THE RUTHERFORD INSTITUTE

Post Office Box 7482
Charlottesville, Virginia 22906-7482

JOHN W. WHITEHEAD
Founder and President

TELEPHONE 434 / 978 - 3888
FACSIMILE 434/ 978 – 1789
www.rutherford.org

The Founding Fathers and the Fourth Amendment's Historic Protections Against Government Surveillance: A Historic Analysis of the Fourth Amendment's Reasonable Expectations of Privacy Standards as It Relates to the NSA's Surveillance Activities

May 2014

A publication of The Rutherford Institute*

* Contributing writers: John W. Whitehead, Douglas McKusick, Adam Butschek

INTRODUCTION

In June 2013, the Guardian newspaper, utilizing documents disclosed by Edward Snowden, a former employee of a National Security Agency (NSA) contractor, reported that the FBI had obtained a ninety-day order from the Foreign Intelligence Surveillance Court (FISC) requiring Verizon Business to provide the NSA daily so-called telephone metadata on all their customers' communications, although none were suspected of a connection with international terrorism or other wrongdoing.[1] Later public revelations established that the order had been renewed thirty-six times since May 2006, and that companion FISC orders had been directed to all major telecommunications companies. This unprecedented intrusion into the activities that citizens heretofore considered private and personal is effected without any suspicion and without any limitation to information related to some known threat from a foreign actor considered dangerous to the United States.[2]

The telephony metadata collected as a result was retained for at least five years and stored in a database that was later queried or searched periodically in an effort to connect a telephone number that the NSA concluded was reasonably suspected of a connection to an international terrorist organization to other telephone numbers, and thus identify previously unknown terrorists or terrorist plots.[3] Because the NSA collected first and queried later, the NSA was collecting in bulk information on virtually every phone call made by American telephone users regardless of whether the calls or individuals had any connection to criminal activity or international terrorism.

While the FISC has uniformly upheld the constitutionality of the dragnet telephony metadata and search program of the NSA in non-adversary proceedings, Article III courts are divided at present. The United States Supreme Court has recently declared that the Fourth Amendment should be interpreted today to secure the same level of privacy protection as was reasonably expected of citizens when the Amendment was ratified in 1792. In making that assessment, law enforcement resources, investigative priorities, and technological and jurisdictional limitations on the government are all pertinent. As elaborated below, the historical interpretation of the Fourth Amendment's privacy guarantees suggests that the NSA's bulk collection of telephone metadata violates the Constitution.

I. Communications in 1792: A History of the United States Postal Service

While obviously telephones did not exist in 1792, an examination of the existing means of communications sheds light on the level of privacy the Founding Fathers expected in their communications. In an early Supreme Court decision addressing wiretapping,[4] both the majority and minority opinions explicitly compare telephone communications to letters sent via the post

[1] Greenwald, Glenn, NSA Collecting Phone Records of Millions of Verizon Customers Daily, GUARDIAN (June 5, 2013).
[2] John W. Whitehead, *A Government of Wolves: The Emerging American Police State* (New York: SelectBooks, 2013), pp. 120-22.
[3] Greenwald, n. 1.
[4] *Olmstead v. United States*, 277 U.S. 438 (1928).

office and the Court's prior decision in *Ex Parte Jackson*,[5] which held that federal government agents could not open mail without a warrant.[6] While the majority declined to give telephone communications the same protections as mail because their intangible nature required neither search nor seizure,[7] the minority argued this was a distinction without a difference.[8] What was important was the invasion of individual privacy. The emphasis on the individual's expectations rather than the nature of the item seizure is clearly maintained in the Court's later Fourth Amendment jurisprudence, and in particular Justices Sotomayor and Alito's recent concurrences in *United States v. Jones*.[9] Thus, a comparison of the information gained from modern telephone communications and that from postal communications in 1792 is pertinent not only on a similarity level but also as a comparison that has been repeatedly used by the Supreme Court itself in its Fourth Amendment jurisprudence.

Although some believe it is fast becoming obsolete in the era of email and instant messages, the Postal Service was the critical means of communication in 1792. From its origins, guiding principles, and operating procedures, it is clear the Founding Fathers were fiercely protective of the Postal Service and adamant that private communications be free from government intrusion. In conjunction with the limitations on police resources discussed above, the Founding Father's expectation of privacy in their communications strongly suggests that the NSA's telephone metadata collection program violates the Fourth Amendment's guarantees as they existed in 1792.

The founding of the United States Postal Service actually predates the Declaration of Independence. The British established a North American Postal Service in 1692 based upon the system then in use in Great Britain itself.[10] Throughout its history, British postmasters general reserved the right to inspect mail sent through the Service, with a particular eye towards identifying subversion. British "clerks of the road" had the right to inspect any piece of mail and to exclude anything they deemed outside of acceptable dissent.[11] British authorities viewed the postal system as a tool of political espionage, and prohibited private mail carriers in order to strengthen their surveillance capabilities.[12]

---

[5] 96 U.S. 727 (1877).
[6] 277 U.S. at 464, 475.
[7] *Id. a*t 464.
[8] *Id. a*t 475.
[9] 132 S. Ct. 949, 565 U.S. __ (2012), as discussed, *infra*, in text accompanying notes 183-190.
[10] U.S. POSTAL SERV., Publication 100 – The United States Postal Service – An American History 1775-2006 (Nov. 2012).
[11] John, Richard R., Spreading the News: The American Postal System from Franklin to Morse 41 (1998).
[12] Melius, Louis, The American Postal Service: History of the Postal Service from the Earliest Times 18 (1917).

After the Boston Riots, facing a groundswell in Revolutionary thought throughout the Colonies, the British authorities cracked down on potentially subversive literature and attempted to prevent the Colonies from communicating with each other.[13] At this time, most mail consisted of newspapers and correspondence between merchants, and it was the newspapers that most felt the British suppression efforts. In Philadelphia, an American printer named William Goddard found himself a focus of these efforts, with the local postmaster general refusing to deliver some editions, raising taxes on delivery to exorbitant levels, and refusing to deliver the mail and non-local newspapers that were the source of Goddard's newspaper content.[14] While Goddard attempted to use private delivery services, his newspapers folded in 1773.[15] When the First Continental Congress met in 1774, Goddard proposed the creation of a rival system to the British postal service, one that would be free of government surveillance and allow the Congress to communicate with the Colonies.[16] The Congress promptly did so, authorizing the creation of the Constitutional Post on July 26, 1775.[17] By the end of the year, the North American Postal Service was out of business.[18]

Befitting a system created to avoid British surveillance, the Founding Fathers were extremely proud of the privacy afforded users of the United States Postal Service. For many Americans, the government's guarantee of the sanctity of the mail was evidence of the nation's moral superiority over European ones.[19] While John Jay served as Minister to France, he complained to George Washington that every single letter he received bore the telltale signs of French inspection.[20] James Madison, Thomas Jefferson, and James Monroe routinely drafted dispatches in code in order to avoid the French "cabinet noir,"[21] and even newspaper editors published warnings to their readers that they could expect French authorities to inspect any correspondence sent to that nation.[22] The British were no better, maintaining their "secrets office" well into the 19th century, and with British judges issuing general warrants allowing the opening of letters from virtually anyone.[23] Well into the 19th century, the United States Post

---

[13] *Id.* at 17.
[14] Pope, Nancy A., Goddard's Petition to the Continental Congress, SMITHSONIAN NAT. POSTAL MUSEUM (May 1, 2006) http://arago.si.edu/index.asp?con=2&cmd=1&id=76935&img=1&pg=1.
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] John at 42.
[20] *Id.* at 44, citing Jay, John to Washington, George, Feb 3. 1788, in Jensen, Merrill, Documentary History vol. 16, p.19.
[21] *Id.*, citing Fowler, Dorothy, Unmailable: Congress and the Post Office 7 (1977).
[22] *Id.*, citing 68 Nile's Nat'l Register 364 (Aug. 10, 1845).
[23] *Id.* at 43, citing Ellis, Kenneth, The Post Office in the Eighteenth Century: A Study in Administrative History 139 (1987).

