NexisUni, pp. 96-97. In retrospect, it was clear to the Privacy and Civil Liberties Oversight Board (PCLOB)--an entity that reviews the IC [intelligence community]--that "without the initial tip-off about Zazi and his plans, which came about by monitoring an overseas foreigner under Section 702, the subway bombing might have succeeded." In other words, foreign intelligence surveillance was critical in preventing the attack. Indeed, the IC has long held that the authority for surveillance granted by Section 702 is vital to national security. There are many more examples of successful counterterrorism beyond the Zazi plot to support this claim. Members of the IC have testified as recently as 2017 that Section 702 is such a critical tool that some "foreign intelligence cannot be practically obtained through other methods" and the authority is a major contributor to counterterrorism and counterintelligence. In fact, former FBI Director James Comey went as far as to say that Section 702 authorities are the "crown jewels" of counterterrorism, without which "we will be less safe as a country."

4. FAILURE TO STOP TERRORIST ATTACK WOULD BE A DISASTER

SK/C08.13) Daniel R. Godefroi [New England Law School], NEW ENGLAND LAW REVIEW, 2017, NexisUni, pp. 65-66. Since it is extremely difficult for authorities to prevent harmful attacks, the identification of terrorist groups and locations has quintessential importance. Not only have attacks become increasingly more difficult to identify, the potential damage that can be inflicted upon unsuspecting victims can be catastrophic. Modern day technology allows for terrorists to inflict damage on a terrifying level. Developments in chemical, biological, and nuclear weaponry can lead to thousands of deaths and can cause billions of dollars in damage. Failing to prevent an attack on this scale would have a catastrophic effect on American society. Failure to prevent such an attack is not an option.

SK/C09. SURVEILLANCE BAN WOULD BE A DISASTER

1. UNIVERSAL PRIVACY PROTECTION LEAVES CITIZENS PROTECTED

SK/C09.01) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, p. 97. Extending Fourth Amendment protections in a universal manner would reduce the difficulty presented by not being able to determine accurately a target's location because this factor would no longer matter as even non-United States persons overseas would receive Fourth Amendment protections. This embrace of universal privacy rights would be a major break with the United States' social compact tradition and would be an explicit rejection of the holding in Verdugo-Urquidez. The approach would also mean that the United States would be accepting the enormous security costs that would come from such a decision. The United States could not maintain nearly the same level of intelligence capabilities as the Intelligence Community currently has if the United States adopted the universalist approach. This would inevitably mean that the Intelligence Community would lose visibility into malicious actors and threats because the United States--as with all countries--has fewer resources to identify threats from foreigners abroad compared with its ability to identify threats from citizens inside the country. Ultimately, pursuing this path would greatly diminish the United States' capacity to gain intelligence to protect the United States' national security interests, the American people, and the Homeland.

SK/C09.02) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, p. 98. Professor Daskal argues that the rules that govern data collection activities "should presumptively apply to U.S. persons and non-U.S. persons alike, regardless of whether the target of the acquisition or the data being acquired is based in the United States--absent a determination that all parties to the communication are non-U.S. persons." This position is based on the desire to protect United States persons' communications that may be implicated in collection activities, especially through incidental collection. In practice, this proposal would mean that Fourth Amendment protections would be extended to most foreign intelligence surveillance targets as it would be extremely difficult to show that no one in a communication was a United States person or located inside the United States, especially if location becomes difficult to ascertain in the future.

The approach is certainly contrary to current practice and would extend Fourth Amendment protections to many foreigners abroad who are not part of the United States' social compact and have therefore not been granted the same privacy protections under law as United States persons.

SK/C09.03) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, p. 98. Professor Daskal's vast extension of Fourth Amendment protections to non-United States persons overseas would hinder the Intelligence Community's ability to gather intelligence and create a culture of diminished aggressiveness, which could result in troubling security harms--especially at a time when the United States faces an exceptionally complex threat environment.

2. WARRANT REQUIREMENT LEAVES CITIZENS UNPROTECTED

SK/C09.04) Rachel G. Miller [U. of Notre Dame Law School], NOTRE DAME LAW REVIEW, 2020, NexisUni, pp. 156-157. Further, implementing a requirement that the government must obtain a warrant before using a U.S. person identifier to query section 702 would severely hamper the speed and efficiency of operations by creating an unnecessary barrier to national security professionals' ability to identify potential threat information already in the lawful possession of the intelligence community.

SK/C09.05) Brittany Adams [U. of Washington School of Law], WASHINGTON LAW REVIEW, March 2019, NexisUni, p. 404. The IC [intelligence community] suggests that a warrant requirement would hamper the speed and efficiency of surveillance operations and run counter to national security by delaying or potentially prohibiting access to intelligence identifying impending threats.

3. SECURITY MUST TAKE PRIORITY OVER PRIVACY

SK/C09.06) Eric Manpearl [Law Clerk, U.S. Court of Appeals, Sixth Circuit], CATHOLIC UNIVERSITY LAW REVIEW, Winter 2020, NexisUni, p. 102. The government has an extremely strong interest in collecting foreign intelligence information and the Supreme Court has noted that "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation."