THE UNCONSTITUTIONALITY OF BULK DATA COLLECTION

RICHARD A. ROBERTSON*

As an eight-year military member and former member of the Intelligence Community, I understand the importance of information and data collection. Frequently, more data allows for better results and more predictive capability from data mining. However, in the post-9/11 world we seem to be consumed by our desire for security and, consequently, have begun to allow practices that our founders would have reviled. The purpose of this paper is to perform an honest analysis of the constitutionality of the National Security Agency's bulk data programs from both a historical and modern case law perspective.

---

* Deputy Prosecuting Attorney, Clark County Indiana Office of the Prosecuting Attorney. J.D. 2014, Ohio Northern University Claude W. Pettit College of Law, LL.M. 2016, The George Washington University Law School.

I. NATIONAL SECURITY AGENCY BULK DATA COLLECTION

> The NSA has built an infrastructure that allows it to intercept almost everything. With this capability, the vast majority of human communications are automatically ingested without targeting. If I wanted to see your emails or your wife's phone, all I have to do is use intercepts. I can get your emails, passwords, phone records, credit cards.[1]

As Edward Snowden indicates in the above statement, the National Security Agency (NSA)'s bulk data collection programs are vast.[2] However, an examination of their legality must be determined program by program, rather than making the blanket assertion that all of the programs are unconstitutional. Therefore, we should attempt to understand these programs to the largest extent possible, given classification issues.

A. The Phone Metadata Collection

On June 6, 2013, former NSA Contractor Edward Snowden shocked the world with a massive leak to The Guardian newspaper.[3] Mr. Snowden leaked a top secret order from the Foreign Intelligence Surveillance Court (FISC),[4] which detailed the mass collection of cellphone metadata from Verizon.5 Under this FISC order, the government required Verizon to hand over "all call detail records or 'telephony metadata' created by Verizon for communications between the United States and abroad" or "wholly within the United States, including local telephone calls."[6] Many presume that the NSA has been securing similar orders against the other cellular carriers as well.[7]

Following the Snowden leaks, Congress intervened to modify the phone records

---

[1] Ewen MacAskill, *The NSA Files*, THE GUARDIAN (June 10, 2013), https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why (quoting Edward Snowden).

[2] *Id.*

[3] *Id.*

[4] *See Edward Snowden: Leaks that Exposed US Spy Programme*, BBC NEWS (Jan. 17, 2014), http://www.bbc.com/news/world-us-canada-23123964. FISC was created by the Foreign Intelligence Surveillance Act (FISA) of 1978. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 92 Stat. 1783-98 (codified as amended at 50 U.S.C. §§ 1801–85c (1978)).

[5] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (quoting Secondary Order, *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc., No. BR13-80, 2 (FISA Ct. Apr. 25, 2013), https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order) (internal quotation marks omitted).

[6] *Id.*

[7] *See id.*; *see also* Lauren Carroll & Kirby Wilson, *Fact-Checking the NSA Phone Records Program*, POLITIFACT (June 4, 2015, 6:22 PM), http://www.politifact.com/truth-o-meter/article/2015/jun/04/fact-checking-nsa-phone-records-program/.

program.[8] As a result, companies are no longer required to turn over all of their data to the NSA; instead, companies maintain possession and the NSA requests the subsets it desires.[9] However, the need to discuss these programs in the absence of the USA Freedom Act is still timely given President Trump's proclivity for mass surveillance.[10]

B. *Midstream Data Collection and PRISM*

The Washington Post and *The Guardian* both published exposés on the NSA's PRISM program following Edward Snowden's leak to them on June 7, 2015.[11] PRISM is a top secret program through which the NSA has obtained direct access to the servers of major technology companies such as Microsoft, Facebook, Google, and Apple.[12] Although the NSA claims in the leaked power point slides that it collects data with the cooperation of individual corporations, corporations have denied such cooperation.[13] The program allows for real-time and in-depth surveillance of communications by those outside the United States and communications that either originate or terminate outside the United States.[14] Alarmingly, the program also surveils communications that take place entirely within the United States.[15]

Compared to the aforementioned FISC order to Verizon, which is just a court order to comply, PRISM is a content collection program.[16] PRISM allows the NSA to "collect material including search history, the content of emails, file transfers and live chats."[17] Federal law requires that companies honor requests from federal law enforcement agencies for data, subject to a search warrant (if content is involved).[18] Notably, PRISM does more than ask companies to fulfill their obligations under federal law; PRISM allows the NSA to overcome the need to obtain a warrant by

---

[8] *See* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268-313 (2015).

[9] *See id.*

[10] *See* Adam Klein, *Trump, Tech, and the Future of Government Surveillance*, CRUNCH NETWORK (Feb. 8, 2017), https://techcrunch.com/2017/02/08/trump-tech-and-the-future-of-government-surveillance/.

[11] *See* Barton Gellman & Laura Poitras, *British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.6fc00c34509e; *see also* Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 7, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[12] *See* Greenwald & MacAskill, *supra* note 11.

[13] *See id.*

[14] *See id.*

[15] *See id.*

[16] *See id.*

[17] *Id.*

[18] *See* 18 U.S.C. § 2703(a) (2009).

collecting whatever data it desires directly from the servers of the participating companies.[19] The NSA created the PRISM program to sidestep the need for a FISC order because it deemed the process too cumbersome.[20] PRISM has become the one of the NSA's most "important and valuable" sources for raw materials.[21]

PRISM is not the only way in which the NSA is collecting data on the Internet.[22] In the same leak as PRISM, Edward Snowden also revealed that the NSA is collecting internet and phone traffic utilizing "upstream collection."[23] Upstream collection is a tool that allows the NSA to collect data directly "from the major nodes and fiber cables" that connect the internet nationwide and globally.[24] A former AT&T technician revealed that the company was routing its network traffic records to the NSA.[25] A *New York Times* article revealed that the NSA has been pulling pictures from all forms of electronic communications, including emails, text messages, and video teleconferencing, in addition to social media.[26]

II. UNCONSTITUTIONALITY OF NSA BULK DATA COLLECTION—AN ORIGINALIST'S APPROACH

To understand the constitutionality of bulk data collection programs, one must first have an understanding of the Fourth Amendment—the governing constitutional provision on government searches and seizures of a citizen's property.

> 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.[27]

Given the extent to which programs like PRISM reach into the lives of U.S. citizens, we must examine the full extent of the evil the Fourth Amendment was designed to combat.

---

[19] *See* Greenwald & MacAskill, *supra* note 11.

[20] *See id.*

[21] *See id.*

[22] *See* Cory Bennett, *NSA to Defend Internet Collection in Court*, THE HILL (Dec. 16, 2014), http://thehill.com/policy/cybersecurity/227283-nsa-heads-to-court-to-defend-internet-collection.

[23] *See id.*

[24] *Id.*

[25] *See id.*

[26] In 2011, the time period covered by the document leaked by Edward Snowden, the NSA was collecting approximately 55,000 images per day, and had begun to rely on facial recognition to the same degree as fingerprints and other unique personal identifiers. *See* James Risen & Laura Poitras, *N.S.A. Collecting Millions of Faces from Web Images*, N.Y. TIMES (May 31, 2014), http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html?_r=0.

[27] U.S. CONST. amend. IV.

A. The General Warrant

"The 'general warrant' was a roving commission to police agents, in seeking out certain types of crime, to search anyone or any place, at anytime, anywhere."[28]

1. The General Warrant in England

The concept of the general warrant dates back to the Roman Empire where Cicero's general authority to search with such warrants was essentially unlimited.[29] In order to seize the goods, the accuser had to seal the documents in the presence of a witness and deliver the seized goods to the custody of the court within a definite timeframe.[30] Since the Romans occupied England for an extensive period of time, they significantly influenced Anglo-Saxon law.[31]

In England, the general warrant was a part of the writ system and was called the writ of assistance.[32] The writ of assistance dates back to 1360, when Parliament passed the first statute to attempt to reign in the methods and apparent abuses during the reign of Edward III.[33] Writs were issued by a court and always ceased to be active six months after the death of the King who reigned when they were issued.[34] The writs did not require evidence against the named person or a list of the items sought, beyond contraband or tax debts, in order to search that person's property.[35]

To illustrate the standard practices regarding a writ of assistance, it is useful to consider a case study. In 1593, people were making objectionable and allegedly libelous posters.[36] A court issued a warrant to three messengers, authorizing them to search for and arrest those suspected of making these posters.[37] The warrant provided authorization to "enter into all houses and places where any such [libelers]

---

[28] Hignut v. State, 303 A.2d 173, 182 (Md. Ct. Spec. App. 1973).