Office offered a level of privacy vastly beyond what could be expected in other countries. In 1833, James Buchanan wrote that while he served as the ambassador to Russia, he had "not received a single communication of any kind…which [had] not been violated."[24] Journalists warned their readers that Russian authorities would inspect their mail, and to use caution lest they "involve their friends in serious embarrassments."[25] German authorities were so reckless in handling mail during inspection that popular American magazines recommended their readers summarize a letter's contents on the cover in case the letter itself was mutilated beyond recognition.[26] Postal officers noted that it was a fundamental tenet of the American postal system that the freedom from government surveillance of one's writings was as "great a privilege as speech,"[27] while Francis Lieber noted that no other nation more respected the inviolability of letters as the United States.[28] Americans were so committed to the inviolability of the mail that some have argued that the Logan Act, prohibiting unauthorized negotiations with foreign nations, was enacted because the federal government could not scrutinize the actual communications and so banned them outright.[29]

The Founding Fathers zealously protected the privacy of post office customers. The Postal Service Act of 1792 established the crime of unauthorized opening of mail and proscribed a maximum fine of $300 and/or six months in jail.[30] The primary concern seems not to have been postmasters stealing valuables from the mail since the Act also established a separate crime of robbery of the mails, punishable by death.[31] When the Postal Service's organizational structure threatened the sanctity of the mail, it inspired a new form of distribution systems. Throughout the 1790s, the postal service grew astronomically.[32] Previously, each letter would pass through each post office between its place of origin and destination, with each postmaster sorting out the letters that needed to continue down the chain.[33] With the ever increasing numbers of post offices, the opportunity for a postmaster to access private correspondence without authorization also increased.[34] This led Joseph Habersham, Postmaster General under

---

[24] *Id.* at 44, citing Buchanan, James to Livingston, Edward, Feb. 22, 1833, in Moore, John Bassett, ed., 2 Works of James Buchanan 320 (1908).
[25] *Id.*, citing *The Post System*, 5 DEBOW'S REV. 155 (1848).
[26] *Id.*, citing 2 LITTELL'S LIVING AGE 28 (Aug. 9, 1844).
[27] *Id.* at 42, citing Holbrook, James, Ten Years among the Mail Bags: Or Notes from the Diary of a Special Agent of the Post-Office Department 6 (1855).
[28] *Id.*, citing Lieber, Francis, *Report of George Plitt*, 9 N.Y. REV. 78 (1841).
[29] *Id.* at 43.
[30] Sess. I, Ch. 7, § 14 (1792).
[31] Sess. I, Ch. 7, § 17 (1792).
[32] Summerfield, Arthur E., U.S. Mail: The Story of the United States Postal Service 38 (1960).
[33] John at 74-75.
[34] *Id.*

Washington and Adams, to create a hub-and-spoke sorting scheme in order to minimize these opportunities.[35]

The only post office employees allowed to open mail without a warrant are those in the dead letter office.[36] While this office had its informal roots in the postal system's 1770s beginnings, it was officially created by the Post Office Act of 1825.[37] The clerks of the dead letter office were permitted to open only undeliverable mail, which was routed to the office from across the country. The clerks were allowed to open and read the contents of these letters only to the extent needed to determine the intended destination and no more.[38] If it was not possible to determine the intended destination of the letter, the clerks removed any valuables from the letter, returning them to the sender, and then promptly burned the letter and the rest of its contents.[39] Beyond the time needed to perform these tasks, the Postal Service did not retain the letters.

If an individual were concerned that government agents might inspect his communications if sent through the postal system, he still had many other options for avoiding government surveillance. Unlike other countries, the United States had a longstanding resistance to banning private mail carriers.[40] In the aftermath of the American Revolution, numerous postal companies were founded by private individuals and the states themselves.[41] In the 1790s, stagecoach passengers carried more mail on some routes than did the post office.[42] In 1800, a massive expansion of the United States postal system led it to deliver approximately 1.9 million newspapers, yet this still represented only about 10% of the total number, with the rest carried privately.[43] The continued use of private mail carriers was in large part due to the high cost of the federal system. Samuel Osgood, the first Postmaster General of the United States, complained to President Washington about the large numbers of letters carried by stagecoaches and private companies, yet resolved to compete against them based on service and price rather than statutory prohibition.[44] At times, even postal clerks themselves used the less expensive private carriers.[45] Private mail carriers were not effectively banned until the Post Office Act of 1845 significantly raised penalties on such private expresses while also lowering postage rates

---

[35] *Id.*
[36] Bruns, James H., *Remembering the Dead*, 1 ENROUTE 3 (July-Sep. 1992), *available at* http://www.postalmuseum.si.edu/resources/6a2c_deadletters.html.
[37] John at 77-78.
[38] *Id.*
[39] *Id.*
[40] John at 48.
[41] *Id.* at 28.
[42] *Id.* at 48.
[43] *Id.* at 38, citing Dill, William A., Growth of Newspapers in the United States 11 (1928).
[44] Summerfeld at 35-36.
[45] John at 159, citing Campbell, Joseph M. to Campbell, Matthew M. (June 13, 1829).

(previously the penalties, established by the 1792 Act, were so light that they were virtually never enforced).[46]

II. A History of American Criminal Justice and Law Enforcement

The criminal justice system of Colonial America and the Founding Fathers differed dramatically from the system that exists today. Not only did virtually all investigative and technological tools, from fingerprints and DNA analysis to wireless communications, not exist, the very philosophy of law enforcement would come as a surprise to modern eyes. At the time of the Fourth Amendment's ratification, there were no purpose-built prisons, full-time prosecutors, or professional police forces at all.[47] Law enforcement personnel did not actively investigate or attempt to prevent crime, but rather only responded once a crime had occurred and the victim brought it to their attention.[48] While the records are fragmented and incomplete,[49] despite the comparative lack of resources and differing approaches to police work, Colonial law enforcement appears to have been successful at social control, with crime and conviction numbers similar to those in late-20th century.[50] While demographic changes in the 19th century produced crime rates and other social ills that prompted the creation of most of the modern criminal justice system, as noted above, Fourth Amendment analysis requires examination of the system as it existed prior to 1792.[51]

Prior to American independence, the American criminal justice system was mostly a carryover of British institutions. The British king appointed Colonial governors who in turn either appointed constables (towns) and sheriffs (counties) directly or appointed local justices of the peace who in turn appointed the constables and sheriffs.[52] Virtually all of these constables, sheriffs, and justices of the peace were prominent local citizens, and, whether to ensure a favorable reaction from the constituency or because the governor simply did not have the capacity to appoint every law enforcement officer, many less populated jurisdictions were responsible for their own constables, sheriffs, and justices of the peace, either electing them or establishing a rotation amongst the citizenry.[53] However, constables and sheriffs were more a feature of populated areas, with rural areas often left with no law enforcement presence at all

---

[46] Summerfeld at 56-57.
[47] Walker, Samuel, Popular Justice: A History of American Criminal Justice, 25 (2 ed., 1998).
[48] Lane, Roger, Urban Police and Crime in Nineteenth-Century America, 2 CRIME & JUSTICE 1, 4 (1980).
[49] *Id.*
[50] Walker at 68. *See also* Lane at 36 (studies suggest "U" pattern in crime rates from early 19th century to late 20th).
[51] Given the sparseness of the data, it is difficult if not impossible to speak of conditions solely in 1792. However, the conditions immediately prior, including the late Colonial era, would have necessarily formed the perspective of the ratifiers of the Fourth Amendment.
[52] Walker at 25-26.
[53] *Id.*

well into the 18th century.[54] Rural western South Carolina did not have a county sheriff until 1769.[55]