[29] *See* NELSON LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE U.S. CONSTITUTION 16 (1937). It should be noted that general warrants were not allowed for cases of theft, where a victim of theft "*had to describe with particularity* the goods he was seeking." *Id.* at 17.

[30] *See id.* at 17.

[31] *See id.* at 18. In fact, the influence of Roman law upon all of Western Christendom, including Anglo-Saxon England, was felt so greatly that it was instrumental in the development of the Law of War as well. *See* M.H. KEEN, THE LAWS OF WAR IN THE LATE MIDDLE AGE 13 (1961). This is due to the balancing of the Christian theory of Just War with the *jus gentium* of Rome which allowed for a great deal more violence than Christian Law of War would have on its own. *Id.*

[32] *Compare Amendment IV: Writs of Assistance*, U. CHI., http://press-pubs.uchicago.edu/founders/documents/amendIVs2.html (last visited Sept. 7, 2015), *with The Common Law and Civil Law Traditions*, U.C. BERKELEY, https://www.law.berkeley.edu/library/robbins/CommonLawCivilLawTraditions.html (last visited Sept. 7, 2015).

[33] *See* LASSON, *supra* note 29, at 22.

[34] *See* George G. Wolkins, *Writs of Assistance in England*, 66 PROC. MASS. HIST. SOC'Y 357, 357 (1936) (citing Act of Trade 1662, 14 Cha. 2, c. 11, § 5 (Eng.)), http://www.jstor.org/stable/25080334.

[35] *See id.* at 363.

[36] *See* LASSON, *supra* note 29, at 27.

[37] *See id.*

shall be remaining."[38] Upon the apprehension of such persons, the investigators were to search "any of the chambers, studies, chests, or other like places for all manner of writings or papers that may give light for the discovery of the libellers [*sic*]."[39]

King Charles I used general warrants (or writs of assistance) to seize and imprison people for merely displeasing him.[40] He was also known to use this power to search for documentary evidence displaying subversive ideas and messages—as he did against Sir Edward Coke.[41] Coke was a "celebrated authority on the common law" and an influential opponent of the King.[42] He had a number of documents that were deemed seditious, and in a move to help them politically, the King's Privy Council acted.[43] When Coke was on his deathbed in 1634, the Council sent a messenger with an order to search for "seditious papers."[44] Nearly all his property was confiscated, and his home ransacked.[45] In 1621, a member of Parliament had already warned against frequent use of writs of assistance, and many victims of Charles I's unfounded general warrants were elected to the Parliament of 1628.[46] Yet, after Parliament was firmly empowered, it was just as bad of a custodian of individual liberty as the previous system, and the writs were codified by statute in 1662.[47]

As the American colonial period came into its own, both sides of the Atlantic developed disdain for writs of assistance. John Wilkes had a reputation in 1760s England for anonymously printing pamphlets that criticized governmental policies.[48] In The North Briton, Number 45, part of Wilkes' pamphlet series, he was unusually critical, and the government took notice.[49] Lord Halifax, then Secretary of State, issued a warrant to four messengers to "make strict and diligent search for authors, printers, and publishers of a seditious and treasonable paper, entitled, The North Briton, No. 45, . . . and them, or any of them, having found to apprehend and seize, together with their papers."[50]

The warrant was general is all respects, including the people to be arrested, places to be searched, and things they were looking to seize.[51] Additionally, since the warrant did not state with particularity any of the aforementioned things, it could

---

[38] *Id.*

[39] *Id.* (quoting C.F. TUCKER-BROOKE, WORKS AND LIFE OF CHRISTOPHER MARLOWE 54 (1930)).

[40] *See id.* at 29.

[41] *Id.* at 31.

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *See id.* at 29–30.

[47] *See id* at 28–29, 33. Even though the practice continued under Parliament's authorization, they did determine that the practice appeared to be done arbitrarily in 1680. *Id.* at 38–39.

[48] See *id.* at 43.

[49] *See id.*

[50] *Id.*

[51] *Id.*

not possibly have contained a probable cause requirement—granting them essentially a "roving commission."[52] In three days, the commission arrested 49 people.[53] Eventually, authorities apprehended the printer of the offensive pamphlet, and the printer informed on Wilkes.[54] Wilkes had been waiting to get caught, and brought suit to invalidate the warrant.[55] Wilkes won his suit and was awarded significant damages.[56] In the decision issued in the case, Justice Pratt stated that the warrants were far too broad and vague because they would grant exorbitant power and discretion to those conducting the searches.[57]

2. The General Warrant in Colonial America

General warrants were authorized in the colonies in 1696 when William III empowered American customs agents with all the powers of their British counterparts, and the warrants were a frequent and preferred tool of government action.[58] When the Seven Years' War broke out, Britain began enforcing trade laws that had previously been largely ignored.[59] For the colony of Massachusetts, the most severe was the Molasses Act.[60] In colonial Massachusetts, rum production was central to the economy.[61] The Molasses Act required colonists to import their much needed molasses and sugar from the British West Indies.[62] Unfortunately, the British West Indies could not produce enough raw materials for the colony's needs.[63] Consequently, the colonists smuggled in the remainder of their materials from the French and Spanish.[64] Once the war broke out, the British had ample motivation to enforce the existing laws. Britain's military spending required as much revenue as possible from the colonies, and they did not want to fund the enemy by purchasing rum from the colonies that was produced with smuggled French materials.[65]

In 1760, customs agents were ordered to crack down on the smuggling of materials from France and Spain into the colonies.[66] As this crackdown began, the colonists started resisting the intrusions and searches of the British.[67] No longer were the colonists content to allow the British agents to enter and search by virtue of their positions alone.[68] The customs officers began to rely more heavily on the

---

[52] *See id.*
[53] *See id.*
[54] *Id.* at 44.
[55] *Id.*
[56] *Id.* at 45.
[57] *See id.*
[58] *Id.* at 53.
[59] *See id.* at 51–53.
[60] *See id.* at 51–52.
[61] *See id.* at 51.
[62] *Id.*
[63] *See id.* at 51–52.
[64] *See id.* at 52.
[65] *See id.* at 51–52.
[66] *Id.* at 52.
[67] *See id.* at 55.
[68] *See id.*

writs of assistance.[69] These writs were more open to abuse than those in England.[70] Because the writs expired six months after the issuing sovereign's death rather than after the execution of the initial search, the writ of assistance was essentially a blanket power to search any person, place, or effect as often as they wished—a license to harass perceived enemies with impunity.[71]

King George II died on October 25, 1760, so six months later, all writs he had presided over expired.[72] When the writs expired, sixty-three Boston merchants petitioned for a hearing on whether to grant new writs.[73] A court granted the writs, but James Otis Jr.'s closing argument against them sowed the seeds for the American Revolution.[74] Otis denounced the Crown's whole policy against the colonies and in particular the use of writs.[75] Describing the event years later, John Adams is often quoted as stating:

> I do say in the most solemn manner, that Mr. Otis's oration against the Writs of Assistance breathed into this nation the breath of life. [Otis] was a flame of fire! Every man of a crowded audience appeared to me to go away, as I did, ready to take arms against Writs of Assistance. Then and there was the first scene of opposition to the arbitrary claims of Great Britain. Then and there the child of Independence was born. In 15 years, namely in 1776, he grew to manhood, and declared himself free.[76]

Though American opposition to the writs of assistance continued to grow, few people resisted them between December 1761, the date on which the writs were affirmed, and the Stamp Act of 1765.[77]

The repeal of the Stamp Act did not satisfy the colonists.[78] After the Stamp Act's repeal, only two seizures were attempted, and both failed.[79] The second incident led to a legal review by the English Attorney General, who explained that the American customs officers were not vested with sufficient legal authority to issue the writs.[80] Unfortunately, the English authorities kept this decision secret from the American Colonies, and utilized the Townshend Acts[81] to both affirm the power of

---

[69] *See id.*

[70] *See id.* at 54 ("The discretion delegated to the official was . . . practically absolute and unlimited.").

[71] *See id.*

[72] *See id.* at 57.

[73] *See id.* at 58.

[74] *See id.* at 58–59.

[75] *See id.*

[76] *Id.* at 59 (quoting CHARLES FRANCIS ADAMS, WORKS OF JOHN ADAMS, SECOND PRESIDENT OF THE UNITED STATES, X, 276 (Little, Brown & Co., 1856)).

[77] *See id.* at 67.

[78] *See id.* at 68.

[79] *See id.*

[80] *See id.* at 70.

[81] These acts were import taxes levied by the British in 1767. *Townshend Acts*, HISTORY.COM, http://www.history.com/topics/american-revolution/townshend-acts (last visited Mar. 19, 2017). These taxes were levied on glass, lead, paints, paper, and tea that were being imported into the colonies. *Id.* The repeal of the Townshend Acts caused a temporary

courts in the colonies to issue writs of assistance, and to sooth objections by the English legal authorities regarding use of writs in the American colonies.[82]

Given the opposition to the writs of assistance, one would think then that the burgeoning United States government (in the form of the Continental Congress) would not use them. However, this was not the case.[83] During the American Revolution, about 40–45% of the population of the American colonies were patriots.[84] Meanwhile, between 15–20% of the population remained loyal to the Crown.[85] On August 28, 1777 the Continental Congress was notified that a large contingent of the British Army had landed at the head of the Chesapeake.[86] The Continental Congress recommended to the executive council of Pennsylvania that they arrest certain people (most of whom were Quakers)[87] who had shown opposition to the American cause.[88]

The Continental Congress also suggested seizing any documents related to "the Meetings of Sufferings, an institution of the Quakers."[89] Pennsylvania acted upon the recommendation of the Continental Congress and arrested and rushed all those named—and many others—to confinement without trial or hearing.[90] Their homes and papers were searched, and their desks were broken into, all in an attempt to find compromising documents.[91] Those jailed in this incident wrote in protest to the Pennsylvania government, highlighting how their detention violated the previously adopted Pennsylvania Declaration of Rights.[92] They argued that the writ was illegal under the Declaration of Rights for two reasons: first, it authorized inspectors to search all papers on the mere possibility that something incriminating would turn up; and second, it gave inspectors such broad authority that it permitted them to search every house in the town.[93] Additionally, after failing to provide copies of the warrant to those targeted for searches and arrests, the inspectors broke into desks and other document storage containers to seize materials not within the scope of the warrant.[94] Moreover, the warrant failed to limit the term of imprisonment as

---

truce between the colonies and Great Britain prior to the Revolutionary War. *Id.*

[82] *See* LASSON, *supra* note 29, at 70.

[83] *See id.* at 76.

[84] ROBERT M. CALHOON, A COMPANION TO THE AMERICAN REVOLUTION 235 (Jack P. Greene & J. R. Pole eds., 2003).

[85] *Id.*

[86] LASSON, *supra* note 29, at 76.

[87] Karin A. Wulf, *"Despise the Mean Distinctions [These] Times Have Made:" The Complexity of Patriotism and Quaker Loyalism in One Pennsylvania Family,* http://revolution.h-net.msu.edu/essays/wulf.html (last visited Sept. 27, 2015) (explaining that most of the neutral parties in the Revolution were Quakers).

[88] LASSON, *supra* note 29, at 76.

[89] *Id.*

[90] *See id.*

[91] *See id.*

[92] *See id.* (noting that the Pennsylvania Declaration of Rights prevented general warrants while guaranteeing the elements of a fair trial).

[93] *See id.*

[94] *See id.*

required for all warrants under Pennsylvania law.[95] Despite the Continental Congress's recommendation that Pennsylvania hear the petitioners, the Pennsylvania council declined to hold a hearing because they claimed they lacked the time in light of their other obligations, including running the militia.[96] In response, Pennsylvania recommended that the Congress hear the case instead. [97] The Congress declined to hold the hearing as well, citing federalism concerns because the protestors resided in Pennsylvania.[98] Despite the writ of habeas corpus, Pennsylvania Chief Justice Thomas McKean sent the prisoners to Virginia in 1778.[99]

B. The Fourth Amendment—The Writing and Ratification

"Now the right to life has come to mean the right to enjoy life, -- the right to be let alone."[100]

As seen above, the founders had grave concerns about the issue of the general warrant, which helped spark the revolution.[101] Unsurprisingly, the fledgling United States incorporated general warrant protections early.[102] Following the Declaration of Independence, all former colonies drafted either a Declaration or Bill of Rights that included some provision against the general warrant.[103] Pennsylvania's 1776 Declaration of Rights was the first true precedent for the Fourth Amendment because it condemned the general warrant and also articulated a principle that is now taken for granted—the principle of freedom from unreasonable search and seizure.[104] Moreover, Massachusetts's 1780 Declaration of Rights originated the expression "unreasonable search and seizure."[105] New Hampshire's 1784 Bill of Rights copied the unreasonable search and seizure language.[106]

After the Articles of Confederation failed, the Continental Congress was called and wrote the Constitution.[107] During the Constitutional Convention, two groups,

---

[95] *See id.*

[96] *See id.* at 77.

[97] *See id.*

[98] *See id.*

[99] *See id.*

[100] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[101] *See* LASSON, *supra* note 29, at 59 (quoting ADAMS, *supra* note 76, at 276).

[102] *See id.* at 80.

[103] *Id.* at 80.

[104] PA. CONST. of 1776, Declaration of Rights, art. X, *available at* http://press-pubs.uchicago.edu/founders/documents/bill_of_rightss5.html (last visited Nov. 1, 2015).

[105] LASSON, *supra* note 29, at 82.

[106] *Id.*

[107] In fact, the Federal Constitutional Convention was the second convention held to address issues with the Articles of Confederation. Gregory E. Maggs, *A Concise Guide to the Records of the Federal Constitutional Convention of 1787 as a Source of the Original Meaning of the U.S. Constitution*, 80 GEO. WASH. L. REV. 1707, 1710–11 (2012). The first convention, held in Annapolis in 1786, only succeeded in deciding that there were "important defects in the system of Federal government," which set the stage for the convention in 1787 in which the constitution was ultimately drafted. *Id.*

the Federalists and the anti-Federalists, engaged in various debates concerning the relationship between the states and the federal government.[108] While both groups believed in state sovereignty and the protection of individual liberties, they disagreed on how much sovereignty the states should enjoy and how much individual liberties should be protected.[109] The Federalists believed in a strong central government, whereas the anti-Federalists believed the States should be the dominant force.[110] In particular, the Federalists narrowly interpreted the drafted Constitution with respect to limits on Federal power.[111]

Five days before the Continental Congress adjourned, the issue of a Bill of Rights came to the floor.[112] The anti-Federalists argued for the inclusion in the Bill of Rights of an amendment addressing general warrants.[113] In response, the Federalists found the Bill of Rights both unnecessary and dangerous.[114] James Wilson, a Federalist leader, argued that, under the Constitution, powers not expressly granted to the Federal government were reserved to the states.[115] Therefore, according to Wilson, a Bill of Rights was dangerous because "a complete list of rights of the people was impossible and to stipulate some of them would be to imply that whatever was not expressed was surrendered."[116] The anti-Federalists maintained that the Bill of Rights was imperative to the new constitution.[117] They further argued that the Constitution, as drafted, created a strong central government that warranted the Bill of Rights to ensure that the Federal government could not infringe upon certain central rights belonging to states or individuals.[118] In contrast to Wilson's positions, John Smilie responded that the Federalists already conceded the necessity for a Bill of Rights by including language relating to the right of Habeas Corpus in the proposed Constitution.[119] John Whitehall, another participant of the convention, posed a seemingly prophetic question:

> I wish it to be seriously considered whether we have a right to leave the liberties of the people to such future constructions and expositions as may possibly be made upon this system; particularly when its advocates, even at this day, confess that it would be dangerous to omit anything in the enumeration of a

---

[108] *See generally Anti-Federalist v. Federalist*, http://www.diffen.com/difference/Anti-Federalist_vs_Federalist (last visited Nov. 1, 2015).