Regardless of how the constables, sheriffs, and justices of the peace came into office, several characteristics were generally applicable to all. First, very few had any sort of formal legal training.[56] Knowledge of the law, law enforcement techniques, or other applicable skills was simply not a prerequisite for the position. Rather, the position was based more on a sense of civic duty which all citizens were qualified to perform.[57] The positions were always of a fixed term, usually one or two years, with a new individual taking over the office at the end of the term.[58] In 18th century North Carolina, 71% of justices of the peace served less than two years in office.[59] As such, even for a particular individual there was very little ability to develop specialized experience or skills nor would this, even if acquired, be of much benefit to society once his term was over. Instead, in the Colonial era and extending into the early 19th century, one of the most popular forms of literature in America was legal manuals.[60] These attempted to codify the common law and provide basic legal reasoning as guidance in the performance of law enforcement duties, sometimes containing detailed histories of crimes and punishments alongside sample indictment forms.[61]

Once law enforcement personnel were chosen, they still faced significant limitations on their actual enforcement resources. In fact, at times they were actively incentivized away from crime control. Prior to the 19th century, there were no professional police departments in the United States.[62] Colonial constables and sheriffs were responsible not only for law enforcement but for all manner of government operations. A constable or sheriff would be expected, in addition to combating crime, to collect taxes, maintain roads, supervise elections, and generally act as an all purpose government administrator.[63] In addition, since these constables and sheriffs were not professionals and were only serving set terms, they would still attend to their own private farms and businesses while serving as constable or sheriff.[64] Very little of a constable or sheriff's time might actually be taken up by law enforcement, a tendency that was only elevated

---

[54] Walker at 26.
[55] *Id.*
[56] Block, Sharon, Rape & Sexual Power in Early America 127 (2006).
[57] Walker at 25, 27.
[58] Uchida, Craig D., The Development of the American Police: An Historical Overview 4-5 (Dec. 2004).
[59] Greenberg, Douglas, Crime, Law Enforcement, and Social Control in Colonial America, 26 American Journal of Legal History 293, 312 (Oct. 1982).
[60] Bryson, William Hamilton, Private Law Libraries Before 1776, 239 VIRGINIA LAW BOOKS 484 (2000).
[61] Block at 127.
[62] Walker at 17.
[63] Walker at 25.
[64] Walker at 26.

by their compensation structure. Prior to the professionalization of police forces in the 19th century, constables and sheriffs were not paid a fixed salary.[65] Instead, they were compensated based on the specific tasks they performed, such as a percentage of tax revenue collected or a fixed fee for each subpoena served.[66] The result of such compensation structures was that most constables and sheriffs found it more profitable to perform virtually any other task besides those related to criminal prosecutions.[67] In the Colonial era, in every single jurisdiction civil litigation was far more common than criminal.[68]

Finally, law enforcement in Colonial America operated with a very different perspective on the nature of police work compared to the modern day. Prior to the mid-19th century, police work was strictly "reactive" in nature.[69] Law enforcement personnel did not try to prevent crimes or actively investigate potential criminals. Instead, virtually all criminal prosecutions started with a victim bringing the crime to the attention of the police.[70] A private individual who was the victim of a crime would go to the local justice of the peace and file an official complaint.[71] The justice of the peace would then certify the alleged offense and order the constable or sheriff to arrest the alleged offender.[72] Law enforcement was reactive in that if a victim did not come forward, the police did not investigate the crime and the courts did not prosecute the offender.[73] While a constable may be expected to arrest individuals in those cases where he actually witnessed a crime,[74] it appears that the only situation where police officers actively looked for crimes was in the enforcement of health and building codes.[75]

Although proposals to do so began in the 1750s, politicians and the public resisted establishing professional police forces in part because of concerns that they were too similar to an army and gave the government tyrannical control over the citizenry.[76] Philadelphia created America's first professional police only in 1845 (with other major cities following in the decade after).[77] Even then, the police force was still generally reactive in nature and responsible for many administrative duties not associated with police work. Well into the 19th century, police

---

[65] *Id.*
[66] Uchida at 5.
[67] *Id.*
[68] Greenberg at 323.
[69] Uchida at 5.
[70] Walker at 29.
[71] *Id.*
[72] *Id.*
[73] Uchida at 5.
[74] Friedman, Lawrence M., Crime and Punishment in American History 68 (1993)
[75] Uchida at 5-6.
[76] *Id.* at 7. *See also* Lane at 6.
[77] Friedman at 69.

were responsible for supervising elections, operating ambulances, and even lodging the homeless in local jails.[78] Large areas of cities were not patrolled at all[79] and most criminals were still tracked down by private investigators hired by the victims.[80] Specialized detective divisions charged with actively investigating crimes through such methods as undercover work were created in Boston in 1846, New York City in 1857, and Chicago in 1861.[81] Once an alleged offender was brought to trial, there was no prosecutor representing the "people."[82] Instead, the victim themselves would present the case to the court.[83] Private prosecutions in this manner occurred well into the late 19th century.[84]

In addition to constables, sheriffs, and justices of the peace, there was one more component of Colonial era law enforcement. Most locales instituted some form of a "watch." These were a similar outgrowth from the civic duty justification for rotating constables, sheriffs, and justices of the peace. All able-bodied male citizens could be expected to take a turn guarding the town from civil disturbances such as riots, fires, or, in the case of the South, slave rebellions.[85] However, once a disturbance arose the watchman was not tasked with stopping it on his own, but rather was responsible for raising a "hue and cry," alerting other citizens to the danger and allowing for a group response.[86] For example, a 1787 New York law prescribed that should a serious crime occur, a hue and a cry was to go up in the area where the crime occurred, whereupon all the men in the area were to give chase to the criminal.[87] All men were required to be armed and ready to respond should the hue and the cry go up.[88] In essence, a watchman acted more as a sentry than a law enforcement officer. He did not engage in the duties of a constable but rather was responsible for alerting the constable when the need arose.

Supposing that law enforcement personnel did actively investigate crime, the number of crimes and their relative frequency is also relevant to the reasonable expectation of privacy test. As noted by one concurrence in the Supreme Court's *Jones* case,[89] only the most important investigations would be deemed worthy of expending vast amounts of police resources, with minor transgressions perhaps receiving little to no investigative attention (for example, modern

---

[78] Walker at 60.
[79] *Id.* at 59.
[80] *Id.* at 59.
[81] Friedman at 204.
[82] Walker at 29.
[83] *Id.*
[84] Walker at 71.
[85] Walker at 27.
[86] Friedman at 64-65.
[87] *Id.*
[88] *Id.*
[89] *Jones*, 132 S. Ct. at 963-64 (Alito, J., concurring).

police generally only issue traffic citation for observed offenses, not those discovered after a months-long investigation). Because the federal government and virtually all the states had yet to codify the English common law which served as the basis for criminal prosecutions, the exact number of possible criminal offenses in 1792 is impossible to calculate.[90] While the Supreme Court in 1812 held that there were no federal common law crimes,[91] in 1821 Maine convicted a defendant for the state common law crime of improper disposal of a body.[92] As late as 1881, Pennsylvania had to rely on the common law in order to convict several individuals of ballot stuffing.[93] However, the efforts to codify the common law do shed some light on the scope of the criminal code. For example, when Congress passed the Crimes Act of 1790, one of the first efforts to define federal crimes, it established only seventeen crimes.[94] In 1982, the Department of Justice attempted to identify the then-number of federal crimes. Ultimately, it failed to calculate the exact number but estimated that it exceeded 3,000.[95] While this stands as the most recent effort to comprehensively identify the number of federal crimes, an informal 1998 American Bar Association study concluded that it was highly likely that the number was by then much higher.[96] When the House Judiciary Committee asked the Congressional Research Service to provide a calculation of the number of criminal offenses in 2013, the CRS responded that they lacked the manpower and resources to accomplish the task.[97] The Committee Chairman estimated that the current number of federal crimes exceeds 4,500.[98]

III. Historical Basis for the Fourth Amendment

It is well-established that the Fourth Amendment's guarantees to privacy and security were born of the American colonists experience with general warrants known as writs of assistance. Under these general warrants, the British Crown's officials were given blanket authority to conduct general searches in order to discover if any goods had been imported into the Colonies in violation of the tax laws.[99] They "allowed the king to break into the homes of any number of citizens in search of suspicious information without particularized suspicion and

---

[90] Block at 147.
[91] United States v. Hudson and Goodwin, 11 U.S. 32 (1812).
[92] Friedman at 64, citing Kanavan's Case, 1 Greenleaf (Me.) 226 (1821).
[93] Friedman at 64, citing Commonwealth v. McHale, 97 Pa. St. 407 (1881).
[94] Crimes Act of 1790, ch. 9, 1 Stat. 112.
[95] Fields, Gary and Emshwiller, John R., Many Failed Efforts to Count Nation's Federal Criminal Laws, WALL ST. J. (July 23, 2011).
[96] *Id.*
[97] Ruger, Todd, Way Too Many Criminal Laws, Lawyers Tell Congress, Blog of the Legal Times (June 14, 2013).
[98] *Id.*
[99] *Berger v. State of New York*, 388 U.S. 41, 58 (1967).

without limitation on its use."[100] Writs of assistance not only authorized these invasions of privacy, but allowed British agents to enlist the assistance of other government officials and private citizens to assist with the searches and seizures. These writs were nothing less than open-ended royal documents which British soldiers used as a justification for barging into the homes of colonists and rifling through their belongings.

James Otis, a renowned colonial attorney, "condemned writs of assistance because they were perpetual, universal (addressed to every officer and subject in the realm), and allowed anyone to conduct a search in violation of the essential principle of English liberty that a peaceable man's house is his castle." Otis also called the practice of issuing and executing general warrants "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law-book."[101]

Indeed, it was the indignities inflicted by the use of general warrants and writs of assistance by the British that sparked the colonists to revolt and assert their independence. In 1761, Otis represented a group of Boston merchants in opposition to writs of assistance in a lawsuit used as a soap box for decrying the practice of general searches and to inspire resistance. Known as Paxton's Case, John Adams described Otis's denouncements of the use of writs of assistance as "then and there was the first scene of the first act of the opposition to the arbitrary claims of Great Britain. Then and there the child of independence was born."[102]

Colonial Americans also were influenced by the controversy involving general warrants which was raging in England at about the same time as Otis was fighting against writs of assistance. In an effort to suppress "libelous" publications that opposed the government and to apprehend the authors of these publications, the English Secretary of State resorted to the issuance of general warrants to ransack unnamed places in an effort to determine and find those critical of the government.[103] In a series of cases, the English judiciary found in favor of those injured by the intrusions under general warrants, asserting that reliance upon the legality of general warrants is an attempt "to destroy the liberty of the kingdom[.]"[104]

The most famous of these cases, *Entick v. Carrington*[105] and *Wilkes v. Wood*,[106] are cited by the U.S. Supreme Court as "the wellspring of rights now protected by the Fourth

---

[100] Jeffrey Rosen, *The Naked Crowd: Balancing Privacy and Security in an Age of Terror*, 46 Ariz. L. Rev. 607, 611 (Winter 2004).
[101] *Stanford v. State of Texas*, 379 U.S. 476, 481 (1965).
[102] *Boyd v. United States*, 116 U.S. 616, 625 (1886).
[103] Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 Va. L. Rev. 869, 876-77 (1985).
[104] *Id.* at 879 (quoting *Huckle v. Money*, 19 How. Str. Tr. 1404, 95 Eng Rep. 768, 769 (C.P. 1763)).
[105] 19 How. St. Tr. 1029, 95 Eng. Rep. 807 (C.P. 1765).

Amendment."[107] In *Wilkes*, a trespass action arising from the execution of a general warrant was upheld, and the presiding justice commented as follows on the crown's position in the case:

> The defendants claim a right, under precedents, to force persons houses, break open escrutores, seize their paper &c. upon a general warrant, where no inventory is made of the things thus taken away, and where no offenders names are specified in the warrant, and therefore a discretionary power given to messengers to search wherever their suspicions may chance to fall. If such a power is truly invested in a Secretary of State, and he can delegate this power, it certainly may affect the person and property of every man in his kingdom, and is totally subversive of the liberty of the subject.[108]

Entick similarly upheld a claim for trespass liability arising from the execution of a warrant allowing the wholesale examination and seizure, in the discretion of the officer, of Entick's books and papers in search of evidence that Entick was the author of libelous matters. Rejecting the defendants' attempts to justify the search and seizure, Lord Camden wrote "if this point should be determined in favor of the jurisdiction, the secret cabinets and bureaus of every subject in this kingdom will be thrown open to the search and inspection of a messenger, whenever the secretary of state shall think fit to charge, or even to suspect, a person to be the author, printer, or publisher of a seditious libel."[109]

Out of this experience, the Fourth Amendment was adopted as a fundamental bulwark against government invasion of the privacy of citizens. The provisions of the Fourth Amendment "are precise and clear they reflect the determination of those who wrote the Bill of Rights that the people of this new Nations should forever "be secure in their persons, houses, papers, and effects from intrusion and seizure by officers acting under the unbridled authority of a general warrant."[110] The commitment to prevent any resurrection of general warrants has been repeatedly restated in court decisions applying the constitution's ban on unreasonable searches and seizures; to this day it informs the judicial conception of the protection of privacy afforded to persons by the Constitution.[111]

---

[106] 98 Eng. Rep. 489 (CP 1763).
[107] *Stanford*, 379 U.S. at 483.
[108] *Wilkes*, 98 Eng. Rep. at 498.
[109] *Entick*, 19 How. St. Tr. at 1063.
[110] *Stanford*, 379 U.S. at 481.
[111] *See Steagald v. United States*, 451 U.S. 204, 220 (1982) (the Fourth Amendment's roots in the outlawing of general warrants requires a ruling that a warrant to arrest an individual does not authorize the search of a third-party's residence) and *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 325 (1979) (warrant allowing executing officers to seize "obscene materials" was tantamount to a general warrant and violated the Fourth Amendment).

IV. Background and Legal Basis for the NSA's Collection of Telephone Metadata

While many details regarding the NSA's activities remain classified, the agency has acknowledged some of the basic facts surrounding its metadata collection operations and provided its interpretation of the statutes authorizing them. While in individual cases NSA employees may exceed the agency's own rules and thus infringe upon the constitutional rights of the individuals involved, the NSA asserts that the program is generally constitutional under its interpretation of Supreme Court precedents. Given the limitations on warrantless searches and seizures set by the Fourth Amendment (discussed below), the specifics of the telephone metadata program are critical in determining whether or not the NSA's interpretation is incorrect and the bulk collection of telephone metadata violates the Constitution.