[109] Joe Wolverton, II, *Federalists, Anti-Federalists, and State Sovereignty*, http://tenthamendmentcenter.com/2011/04/21/federalists-anti-federalists-and-state-sovereignty/ (last visited Nov. 1, 2015).

[110] *Id.*

[111] *Id.*

[112] LASSON, *supra* note 29, at 83.

[113] *Id.*

[114] *Id.* at 84, 85.

[115] *Id.* at 90.

[116] *Id.* (citing JOHN BACH MCMASTER & FREDERICK STONE, PENNSYLVANIA AND THE FEDERAL CONSTITUTION, 1787-1788, 576 (1888)).

[117] *Id.* at 87.

[118] *Id.*

[119] *Id.* at 91.

> bill of rights, and according to [the principle articulated by Wilson that all rights not delegated are reserved], the reservation of the habeas corpus, and trial by jury in criminal cases, may hereafter be construed to be the only privileges reserved to the people.[120]

An attempt was even made by Richard Henry Lee of Virginia to append a bill of rights to the Constitution before submitting it to the states for ratification; ultimately this was not done.[121] However, the Constitutional Convention would not have ratified the Constitution with the tacit understanding that a future Bill of Rights would be passed to protect personal liberties.[122] After George Washington's inauguration as president in 1789, James Madison gave notice of his intent to offer the amendments that would one day become the Bill of Rights, including the Fourth Amendment.[123] When speaking to the Virginia convention the previous year, Madison spoke about the need for the amendments.[124] Mr. Madison argued:

> It is true, the powers of the General Government are circumscribed, they are directed to particular objects; but even if [the] Government keeps within those limits, it has certain discretionary powers with respect to the means, which may admit of abuse to a certain extent, in the same manner as the powers of the State Governments under their constitutions may to an indefinite extent; because in the constitution of the United States, there is a clause granting to Congress the power to make all laws which shall be necessary and proper for the carrying into the execution all powers vested in the Government of the United States, or in any department or officer thereof; this enables them to fulfill every purpose for which the Government was established. Now, may not laws be considered necessity and propriety to accomplish those special purposes which they have in contemplation, which laws in themselves are neither necessary or proper; as well as improper laws could be enacted by the State Legislatures, for fulfilling the more extended objects of these governments. I will state for instance, which I think in point, and proves that this might be the case. The General Government has a right to pass all laws which shall be necessary to collect its revenue; the means for enforcing the collection are within the discretion of the Legislature; may not general warrants be considered necessary for this purpose, as well as for some purposes which it was supposed at the framing of their constitutions the State Governments had in view? If there was reason for restraining the State Governments from exercising this power, there is like reason for restraining the Federal Government.[125]

The Fourth Amendment emerged after several drafts.[126] Madison proposed the first of a series of drafts.[127] While Madison's proposal contained a bar to unreason-

---

[120] *Id.* (quoting MCMASTER & STONE, *supra* note 116, at 576, 262).

[121] *Id.* at 87.

[122] *Id.* at 97.

[123] *Id.* at 98.

[124] James Madison, among the most ardent supporters of the notion of the self-limiting Constitution, surprisingly took this anti-Federalist position. *Id.* at 99.

[125] *Id.* at 99 (quoting 1 ANNALS OF CONG. 455–456 (1789) (emphasis added)).

[126] *See id.* at 100.

[127] *Id.* at 100.

able searches and seizures, it did not have a warrant requirement.[128] When the House of Representatives voted on the Amendment, the Amendment's original language read as follows:

> The right of the people to be secured in their persons, houses, papers, and effects, shall not be violated by warrants issuing without probable cause, supported by oath or affirmation, and not particularly describing the place to be searched, and the persons or things to be seized.[129]

In point of actual fact, the House voted down the current language.[130] The House's approved language came to existence after the Committee in charge of arranging the amendments held a vote.[131] No one in the House noticed the change before the states ratified the Amendment, which helps explain why the change still stands today.[132] The reason behind the current phrasing is that Egbert Benson, the Committee Chair, believed that the original Amendment's phrasing only created the need for a valid warrant and did not reach the broader issue of freedom from unreasonable searches and seizures.[133] Benson's change of the language sought to remedy that problem by creating two clauses: 1) valid warrants and 2) freedom from unreasonable searches and seizures.[134]

1. Why the bulk data programs are violating the Fourth Amendment.

In interpreting the Fourth Amendment, one should consider the evil it was designed to prevent. Failure to do so would render the Fourth Amendment vacuous. At the time, the Fourth Amendment was drafted, the American founders had just fought a war caused, in part, by the use of general warrants.[135] The crown used these warrants to effectively suppress the colonists' ability to trade and produce, as well as quash any activity that it viewed as seditious.[136] General warrants are an easy analog to the NSA programs in question here.

i. PRISM and Midstream Collection

The PRISM system allows the NSA to circumvent the warrant requirement under the Fourth Amendment to obtain direct access to the mainframes of big technology and software companies, and ultimately, pull data pertaining to Americans directly from the remote storage facilities.[137] The NSA is using this access to hunt for any

---

[128] *Id.*
[129] *Id.* at 101.
[130] *Id.*
[131] *Id.*
[132] *Id.* at 102.
[133] *Id.* at 103.
[134] Since this changed language was the language voted upon and approved by Congress and ratified by the states, the intended version has no binding effect. *Id.*
[135] *See generally* LASSON, *supra* note 29 (quoting ADAMS, *supra* note 76).
[136] *See generally id.*
[137] *See* Gellman & Poitras, *supra* note 11; Greenwald & MacAskill, *supra* note 11.

materials that would indicate a person is associated with terrorism.[138] This bares striking resemblance to the Crown's use of the general warrant, where in one case, the warrant permitted the investigators to search "any of the chambers, studies, chests, or other like places for all manner of writings or papers that may give light for the discovery of the libellers [sic]."[139]

In both cases, the government determined an offense that it deemed of great interest to it and/or the protection of itself. In the case of the Crown, it was frequently libel and/or sedition.[140] In the case of the modern United States, the offense of interest is terrorism.[141] British writs of assistance granted essentially a non-expiring roving commission to hunt down anyone and everyone they believed had created libelous materials, enter their property, and search their papers and effects without the need for probable cause or additional judicial oversight.[142] NSA practices under PRISM comport even less with notions of due process than the writs of assistance. Whereas the Crown at least had to use a court to generate the writ,[143] PRISM, which the NSA crafted solely under executive authority, circumvents the statutorily constructed FISA Court.[144] Additionally, PRISM—much like its cousin the writ of assistance—has no foreseeable ending date.[145]

PRISM is effectively an electronic roving commission that allows the NSA to search Americans' files through technology companies' servers to look for connections to terrorism.[146] This pervasive roving authority to search is more than reminiscent of the search authority granted by British writs of assistance. Because the NSA's search powers under PRISM do not naturally terminate,[147] the roving search

---

[138] Loren Thompson, *Why the NSA's Prism Program Makes Sense*, FORBES (June 7, 2013, 3:05 PM), http://www.forbes.com/sites/lorenthompson/2013/06/07/why-nsas-prism-program-makes-sense.

[139] LASSON, *supra* note 29, at 27 (quoting TUCKER-BROOKE, *supra* note 39).

[140] *Id.* at 26.

[141] Thompson, *supra* note 138.