As set forth in Executive Order 12333, the NSA's mission is to collect information that constitutes "foreign intelligence or counterintelligence" but without "acquiring information concerning the domestic activities of United States persons."[112] Thus, the NSA has authority to operate within the United States and in regards to United States citizens so long as the activities at issue have a foreign connection. As with all agencies of the federal government, the NSA's activities with respect to United States citizens and persons within the United States are restricted by the United States Constitution. In effort to ensure compliance with constitutional safeguards, the NSA's domestic surveillance activities are governed by the Foreign Intelligence Surveillance Act of 1978 (FISA).[113]

FISA sets forth procedural and substantive rules governing specific NSA intelligence gathering techniques. The NSA has asserted that its telephone metadata collection program operates pursuant to Section 501 of FISA, which governs "access to certain business records for foreign intelligence and international terrorism investigations."[114] This section was amended by Section 215 of the USA PATRIOT Act of 2001, and it now allows the NSA, upon application to a special FISA court, to obtain "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities."[115] Importantly, a FISA court order is not the same as a warrant, which can only be issued by upon a showing of probable cause that evidence of a crime will be found in the places to be searched. Rather, a FISA court must only find that there are reasonable grounds "to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States

---

[112] Exec. Order No. 12,333, 3C.F.R. (1981 Comp.)
[113] 50 U.S.C. § 1801 *et seq*.
[114] National Security Agency Section 215 of PATRIOT Act Fact Sheet, *available at* http://www.scribd.com/doc/149791922/National-Security-Agency-Section-702-of-FISA-and-Section-215-of-PATRIOT-Act-Fact-Sheets.
[115] 50 U.S.C. § 1861.

person or to protect against international terrorism or clandestine intelligence activities."[116] The NSA has argued that telephone metadata is a tangible "thing" within the meaning of Section 501, and its telephone metadata collection program (having been authorized pursuant to the procedures set forth in FISA) is thus authorized by statute.

However, the Privacy and Civil Liberties Oversight Board (PCLOB), an executive agency established to ensure executive branch counterterrorism efforts appropriately protect privacy and civil liberties, has rejected the NSA's position. In its report on the NSA program, it concluded that the bulk collection of metadata is not authorized by Section 215 of the USA PATRIOT Act.[117] First, the PCLOB report noted that Section 215 is designed to enable the Federal Bureau of Investigation to acquire relevant business records as part of an FBI investigation.[118] Because the NSA's bulk collection has no connection to any specific FBI investigation at the time of collection, it does not satisfy Section 215's requirements.[119] Additionally, because the metadata is collected in bulk, it cannot be regarded as relevant to an investigation unless the meaning of "relevant" is expanded beyond any reasonable interpretation.[120] Third, the metadata records are collected in real-time and so cannot be considered the already existing business records to which Section 215 was meant to apply (FISC orders require future records to be turned over, not ones already existing).[121] Finally, the PCLOB report noted that Section 215 authorized only the FBI to collect records, not the NSA.[122]

Assuming that the NSA's telephone metadata program is properly authorized by FISA, as noted above, it would still need to operate within the limitations imposed by the United States Constitution. Since the metadata program collects this information in bulk, it necessarily gathers information from United States citizens with no connection to foreign intelligence or international terrorism. The PCLOB report noted that the vast majority of the telephone calls the NSA collects metadata from are strictly domestic, with both participants located in the United States.[123] Additionally, because the program is authorized only by a Foreign Intelligence Surveillance Court (FISC) order, the collection of this metadata is not done pursuant to a warrant. Thus, without proper limitations, the NSA's program may violate the

---

[116] 50 U.S.C. § 1862(b)(2)(A).
[117] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 10 (Jan. 23, 2014) [hereinafter "PCLOB Report"].
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] *Id.* at 22.

constitutional rights of those individuals with no foreign connection, specifically their right under the Fourth Amendment to be free from unreasonable searches and seizures.

The NSA asserts that several key facts and limitations on its program ensure that it is compatible with Americans' Fourth Amendment rights. First, the NSA notes that its Section 215 program only collects metadata, not actual conversations.[124] This means that while the NSA does collect information such as the telephone numbers involved in the call, the duration of the call, the time of day when the call was made, and some information on the caller's location, it does not collect the actual conversations themselves. The NSA does not obtain the metadata information directly from individuals, but rather from telecommunications companies.[125] Metadata, in addition to apparently having some intelligence gathering utility, is a functional requirement of the telephone system itself. Telecommunications firms obtain this information from their customers simply as a result of operating a telephone system. While it does not claim to be under an obligation to do so, the NSA limits the time it stores the metadata to a maximum of five years, whereupon it is destroyed unless previously connected to a phone number reasonably suspected of use by a listed international terrorist organization.[126] Presumably, this five year period vastly exceeds the typical storage period of telecommunications firms since the Federal Communications Commission currently requires telecommunications firms to store telephone metadata for a minimum of only eighteen months.[127] The NSA now collects this data at least partially in "real-time," negating the need to rely on the firms for storage.[128] Additionally, if a metadata record turns up as a "hit" in response to a query during the five year storage period (see below), those records are never destroyed.[129]

Once the NSA has obtained and stored telephone metadata, NSA analysts access the data through the usage of "queries" or searches for particular telephone numbers or other selection terms within the database.[130] Prior to any query, one of twenty-two designated NSA officials must certify that there is a "reasonable, articulable suspicion" that the telephone number is associated with terrorism.[131] The NSA officials' certifications are not reviewed by any court prior or subsequent to a query.[132] NSA analysts use the queries to develop "contact chaining" on the target: the database allows the analysts to see not only all telephone numbers that have

---

[124] National Security Agency Section 215 of PATRIOT Act Fact Sheet.
[125] *Id.*
[126] *Id.*
[127] PCLOB Report at 21.
[128] Greenwald, *supra* n. 1.
[129] PCLOB Report at 25.
[130] *Id.* at 8.
[131] *Id.* at 8-9.
[132] *Id.* at 54.

called the targeted telephone number but also all the telephone numbers that have called those numbers as well as all telephone numbers that have in turn called that number.[133] These are called "hops", with numbers contacting the targeted number called "first hops," the telephone numbers the first hop numbers contacted so-called "second hops," and the numbers those telephones contacted referred to as "third hops."[134] All numbers in contact are collected; there is no requirement for a reasonable, articulable suspicion beyond the target telephone number. As such, a single query can reveal the metadata information of voluminous numbers of individuals, particularly as the search extends to second and third hops, with the only requirement that the telephone numbers have been in some sort of contact (in other words, regardless of duration or other circumstances).

The NSA's Section 215 program has its roots in the aftermath of the September 11, 2001 terrorist attacks. The NSA began bulk collecting metadata in late 2001 based upon presidential authorizations issued every thirty to forty-five days pursuant to the USA PATRIOT Act (enacted in October 2001).[135] In May 2006, the federal government applied for and received authorization from the FISC to continue its bulk metadata collection program under Section 215 of the PATRIOT Act.[136] This FISC authorization has been continuously renewed every ninety days since then, or approximately thirty-six times since May 2006.[137] The NSA has given no indication that it ever plans to cease its Section 215 collection activities, so presumably the FISC reauthorizations will continue indefinitely. Because of the universal collection of metadata from all telephone users and the indefinite duration of the collection activities, the NSA's Section 215 program represents one of the largest collections of information in human history.

V. The Fourth Amendment's Protection Against Unreasonable Searches and Seizures

While it has been alleged that the NSA's Section 215 program violates other provisions in the Constitution and the law, the principal objection to the program is that it violates the Fourth Amendment rights of American telephone users.[138] As discussed, *supra*, the Fourth Amendment to the United States Constitution guarantees individuals the right to be secure from "unreasonable searches and seizures" of their persons, houses, papers, and effects.[139] The government is generally required to obtain a warrant based on probable cause prior to a search or

---

[133] *Id.* at 9.
[134] *Id.*
[135] *Id.*
[136] *Id.*
[137] *Id.* at 46.
[138] The PCLOB Report suggested that the program may violate the First Amendment's freedom of association guarantee as well as the provisions of the Electronic Communications Privacy Act (18 U.S.C. § 2703).
[139] U.S. CONST. amend. IV.

seizure, subject to a handful of exceptions. Importantly, a warrant is not required when the government's actions either do not consist of a search or seizure or if an individual, in a given context, does not have an expectation of being free from a government search or seizure. This latter requirement is an individual's "reasonable expectation of privacy" from government searches and seizures, and a warrantless search or seizure that infringes upon it is unconstitutional. Modern American jurisprudence often turns on exactly what is a reasonable expectation of privacy. Reflecting a common philosophical split, some courts argue that the expectation of privacy is fluid and dependent on what society currently understands as reasonable, while others argue that the Fourth Amendment protects the expectation of privacy as it existed when the Amendment was ratified, in this case 1792.

The NSA has asserted that the Section 215 program is permissible under current Fourth Amendment jurisprudence, in particular the Supreme Court's 1979 ruling in *Smith v. Maryland*.[140] In that case, the defendant was a suspect in an armed robbery who began harassing the victim with threatening and obscene telephone calls.[141] After police were able to obtain his address from his vehicle license plate number, they requested that the defendant's telephone company install a pen register at its central office.[142] This device recorded for the next two days the numbers dialed from the defendant's telephone.[143] Importantly, the device did not record actual conversations, incoming telephone calls, the duration of the calls, or even whether the caller had been able to reach the other party. The device was only installed at the telephone company's premises, and so involved no intrusion upon the defendant's property nor obtained any information beyond that which was sent to the telephone company in the course of the use of the defendant's telephone. The Court held that the defendant did not have a reasonable expectation of privacy in the telephone numbers he dialed and therefore the installation of the pen register did not constitute a search within the meaning of the Fourth Amendment.[144] The Court emphasized that all telephone users are aware that they must convey phone numbers to the telephone company in order to place a telephone call, and that indeed the telephone subscriber will see a list of their long-distance calls on their monthly bills.[145] Citing its previous holdings on third-party disclosures, the Court held that it was not reasonable for the defendant to expect the telephone company to maintain his privacy.[146] By voluntarily providing the telephone numbers he wished to call to the telephone company, he assumed the risk that the company

[140] 442 U.S. 735 (1979).
[141] *Id.* at 737.
[142] *Id.*
[143] *Id.*
[144] *Id.* 742.
[145] *Id.*
[146] *Id.* at 743-44.

might then disclose those numbers to the police, and thus could not have a reasonable expectation of privacy in his dialing habits.[147]

It is the *Smith* distinction between actual conversations and the information provided to a telephone company in order to connect a call that the NSA relies upon when declaring its bulk telephone metadata collection constitutional. Because the NSA restricts its program only to metadata and not the calls themselves, the collection of metadata from United States citizens unconnected to foreign intelligence does not constitute a search within the meaning of the Fourth Amendment according to the NSA.[148] However, the NSA's reliance on *Smith* is misplaced. *Smith* has been controversial since it was decided, and the Court's Fourth Amendment jurisprudence has evolved to include limitations on warrantless searches aided by technological advances. While none of these cases address the Section 215 program or the bulk collection of telephone metadata generally, they contain important caveats that call into question whether the Section 215 program is constitutional. The technological advances that allow the NSA's program to operate also serve to distinguish it from the police surveillance in *Smith*.

The Supreme Court has repeatedly emphasized that the Fourth Amendment protects people, not places.[149] What a person knowingly exposes to public view is not subject to Fourth Amendment protection even if he does so in a place normally thought of as "private" such as a home or office.[150] Likewise, although a person may be in an area accessible to the public, if he seeks to preserve his privacy, he may be afforded constitutional protection from a government search or seizure.[151] Although the Fourth Amendment was at one time held not to cover government actions that did not constitute a physical trespass upon the individual's property, the Supreme Court has since emphasized that the Fourth Amendment extends to intangible items such as telephone conversations.[152] As a result, regardless of the type of thing being protected, there is a two-part test: did the person exhibit an expectation of privacy and does society recognize that expectation as reasonable?[153] If the answer to either question is no, then the government's conduct does not constitute a search within the meaning of the Fourth Amendment and the Amendment's protections will not apply.

---

[147] *Id.* at 744.
[148] *See* Memorandum of Law in Support of Defendants' Motion to Dismiss, Paul v. Obama, No. 1:14-cv-0262-RJL 28 (D.C.D.C. May 2, 2014).
[149] *Katz v. United States*, 389 U.S. 347, 351 (1967).
[150] *Id.*
[151] *Id.*
[152] *Id.* at 352-53.
[153] *Id.* at 361 (Harlan, concurring).

Because the Fourth Amendment requires an individual to display a subjective intent to keep information private, an individual can waive his Fourth Amendment protections by disclosing the information to the public. The individual need not provide the information directly to the government. In fact, he very well might intend that the information not be provided to the government. However, once the information is exposed to public view, the individual will not be afforded Fourth Amendment protection if the government then becomes aware of it. For example, a criminal defendant might conspire with a government informant or reveal his criminal behavior to a friend or family member. While he may not intend that this information will end up in government hands, if the confidant relays the conversation to government authorities it will not constitute a search or seizure within the meaning of the Fourth Amendment.[154] By disclosing the information to other individuals, even if he entrusts them to maintain secrecy, the criminal defendant shows that he does not have an expectation of privacy in these matters. The Court has generally held that an individual does not have an expectation of privacy in information or items disclosed to any third parties.[155] Thus, a package sent through a private freight carrier may be turned over to police without the sender's knowledge[156] or a bank may turn over account and deposit information without notifying the account holder.[157] Perhaps most famously, an individual no longer manifests an expectation of privacy in their household waste once it is brought to the curb for trash collection since the individual voluntarily disclosed it to a third party, the trash collector.[158]

The waiver of Fourth Amendment protections when information is disclosed to third parties leads to critically different results in seemingly similar contexts. In *Katz*, the police obtained the defendant's telephone conversations by attaching an electronic listening and recording device to the outside of the public phone booth the defendant used in his criminal enterprise.[159] As noted above, the Court emphasized that the Fourth Amendment protected people, not places, and held that the defendant retained his Fourth Amendment rights. The nature of a phone booth created a physical separation between the defendant and the outside world, such that the defendant was entitled to presume that his conversations could and would not be overheard.[160] Thus, the defendant had not disclosed his communications to a third party, notwithstanding the fact that he used a public phone booth or even that the phone booth was partially made of glass (theoretically allowing someone to at least partially read his lips).[161]

---

[154] *Hoffa v. United States*, 385 U.S. 293, 302 (1966).
[155] *United States v. White*, 401 U.S. 745, 752 (1971).
[156] *United States v. Jacobsen*, 466 U.S. 109, 121 (1984)
[157] *United States v. Miller*, 425 U.S. 435, 443 (1976).
[158] *California v. Greenwood*, 486 U.S. 35, 41 (1988).
[159] *Katz* at 348.
[160] *Id.* at 352.
[161] *Id.*

As technology has improved, courts have struggled with determining when information has been disclosed to third parties. Technology that allows information to be gleaned in a manner beyond the capability of human senses has caused particular uncertainty regarding an individual's reasonable expectation of privacy. At times the Court has emphasized the nature and level of intrusion a given technology may present. For example, a "canine sniff" of a suspicious package has been held not to constitute an unreasonable search because it provides very limited information (the presence or absence of illegal contraband) without exposing the contents of the package to public view, despite the fact that no human could replicate the canine's abilities.[162] Although police generally may not search a home for the presence of illegal drugs without a warrant, the Court has held that installing an electronic "beeper" in a barrel of precursor chemicals and then tracking that barrel to the defendant's property did not violate the defendant's expectation of privacy as to the contents of his home.[163] The Court had previously held that when an automobile travels on public thoroughfares, the occupant has no reasonable expectation of privacy in his movements from one place to another.[164] The police may follow ("tail") the suspect's car in order to ascertain his movements and whereabouts without a warrant. Thus, the electronic beeper did not provide any information that might otherwise have been gained through constitutionally permissible visual surveillance.[165] The Fourth Amendment does not place an absolute prohibition on police augmenting their senses with technology.[166] However, in an important caveat, the Court noted that at the time it was technologically impossible for the government to conduct 24-hour surveillance of any and all citizens, and that should such "dragnet type" law enforcement practices occur, different constitutional principles may apply.[167]

Since the Court's 1983 decision in *United States v. Knotts*, several decisions have significantly limited its scope. In 1984, the Court held that a similar electronic tracking device did violate a person's reasonable expectation of privacy when it revealed information that could not have been obtained through visual surveillance.[168] The critical distinction between *Knotts* and *Karo* was that in the former case the electronic beeper was used only to verify that the barrel was brought to the defendant's property, where it remained in an open field (an area subject to less constitutional protection).[169] In *Karo*, the police used the electronic beeper to determine that

---

[162] *United States v. Place*, 462 U.S. 696, 707 (1983).
[163] *United States v. Knotts*, 460 U.S. 276, 282 (1983).
[164] *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974).
[165] *Knotts* at 281.
[166] *Id.* at 282.
[167] *Id.* at 283-84.
[168] *United States v. Karo*, 468 U.S. 705, 714 (1984).
[169] *Knotts* at 282.

a can of chloroform had been brought inside the defendant's home which, given the context of that case, was a fact that could not have been discovered via constitutionally acceptable visual surveillance.[170] Thus, technology can be used as a substitute for police surveillance but not to overcome constitutional limitations on that surveillance.