[142] LASSON, *supra* note 29, at 26–27.

[143] The courts in question were the Courts of Star Chamber and High Commission. *Id.* at 25–26.

[144] *See* Greenwald & MacAskill, *supra* note 11.

[145] Please note, however, that the writ of assistance would expire six months following the death of the king who issued the writ. LASSON, *supra* note 29, at 57. None of the new publications regarding PRISM indicate that the NSA or the President contemplate ever terminating the program, and since it is not a creature of statute there is no sunset provision. *See, e.g.*, Benjamin Dreyfuss & Emily Dreyfuss, *What is the NSA's PRISM Program? (FAQ)*, CNET (June 7, 2013, 11:44 AM), https://www.cnet.com/news/what-is-the-nsas-prism-program-faq/; T.C. Sottek & Joshua Kopstein, *Everything You Need to Know About PRISM*, THE VERGE (July 17, 2013, 1:36 PM), http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet; Chris Strohm, *FBI and NSA Poised to Gain New Surveillance Powers Under Trump*, BLOOMBERG (Nov. 29, 2016, 5:00 AM), https://www.bloomberg.com/news/articles/2016-11-29/fbi-and-nsa-poised-to-gain-new-surveillance-powers-under-trump.

[146] Greenwald & MacAskill, *supra* note 11.

[147] *See, e.g.*, Dreyfuss & Dreyfuss, *supra* note 145; Sottek & Kopstein, *supra* note 145;

authority exceeds the authority conveyed under a classical writ of assistance. In an age where we are being encouraged evermore to engage in cloud storage for all our personal files,[148] we are in fact being invited to hand over our files to be searched by the NSA, rendering Fourth Amendment protections moot.

For mid-stream data collection, the NSA pulls data directly from major nodes and fiber cables that carry the internet.[149] The NSA is again executing a roving authority to search all of the data and internet transactions of billions of people—including Americans entitled to the protections of the Fourth Amendment—to search for indications that a person is associated with terrorism.[150] Whether or not the NSA has people looking at the data is irrelevant. Therefore, both the PRISM and mid-stream programs are unconstitutional under an analysis of purpose and original intent of the Fourth Amendment.

ii. Cellphone Metadata

The NSA's cellphone metadata collection was conducted pursuant to a FISA Court (FISC) order for the production of all cell records for a given cell carrier.[151] The FISC order was based on the idea that the collection of all the phone records was relevant to terror investigation, pursuant to a statutory rule in the USA PATRIOT Act.[152] There is a clear distinction between relevance and probable cause. However, even without addressing the constitutionality of the USA PATRIOT Act, the FISC order was still unconstitutional because the FISC granted a roving commission to the NSA to seize the records and search them.[153] An original intent analysis of constitutionality under the Fourth Amendment starts with determining who owns the records (most likely the cellphone company), and then determining who the victim of the unwarranted search was.[154]

When an owner of a non-trust bank account makes a deposit with the bank, the funds deposited cease to be the depositors and become the property of the bank.[155] Meanwhile, the depositor maintains a creditor interest.[156] The relationship between the depositor and the bank is contractual in nature.[157] When the depositor deposits

---

Strohm, *supra* note 145.

[148] *See* Quentin Hardy, *Google, Microsoft and Others Delve Deeper into Cloud Storage for Businesses*, N.Y. TIMES (June 25, 2014), https://www.nytimes.com/2014/06/26/technology/google-microsoft-and-others-delve-deeper-into-cloud-storage-for-businesses.html.

[149] Bennett, *supra* note 22.

[150] *See* Greenwald & MacAskill, *supra* note 11.

[151] Greenwald, *supra* note 5.

[152] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 [hereinafter USA PATRIOT Act], Pub. L. No. 107-56, 115 Stat. 272, 286 (2001).

[153] *See* Greenwald, *supra* note 5.

[154] *See* U.S. CONST. amend. IV.

[155] Shipman v. Bank of New York, 27 N.E. 371, 371 (N.Y. 1891).

[156] *Id.*

[157] *Id.* at 372.

the money, he loses the possessory interest in the money; the bank gains a possessory interest; and the depositor takes on a creditor interest in the deposited money.[158] The banks, therefore, also own the records regarding the accounts. Similarly, in order for a cellphone owner to place a call, he must have entered into a contract of some sort with the cellphone company.[159] The call utilizes the cellphone company's equipment,[160] and the cellphone company maintains the information of numbers called and length of call for the purposes of billing, forming a record in the course of regular business.[161] Therefore, the cellphone records belong to the cellphone companies.

If the cellphone records belong to the cell companies, then the historical analysis is concluded, and the unconstitutionality of the bulk data collection will be derived later in this paper. However, if the cell records are property of the phone owner, then the lack of a particularized warrant is the same sort of roving search authority as discussed in the PRISM section and would constitute an unlawful search.

III. FOURTH AMENDMENT—THE MODERN INTERPRETATION RELATING TO ELECTRONIC SURVEILLANCE

A. The Law

The Supreme Court's interpretation of the Fourth Amendment has undergone quite a bit of evolution.[162] This evolution begs two questions: whether the Fourth Amendment protects places or people; and whether the Fourth Amendment protects against unreasonable searches and seizures of both intangible and tangible personal property.[163] In *Olmstead v. United States*, the Court for the first time looked at the issue of "whether the use of evidence of private telephone conversations between the defendants and others, intercepted by means of wiretapping, amounted to a violation of the Fourth and Fifth Amendments."[164]

The Court in *Olmstead* held that wiretapping without a warrant is constitutional so long as there is no physical trespass onto the property of the suspect.[165] The Court stated unequivocally that "[t]he language of the Amendment can not [sic] be extended and expanded to include telephone wires reaching to the whole world

[158] *Id.*

[159] *See* Liane Cassavoy, *Before You Sign a Cell Phone Contract: What You Need to Know*, LIFEWIRE (Apr. 6, 2017), https://www.lifewire.com/before-signing-cell-phone-contract-579606.

[160] *See* Rong Wang, *How Do Cell Phones Work?*, PONG (Dec. 20, 2014), http://www.pongcase.com/blog/cell-phones-work/#sthash.0NUUVQdL.dpbs.

[161] *See* Suzanne Choney, *How Long Do Wireless Carriers Keep Your Data?*, NBC NEWS (Sept. 29, 2011, 3:05 PM), http://www.nbcnews.com/tech/mobile/how-long-do-wireless-carriers-keep-your-data-f120367.

[162] Goldman v. United States, 316 U.S. 129 (1942); Olmstead v. United States, 277 U.S. 438 (1928).

[163] *Goldman*, 316 U.S. 129; *Olmstead*, 277 U.S. 438.

[164] *Olmstead*, 277 U.S. at 455.

[165] *Id.* at 466.

from the defendant's house or office."[166] In its reasoning, the Court considered whether the Fourth Amendment protected tangible versus intangible things, and determined via a textualist analysis that the Amendment covered only tangibles.[167] In *Goldman v. United States*, the Court further emphasized their non-focus on privacy when they upheld the use of a detectaphone held to the wall between apartments in order to listen into one-half of a telephone conversation.[168] In this instance, the Court refused to acknowledge a meaningful difference between communications projected out into the world on a telephone—assuming the risk of the signal being intercepted on the line—and a person talking in their own office where they do not expect to be overheard.[169]

Thankfully, in the Court's interpretation of the Fourth Amendment, the focus transitioned from protecting tangible property (as was the prevailing view under *Olmstead* and *Goldman*) to preserving a person's privacy, thereby protecting both tangible property and intangible property.[170] In *Katz*, the Supreme Court held that "the Fourth Amendment protects people, not places."[171] "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[172] The Court then specifically noted that it had already rejected the notion that the Fourth Amendment did not protect intangibles.[173]

Ultimately, the modern test for the Fourth Amendment is derived from Justice Harlan's concurrence in *Katz*: whether or not a subject has a reasonable expectation of privacy.[174] While the case did not deal with national security, Justice White argued in his concurrence that the warrant requirement should not exist in the national security context, stating that "[w]e should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable."[175] However, Justice Douglas, joined by Justice Brennan, disagreed, arguing instead that judicial authorization should still be required.[176]