While the Court has never specifically repudiated its reasoning in *United States v. Place*, it appears that it is increasingly concerned with technology that allows police to observe information that, while technically exposed to the public, is not observable with ordinary human senses. In *Kyllo v. United States*, the Court had the opportunity to consider police use of a thermal imaging camera.[171] The police suspected that the defendant grew marijuana plants inside his home, an operation that necessitated high-intensity lamps which produce significant amounts of heat. The police, from a public street, observed the defendant's home with a thermal imaging device that revealed the defendant's garage was relatively hotter than both the rest of his home and the garages of his neighbors, evidence which was then used to obtain a search warrant for the house. While such heat signatures were easily observed from a public location, the Court held that the defendant had not publicly disclosed the information and that the use of the thermal imaging device violated his reasonable expectation of privacy.[172] Unlike typical visual surveillance that had been held constitutional in the past, the use of the thermal imaging device, particularly in respect to a private home (which is afforded a higher standard of privacy under the Fourth Amendment), allowed the police to obtain information that they otherwise would not have been able to obtain without physically entering the premises.[173] Technology could not be used to obtain information that would require, in its absence, an unconstitutional search, even if that information was technically exposed to the public.[174] While the Court noted that this analysis might change if the technology was in general public use, thus shifting the individual's subjective expectation of privacy, it noted that at a minimum the Fourth Amendment should preserve that degree of privacy against government intrusion that existed when the Amendment was adopted.[175] While technology might shift social expectations of privacy, the originalist understanding of the Fourth Amendment acts as a floor: this is the minimum expectation of privacy that exists and police technology must not be permitted to erode it, regardless of changing social expectations.[176]

---

[170] *Karo* at 715.
[171] 533 U.S. 27 (2001).
[172] *Id.* at 34.
[173] *Id.*
[174] *Id.*
[175] *Id.* at 34-35.
[176] *Id.* at 34.

Justice Scalia's opinion in *Kyllo* echoes Justice Brandeis's famous dissent in *Olmstead v. United States*.[177] That case also involved a police wiretap of the defendant's telephone and its holding that a wiretap did not constitute a search was expressly overruled by *Katz*.[178] Justice Brandeis acknowledged that the wiretapping might have physically taken place outside the home and therefore might not be considered the trespass necessary for finding a Fourth Amendment search under a strict reading of the Amendment.[179] However, he argued that was immaterial.[180] The Fourth Amendment protects individuals' right to privacy, regardless of the means used to intrude upon it.[181] Recognizing that technology would progress and allow the government to spy upon citizens with means more effective than wiretapping, he insisted that technological advances should not erode the protections of the Fourth Amendment.[182] The Fourth Amendment stood for a principle of personal privacy that should be given effect without "an unduly literal construction upon it" that might allow intrusions simply because the Founding Fathers had not anticipated the technological means by which they occurred.[183]

Since *Kyllo*, the Court has continued to stress that the standard for Fourth Amendment privacy protection must be construed in light of what was considered an unreasonable search and seizure when it was adopted. Most recently, the Court had the opportunity to revisit police conduct similar to that in *Karo* and *Knotts*. In *United States v. Jones*, the police installed a Global Positioning System tracker on the defendant's automobile in order to log his movements on public roads without requiring constant police visual surveillance.[184] Although there were two separate concurrences, the decision was unanimous and all the Justices used the reasonable expectation of privacy at the time of ratification as the standard in their analysis. While the majority opinion held that the installation of the GPS tracker constituted a trespass against the defendant's property (a return to pre-*Katz* jurisprudence), holding the Fourth Amendment's protections contingent upon common law property rights,[185] Justice Alito's concurring opinion (joined by Justices Ginsburg, Breyer, and Kagan) held that "long-term" GPS surveillance violated the defendant's reasonable expectation of privacy.[186] In both opinions, emphasis was again put on the protections the Fourth Amendment provided at the time of its ratification. In the majority's opinion, this meant that government officers could not trespass on private property

---

[177] 277 U.S. 438 (1928).
[178] *Katz*, 389 U.S. at 353.
[179] 277 U.S. at 479.
[180] *Id.*
[181] *Id.* at 478.
[182] *Id.* at 474.
[183] *Id.* at 476
[184] 132 S. Ct. 949, 565 U.S. __ (2012).
[185] *Id.* at 950.
[186] *Id.* at 964.

without a warrant, regardless of the insignificance or duration of the trespass.[187] However, Justice Alito's concurring opinion viewed the trespass itself as insufficient context for determining the defendant's Fourth Amendment rights.[188] Rather than focus on the trivial trespass the GPS tracker represented, it was the information it transmitted that was at issue.[189] A GPS unit allowed the police to record the defendant's movements 24 hours a day for months at a time without expending the vast amount of police resources that comparable visual surveillance would require. Because only the most important investigations would possibly justify such expenditure of police resources, the concurrence noted that historically the "greatest protections of privacy were neither constitutional nor statutory, but practical."[190] Society's expectation was that law enforcement would not, indeed could not, secretly monitor and catalogue every single movement of the defendant.[191] Thus, by doing so, the police violated the defendant's reasonable expectation of privacy in his movements.

The Court's decision in *Jones* was unanimous, but the concurring opinions and their differing legal rationales has led to some confusion regarding the actual holding of the case. While five Justices joined the majority opinion holding the government's conduct unconstitutional based upon the common law theory of trespass, Justice Sotomayor also drafted a separate concurring opinion. In her concurrence, Justice Sotomayor noted that she believed the government conduct was a violation of the Fourth Amendment under both the majority's trespass theory as well as Justice Alito's reasonable expectation of privacy test.[192] Thus, both rationales had support from a majority of Justices. However, this appears to have been overlooked by some. In March 2014, the FISC issued an opinion analyzing the NSA's collection activities in light of *Smith* and *Jones*.[193] In its opinion, the FISC argued that *Jones* provided no basis for departing from *Smith* because the controlling opinion relied solely on the trespass theory of the Fourth Amendment violation.[194] While noting Justice Sotomayor's concurrence and conceding that it suggested a majority of Justices may be ready to endorse a "new" Fourth Amendment standard, it denied that this had any impact on the *Smith* standard.[195] The FISC opinion argues that the Alito and Sotomayor concurrences actually present two separate and distinct analytical approaches towards the Fourth Amendment, and therefore neither one could be viewed as having majority support.[196] Furthermore, the FISC observed the near total lack of discussion of *Smith* in