Other than *Katz*, the other seminal case for our consideration is *Smith v. Maryland*.[177] In *Smith*, the Court examined whether the use of a trap and trace or key register required a warrant.[178] This case was, again, in the criminal context rather than national security context; however, the Court ruled that even in the criminal

---

[166] *Id.* at 465.
[167] *Id.* at 463–65.
[168] *Goldman*, 316 U.S. at 135–39.
[169] *See id.*
[170] *See generally* Katz v. United States, 389 U.S. 347 (1967).
[171] *Id.* at 351.
[172] *Id.*
[173] *Id.* at 353 (citing Silverman v. United States, 365 U.S. 505, 511 (1961)).
[174] *Id.* at 360–61 (Harlan, J., concurring).
[175] *Id.* at 364 (White, J., concurring).
[176] *Id.* at 359 (Douglas, J., concurring).
[177] Smith v. Maryland, 442 U.S. 735 (1979).
[178] *Id.* at 735.

context, trap and trace and key registers do not require a warrant under the Fourth Amendment.[179] The Court reasoned that call data—the number from which the call originated, the number dialed, and the length of the call—were not protected under the Fourth Amendment.[180] That data belongs to the company as part of their business records, and not to the individual.[181] Therefore, the individual does not have a reasonable expectation of privacy in a third party's business record.[182]

In his dissent, Justice Stewart (joined by Justice Brennan) argued that the necessity of using public phone equipment and lines to place phone calls does not negate a reasonable expectation of privacy.[183] He argued that the caller made the calls, which inevitably shared the call data with the phone company, reasonably expecting that the company would not share the information with the world.[184] Justice Stewart argued that this is the natural extension of the decision in *Katz*.[185]

This unprotected call data does not pertain to the content of the conversation, only the information that the phone company utilizes for billing purposes—what we now term metadata.[186] Following the *Smith* decision, Congress enacted legislation requiring law enforcement to seek a subpoena to examine metadata.[187] While the legislation does not require the government or the police to establish probable cause, it does require an affidavit swearing that the trap and trace or key register be relevant to an ongoing investigation.[188] It should be noted that these statutes were incorporated into the national security domain by the USA PATRIOT Act.[189] The USA PATRIOT Act accomplished this incorporation by modifying the Foreign Intelligence Surveillance Act (FISA) statute.[190]

In 1978, Congress developed FISA to be the sole means of domestic foreign intelligence collection.[191] FISA does not severely restrict the President's ability to act in foreign intelligence collections outside the United States.[192] The President's only limitations in the collection of intelligence arise from potential Constitutional protections of U.S. citizens who may be outside the United States[193] and minimiza-

[179] *Id.* at 744–46.
[180] *Id.* at 745–46.
[181] *See id.* at 743.
[182] *Id.* at 743–44.
[183] *Id.* at 746–47 (Stewart, J., dissenting).
[184] *Id.* at 746–47 (Stewart, J., dissenting).
[185] *Id.* at 747–48 (Stewart, J., dissenting).
[186] *Id.* at 739.
[187] *See* 18 U.S.C. § 2709 (2017).
[188] 18 U.S.C. §§ 3121, 3123 (2016).
[189] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, §§ 214–15 (2001).
[190] *Id.*
[191] 50 U.S.C. § 1809(a)(1) (2016).
[192] *Id.* § 1804(a)(6)(B).
[193] The Supreme Court held in *Reid v. Covert* that the right to due process follows a U.S. citizen whether or not they are in the United States, and the question of what process is due is determined by the totality of the circumstances. 354 U.S. 1, 8–9 (1957). While the Supreme Court has not weighed in, the Second Circuit did hold that Fourth Amendment Protections were not vested in citizens outside the United States. United States v. Odeh (*In re* Ter-

tion requirements under FISA.[194]

The courts have continued to drift towards an individual privacy-centric approach to the Fourth Amendment.[195] The Sixth Circuit Court of Appeals held in *United States v. Warshak* that portions of the Stored Communication Act (18 U.S.C. § 2701 *et. seq.*) were unconstitutional.[196] The act as it was written provided for different levels of protections depending on the length of time an email was stored, and required a warrant only for emails that were stored for less than 180 days.[197] Emails older than 180 days were obtainable by law enforcement by (1) obtaining a warrant; (2) using an administrative subpoena; or (3) obtaining a court order under 18 U.S.C. § 2703(d).[198] The Court held that the expectation of privacy and Fourth Amendment protections afforded to the emails did not change based on how long the emails were stored.[199] Additionally, the Supreme Court recently held in a unanimous opinion that the search of a suspect's smart phone incident to arrest was unconstitutional without a warrant.[200] In her concurrence in *Jones*, Justice Sotomayor suggested that the Court needs to reexamine the third party exceptions doctrine that allows records and files maintained by a third party, either at the request of an individual or as a result of the individual doing business with a particular person or company, to be acquired by police without probable cause or a warrant.[201]

B. The Bulk Data Programs are Unconstitutional—Modern Reasoning

The Bulk Data Programs are justified largely by Section 215 of the USA PATRIOT Act.[202] In granting the authorization orders, the FISC—on at least one occasion—stated that the decision regarding the third party exception articulated in *Smith v. Maryland* is still controlling.[203] *Smith* makes a distinction between the collection of content and non-content data.[204] This distinction is important for a constitutional analysis because when content is being sought, the courts have crafted an exception to the Fourth Amendment for national security that was alluded to in Justice White's concurrence to *Katz*.[205] This exception extends as far back as World

---

rorist Bombings), 552 F.3d 157, 159 (2d Cir. 2008).

[194] *See* 50 U.S.C. §§ 1801(a)(1)(C), 1813(b)(3)(B).

[195] Interestingly, this appears to only be true in the context of criminal law and not national security law, as will be discussed later.

[196] United States v. Warshak, 631 F. 3d 266, 274 (6th Cir. 2010).

[197] *Id.* at 283.

[198] *Id.*

[199] *Id.* at 274.

[200] Riley v. California, 134 S. Ct. 2473, 2495 (2014).

[201] United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

[202] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, § 215.

[203] *See In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [redacted], No. BR 13-158, 5 (FISA Ct. Oct. 11, 2013).

[204] Smith v. Maryland, 442 U.S. 735, 743 (1979).

[205] *See* Katz v. United States, 389 U.S. 347, 364 (1967) (White, J., concurring). *See generally* L. Rush Atkinson, *The Fourth Amendment's National Security Exception: Its History*

War II, and was viewed then as an "intelligence only" tool by the FBI director, J. Edgar Hoover.[206] The exception was built around the friction between the Fourth Amendment's protections, and the President's inherent power and responsibility to protect the nation.[207]

However, the language of the Fourth Amendment is unambiguous, and never contemplates the creation of any exceptions—let alone one at the sole discretion of the President.[208] The very notion seems to be in conflict with the principle of separation of powers that the founders integrated into the Constitution. However, a reinterpretation which departs from a carte blanche national security exception in favor of a case-by-case determination would reach many of the same results, and realign law and policy with constitutional principles.

C. *Fourth Amendment Exceptions or Reasonability?*

Over the years, the Supreme Court has crafted a number of so-called exceptions to the Fourth Amendment such as (1) search incident to arrest,[209] (2) automobile exception,[210] (3) hot pursuit,[211] and (4) exigent circumstances.[212] In every case, as the Court begins to contemplate an exception, it always returns to the text of the Fourth Amendment, and discusses the presumed unreasonableness of searches without a warrant and/or probable cause.[213] For instance, if a police officer has probable cause to believe that contraband is inside an automobile, few would argue that it is unreasonable for the police officer to perform the search at the time he obtains probable cause.[214] Since the vehicle is mobile, there is a fair chance that the subject vehicle will vanish and/or the contraband inside will be destroyed before the police can obtain the warrant.[215] This reasoning led the way to the automobile exception,[216] and similar reasoning generated the other exceptions.

The national security exception is different from the other exceptions in a few ways, but largely in scope. The other exceptions are very narrow. The automobile exception applies to vehicles due to their mobility.[217] Hot pursuit is restricted to the immediate pursuit of the suspect.[218] This is not the case with the national security exception. The national security exception is cited for a wide array of instanc-

and Limits, 66 VAND. L. REV. 1343, 1405 (2013).

[206] Atkinson, *supra* note 205, at 1346–47.

[207] *Id.* at 1345–46.

[208] *See* U.S. CONST. amend. IV.

[209] Chimel v. California, 395 U.S. 752, 770–71 (1969).

[210] Carroll v. United States, 267 U.S. 132, 155–56 (1925).

[211] United States v. Santana, 427 U.S. 38, 41–42 (1976).

[212] Coolidge v. New Hampshire, 403 U.S. 443, 460 (1971).

[213] *See Chimel*, 395 U.S. at 768; *Carroll*, 267 U.S. at 143, 159; *Santana*, 427 U.S. at 42; *Coolidge*, 403 U.S. at 454–55.

[214] *Carroll*, 267 U.S. at 153.

[215] *Id.* at 146.

[216] *See id.*

[217] *See id.*

[218] *See Santana*, 427 U.S. at 42–43.

es: the placing of surveillance equipment in a room, wiretaps, trap and trace, or whenever else the executive believes that national security is at stake or there is an intelligence interest.[219]

Given the rebuttable presumption that all warrantless searches are *per se* unreasonable, the mere fact that the executive's power under the national security exception is so broad should make it nearly impossible for the exception to survive as a whole. Instead, each individual attempted use, or at a minimum categorical use, of the exception should be measured against an objective reasonability standard. In fact, it appears Congress believed this standard applies at least to the President's power to use the domestic security exception, due to the enactment of FISA. FISA establishes the sole means by which the executive can collect intelligence or investigate foreign powers, agents of foreign powers, and international terrorism within the United States.[220]

If the FISA statute had not been changed, it would have limited the use of the FISC orders solely to the realm of non-criminal matters—echoing Director Hoover's belief of the "intelligence only" national security exception.[221] However, that is not the case. Most recently, the USA PATRIOT Act included language that allowed the FISC to grant a search order so long as a significant purpose of the search is foreign intelligence or anti-terrorism.[222] This new language opens the door to abuse by law enforcement since it allows otherwise illegal surveillance if its purpose is significantly, albeit non-primarily, for intelligence.[223]

This new power of allowing information gained during intelligence surveillance to be utilized in a criminal proceeding is chilling. The FISC, operating under the legal notions of *Smith*, does not require probable cause to collect telephone metadata, rather merely a sworn statement of the metadata's relevance to an on-going investigation.[224] Beyond that, when the FISC does issue warrants for content, they claim to use probable cause as required by statute and by the Fourth Amendment; however, they do not.[225] The FISC uses a lower standard of evidence to establish "probable cause" than that of the criminal courts under Title 18.[226]

---

[219] *See generally* Atkinson, *supra* note 205.

[220] 50 U.S.C. § 1802(b).

[221] JAMES G. MCADAMS, III, FED. LAW ENF'T TRAINING CTRS., FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA): AN OVERVIEW, https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf (last visited Jan. 4, 2016).

[222] 50 U.S.C. § 1804(a)(7).

[223] This is a significant problem because the standard for probable cause in the FISC is a lower standard than the standard for Title 18 Courts. United States v. Rosen, 447 F. Supp. 2d 538, 549 (E.D. Va. 2006) (citing *In re* Sealed Case, 310 F. 3d 717, 738 (FISA Ct. Rev. 2002)).

[224] *See In re* Application of the F.B.I., Investigation for an Order Requiring the Prod. of Tangible Things from [redacted], No. BR 13-158, 5 (FISA Ct. Oct. 11, 2013); *see also* Smith v. Maryland, 442 U.S. 735 (1979).

[225] *Rosen*, 447 F. Supp. 2d at 549 (citing *In re* Sealed Case, 310 F. 3d at 738).

[226] *Id.*

Ultimately then, the solution to the national security exception's pitfalls is two-fold. First and foremost, executive agencies must respect and follow the procedures of domestic surveillance outlined in FISA as amended by the USA PATRIOT Act. Additionally, the carte blanche national security exception must be considered a relic of a by-gone era. The exception, allowed to cover so much with so little oversight, must be seen as what it is: a step back to an age where kings would order their agents to seek out by any means necessary those publishing seditious posters.[227] If the national security exception applies only when surveillance is taking place outside the United States, or the electronic communication's end point is outside the United States, then the President is acting to a greater extent under his Article 2 powers, and we are minimizing the risk of violating the due process rights of American citizens. The FISC must also return to an understanding that probable cause is probable cause, and while the definition may be hard to nail down, it is the same definition in criminal law as it is in national security law.

D. Why then are the NSA's bulk data programs unconstitutional?

1. Metadata Program

A user of a mobile device has a reasonable expectation of privacy in the metadata.[228] Under *Katz*, a reasonable expectation of privacy is not just a subjective expectation of privacy, but also one that society at large would grant.[229] Both the FISC and the Title 18 courts continue to cite to *Smith* in holding that there is no privacy interest in phone records because of the third party exception.[230] This holding ignores the fact that this exception was crafted well before the advent of the modern cellphone, the internet, and the changes that these inventions have brought upon society. This is important because, in the era of the internet, the line between content and metadata is becoming blurred. For instance, internet service providers record all internet protocol (IP) addresses that you access.[231] The IP address is technically metadata; however, because the IP address takes a user directly to the requested website, the content that the user requested is immediately viewable to anyone who has obtained the IP address.[232] This is an analogous situation to *Katz*.[233]

Metadata for cellphones, in addition to the outgoing numbers, incoming num-

---

[227] *See* LASSON, *supra* note 29, at 31.

[228] See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[229] *Id.*

[230] *See* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE (2014), https://www.fas.org/sgp/crs/misc/R43586.pdf; *see also* Smith v. Maryland, 442 U.S. 735 (1979).

[231] *See* Lincoln Spector, *Is Your ISP Spying on You?*, PCWORLD (Sept. 3, 2012, 7:42 AM), http://www.pcworld.com/article/261752/is_your_isp_spying_on_you_.html.

[232] *See* Marshall Brain, *How Web Servers Work*, HOWSTUFFWORKS.COM, http://computer.howstuffworks.com/web-server5.htm (last visited Jan. 13, 2016).

[233] *See generally Katz*, 389 U.S. 347.

bers, length of the call, and time off the call, also frequently includes location information based on where the call was made.[234] Because of this location data, the government can effectively track every person who has a cellphone.[235] This, along with the information relating to calls, could allow the government to develop true pattern of life intelligence, which would otherwise be unavailable.[236]

The above changes in the type of information available with metadata have garnered some attention from many in the political class.[237] The judicial branch has also taken notice. In *U.S. v. Jones*, the Court examined whether the police tracking of a suspect by placing a GPS tracker on the target vehicle required a warrant.[238] In *Jones*, the FBI obtained a warrant to secure a GPS tracker to the undercarriage of the petitioner's vehicle.[239] The day after the warrant expired, the FBI finally affixed the tracker to the petitioner's vehicle and tracked his movements for four weeks.[240] Based in part on the tracker's location data, the government secured criminal indictments against the petitioner.[241] The trial court denied the motion to suppress the GPS data, except during the period when the petitioner was parked in the garage adjoining the petitioner's residence, finding that a person traveling in an automobile on public streets has no reasonable expectation of privacy in his movements.[242]

The Supreme Court held that the installation of a GPS device on the petitioner's vehicle and using the device to track the vehicle's movements was a search.[243] In justifying its opinion, the Supreme Court noted that the *Katz* analysis of whether there is a reasonable expectation of privacy is not the core of Fourth Amendment analysis, but merely an augmentation to the traditional interpretation of the Fourth

---

[234] *See* Michael B. Kelley, *Astonishing Graphic Shows What You Can Learn from 6 Months of Someone's Phone Metadata*, BUS. INSIDER (July 2, 2013, 11:30 AM), http://www.businessinsider.com/what-you-can-learn-from-phone-metadata-2013-7.

[235] *Id.*

[236] Pattern of life intelligence, or analytics, refers to "a computerized data collection and analysis method used to establish a subject's past behavior, determine its current behavior, and predict its future behavior." Lisa Brownlee, *The $11 Trillion Internet of Things, Big Data and Pattern of Life (POL) Analytics*, FORBES (July 10, 2015, 2:01 PM), https://www.forbes.com/sites/lisabrownlee/2015/07/10/the-11-trillion-internet-of-things-big-data-and-pattern-of-life-pol-analytics/#722f24374eb8.

[237] *See* Scott Shackford, *Sen. Rand Paul Continues Beating the Drum About the Privacy of Our Metadata*, REASON.COM (June 4, 2015, 11:25 AM), https://reason.com/blog/2015/06/04/sen-rand-paul-continues-beating-the-drum; *see also* Matthew Boyle, *Ted Cruz Crushes Marco Rubio in South Carolina over National Security, Bulk Metadata Collection*, BREITBART (Dec. 7, 2015), http://www.breitbart.com/big-government/2015/12/07/ted-cruz-crushes-marco-rubio-in-south-carolina-over-national-security-bulk-metadata-collection/.

[238] United States v. Jones, 565 U.S. 400, 402 (2012).

[239] *Id.*

[240] *Id.*

[241] *Id.*

[242] *Id.* (internal citation omitted) (citing United States v. Jones, 451 F. Supp. 2d 71, 73 (D.D.C. 2006)).

[243] *Id.* at 404.

Amendment.[244] This traditional view requires that the Court "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted"[245] and is based on the concern for government trespass on the areas enumerated in the amendment.[246] The Court reasoned that because there was no valid warrant for the FBI to affix the GPS tracker, there was no legal justification for the government trespass on the petitioner's vehicle.[247] In her concurrence, Justice Sotomayor stated that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[248] She further states that such an approach is problematic in the modern digital age because "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[249]

The essence of Justice Sotomayor's concurrence is best articulated by the principle "[p]rivacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[250] Justice Sotomayor was correct to call for the third party exception doctrine to be reviewed and overturned. When digital metadata is viewed in light of the majority's opinion in *Jones*,[251] application of the third party exception yields a preposterous result. Consider, for instance, cellular phone metadata. Cellphone metadata contains GPS data, as well as time and duration of calls.[252] Therefore, without a warrant and merely by tracking a cellphone, police can gain the same information (and more) from cellphone metadata as they could by affixing a GPS tracker to a vehicle, as in *Jones*.[253]

The metadata situation for internet traffic is perhaps even more disturbing. As mentioned previously, the IP address of a website is tantamount to the content of the website.[254] The webpages and cloud services for data storage, which are increasingly popular, are all tethered to some IP address.[255] With this metadata so readily available to the government without a warrant, it is effectively the same as allowing the government to walk into an office and rummage for seditious papers

---

[244] *Id.* at 407.

[245] *Id.* (internal quotations omitted) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

[246] *Id.*

[247] *Id.* at 404–05.

[248] *Id.* at 417 (Sotomayor, J., concurring).

[249] *Id.*

[250] *Id.* at 418 (quoting Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting)).

[251] *See generally id.*

[252] Greenwald & MacAskill, *supra* note 11.

[253] *See Jones*, 565 U.S. at 402.

[254] Brain, *supra* note 232.

[255] *See generally What is the Cloud?*, http://whatismyipaddress.com/the-cloud (last visited Mar. 19, 2017).

during the Founding Era.[256] If, as Justice Scalia stated in *Jones*, the purpose of the Court is to ensure "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted,"[257] then we must accept that privacy is not necessarily forfeited when we share our information with another party—that "privacy is not a discrete commodity."[258] As the third party exception is an antiquated notion, the NSA metadata programs—whether authorized by executive fiat or not—are unconstitutional.

E. PRISM and Midstream Collection

The PRISM and Midstream data programs were created to circumvent the requirement for a warrant.[259] The Midstream data collection program's parallel to *Katz* is evident from the start. In *Katz*, the government placed the listening device outside the phone booth to intercept and obtain the content of the phone call.[260] Likewise, with the Midstream data collection program, the government is pulling the content of the internet "conversation" while outside the home/device.[261] The phone booth and the operation of internet-accessing technology are analogous, as well. Both users have a general expectation of privacy: a smart phone user does not expect someone to be looking over his or her shoulder, just as a person in a phone booth assumes that the content of his or her conversation will not be overheard.

For PRISM, it is best to return to Justice Scalia's majority opinion in *Jones*, in which he stated that the court's role is the "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[262] Since the data that the government is seizing from company servers is data that users—individual citizens—are storing there, the servers are equivalent to file cabinets.[263] The Fourth Amendment, as was discussed above ad nauseam, was designed to protect citizens from precisely these kinds of intrusions.[264] Therefore, the PRISM program is again patently unconstitutional.

IV. CONCLUSION

This paper explored the history of the Fourth Amendment to gain a deeper understanding of the context in which it was written.[265] This context demonstrates the

---

[256] *See* LASSON, *supra* note 29, at 31.

[257] *Jones*, 565 U.S. at 405 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

[258] *Id.* at 418 (quoting Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting)).

[259] *See* Gellman & Poitras, *supra* note 11; Greenwald & MacAskill, *supra* note 11.

[260] Katz v. United States, 389 U.S. 347, 348 (1967).

[261] *See* Gellman & Poitras, *supra* note 11; Greenwald & MacAskill, *supra* note 11.

[262] *Jones*, 565 U.S. at 947 (quoting *Kyllo*, 533 U.S. at 34).

[263] Gellman & Poitras, *supra* note 11; Greenwald & MacAskill, *supra* note 11.

[264] *See supra* Part II.B.

[265] *See supra* Part II.B.

evil against which it was designed to protect.[266] Armed with that knowledge, this paper explored the NSA bulk data collection programs of PRISM, Midstream data collection, and metadata collection.[267]

PRISM and Midstream collection were found to be strongly analogous to the writs of assistance that gave birth to both the American Revolution and the Fourth Amendment to the United States Constitution.[268] PRISM and Midstream were shown to be unconstitutional even under a modern analysis, following closely the language of the *Jones* decision.[269] *Jones* refocused the Court's jurisprudence on ensuring that citizens' privacy remains at least where it was when the Fourth Amendment was drafted, thereby protecting citizens from either direct or constructive trespass from government agents without a warrant.[270]

Most crucially, this paper argued that the national security exception to the Fourth Amendment grants excessively wide-sweeping powers to the executive and, therefore, should be narrowed in scope to ensure full protection of civil liberties.[271] Tying into that idea is the need to abolish the antiquated third party exception.[272] The third party exception allows for the government to utilize citizens' own technology to track and monitor them, which would be unconstitutional if the government took action directly.[273] The most obvious instance is using a cellphone as a GPS tracker, which is comparable to the warrantless placement of a GPS tracker that was deemed a Fourth Amendment search in *Jones*.[274]

As evidenced by the metadata programs explored above, the NSA's bulk data collection programs are unconstitutional because they violate the Fourth Amendment to the United States Constitution. The Fourth Amendment was designed to protect citizens' privacy from unreasonable governmental interference without a warrant, and the NSA programs undermine the principles of the Amendment.

---

[266] *See supra* Part II.B.
[267] *See supra* Part II.C.
[268] *See supra* Part II.C.
[269] *See supra* Part III.B.; *see also* United States v. Jones, 565 U.S. 400 (2012).
[270] *See Jones*, 565 U.S. 400.
[271] *See supra* Part III.B.
[272] *See supra* Part III.B.
[273] *See supra* Part III.B.
[274] *See supra* Part III.B; *see also Jones*, 565 U.S. 400.