---

[187] *Id.* at 950-51.
[188] *Id.* at 958.
[189] *Id.* at 961.
[190] *Id.* at 963-64.
[191] *Id.*
[192] *Id.* at 957.
[193] In re Application of the Federal Bureau of Investigation, No. BR 14-01 (FISA Ct. Mar. 20, 2014).
[194] *Id.*
[195] *Id.*
[196] *Id.*

the concurring opinions, and took this as evidence that *Jones* left the *Smith* standard completely undisturbed.[197] However, others have viewed the lack of *Smith* discussion in *Jones* as merely an exercise of judicial restraint to the facts of the specific case before the Court and argued that the *Jones* concurring opinions do present a Fourth Amendment analysis for courts to apply. In its January 2014 report, the PCLOB specifically stated that the "approach" set forth in the Alito and Sotomayor opinions (which were also similar to the Court of Appeals opinion in *Jones*) would suggest a distinction between the Section 215 program and the pen register in *Smith*.[198] The PCLOB report suggested that this might lead to the conclusion that the totality of the information collected by the Section 215 program renders it a violation of a reasonable expectation of privacy even if a more limited collection of the same type of information was not.[199] The March FISC opinion did not address the PCLOB Report analysis, but it is clear that *Jones* does leave open significant questions for future Fourth Amendment jurisprudence.[200]

Regardless of whether the *Jones* concurrences present a coherent approach to Fourth Amendment analysis, it appears that the NSA has overlooked other developments since *Smith*. At the time of the Court's decision in *Smith*, the reasonable expectation of privacy standard was defined by *Katz*. As neatly summarized in Justice Harlan's concurrence, this test asked two questions: did the person show an actual expectation of privacy and, if so, is that expectation one that society is prepared to recognize?[201] While the first part is clearly subjective, the second relies upon a social understanding. Crucially, the *Katz* and *Smith* Courts examined the expectation relative to contemporaneous social norms. In *Katz*, the Court emphasized the physical characteristics of a telephone booth and compared it to a taxicab.[202] In *Smith*, the Court's decision rested upon the specific operations of the telephone system. Neither opinion made any reference to expectations of privacy at the time of the Fourth Amendment's ratification, preferring to focus on society's expectation at the time of the case. However, as noted above, this is no longer the standard for a reasonable expectation of privacy. As the Court emphasized in both *Kyllo* and *Jones*, Fourth Amendment analysis now requires courts to examine the expectation of privacy at the time of ratification, not today. Thus, the second prong of the *Katz* test looks not to whether today's society is prepared to recognize an expectation of privacy as reasonable, but rather whether society in 1792 would have recognized it.

While the Court has not expressly overruled *Smith*, it is clear that the NSA Section 215 program must be examined under a different constitutional standard. As noted, the Court has

---

[197] *Id.*
[198] PCLOB Report at 124.
[199] PCLOB Report at 125.
[200] In re Application of the Federal Bureau of Investigation, No. BR 14-01.
[201] *Katz* at 361.
[202] *Katz* at 352.

now repeatedly emphasized that the expectation of privacy must be analyzed according to the level that was present at the time of the Fourth Amendment's ratification in 1792. This standard was most recently unanimously upheld in *Jones*. While the Court has not addressed how this expectation may be determined, Justice Alito's reasoning suggests that practical limits on law enforcement capability be considered, including issues such as manpower, budgets, and investigative priorities.[203] Therefore, an individual's reasonable expectation of privacy depends, in part, on law enforcement resources as they existed in 1792.

VI. Application of the Historical Fourth Amendment Test

Following revelations of the extent of the Section 215 collection program and the issuance of the Privacy and Civil Liberties Oversight Board's report in January 2014, President Obama proposed several reforms to the program. In his speech announcing these proposed reforms, President Obama defended the NSA, comparing its role in foreign intelligence surveillance to the conduct of Paul Revere during the American Revolution.[204] Noting that Revere was a member of the Sons of Liberty, a secret group that patrolled the streets of Boston in an effort to detect signs of British raids, President Obama drew a parallel to the modern efforts of the NSA.[205] The comparison is inapt, papering over key distinctions between the NSA program and early intelligence efforts and ignoring inconvenient aspects of Revere's service. Paul Revere was not only a silversmith and a spy, but he was also an early post rider for the Constitutional Post.[206]

The differences between the two positions Paul Revere held in Revolutionary-era America highlight the critical distinctions that render the NSA's Section 215 program unconstitutional. Revere personally monitored British and Loyalist individuals. Each night, he patrolled public areas and gathered information he observed with his own senses. Revere did not trespass into homes, steal personal property, or otherwise invade the privacy of their targets, but rather scrutinized the information those individuals exposed to public view. In essence, Revere's activities fit the mold of the police officers who physically follow an individual's movements on public highways and comport with the standard that finds no reasonable expectation of privacy in information disclosed to third parties. However, while acting as a post rider, Revere would have been under a strict duty not to inspect the communications placed in his care. While the temptation was no doubt very real, violation of this duty would have been grounds for his immediate termination and potentially criminal prosecution.

---

[203] *Jones* at 963-64.
[204] President Barack Obama, Address to the U.S. Dep't of Justice (Jan. 17, 2014) (transcript available at http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html).
[205] *Id.*
[206] Melius at 4.

Even if Paul Revere had attempted to gather intelligence through observation of an envelope's intended recipient, this information may have been of very little use to him. Prior to the invention of modern postal addresses (e.g., street numbers and zip codes), there was much less formality in addressing letters. A letter may be addressed simply "To Mike Donavan or his cousin Eliza MacFarrelly. Postman will find him by findin [sic] Betsy Brennan who was engaged to Mike before they left Ireland and may be married."[207] As noted above, the postal system originally operated in a chain-like system, with each postal office moving a letter one step closer to its apparent destination. A given postal clerk would likely have no idea whom the ultimate recipient would be, seeking only to get it closer to the destination.[208] Thus, in order to collect the information comparable to that contained in telephone metadata, government agents would have had to observe the final delivery of every single piece of mail sent through the U.S. Postal Service. Even then, any person wishing to avoid prying eyes could have sent their mail through a private carrier. Finally, the amount of letters sent via the postal system in the late 18th century was so little as to call into question whether collecting information even on every single letter would have led to worthwhile intelligence. In 1790, Americans sent only 300,000 letters total, just 0.1 per capita for the year.[209] While these numbers skyrocketed over the next decade as postal service improved, in 1800 the total numbers of sent letters still only corresponds to 0.5 letters per capita.[210] While the current annual number of telephone calls made per capita is unknown, it is clearly far beyond these numbers. As such, a surveillance program comparable the NSA's Section 215 program would have been neither within the capacity of law enforcement nor, if its target was the postal system, been consistent with the Founding Fathers' view of the Fourth Amendment.

Indeed, the FISC orders allowing the bulk collection of metadata are the modern-day incarnations of the general warrants which were the government practice specifically targeted by the framers in adopting the Fourth Amendment. By authorizing the government to force telecommunications providers to divulge telephony metadata in bulk, without any limitation relating to suspicion or particularity, the orders violates the most fundamental safeguards against intrusion that the Fourth Amendment was intended to make impossible. Thus, general warrants and writs of assistance gave the Crown's officers blanket authority to search where they pleased

---

[207] John at 146, citing Rees, James, *Foot-prints of a Letter-Carrier: Or, a History of the World's Correspondence* 241-42 (1866).
[208] This often led to mistakes. In one example from 1853, a Washington, D.C. resident received a letter addressed without the "D.C." which had previously been sent to twenty-three other Washingtons, with postal clerks marking the letter with messages such as "not known here" and "no such person." John at 146, citing Bunn, Alfred, *Old England and New England, in a Series of Views Taken on the Spot* 278-79 (1853).
[209] Johns at 4.
[210] *Id.*

for goods imported in violation of the customs law. They allowed the king to invade the security of any number of citizens and search for information without particularized suspicion.[211] The telephony metadata collection orders are plainly contrary to this fundamental guarantee of the Fourth Amendment. Under it, the government is authorized to collect, store, and examine personal information on each and every citizen who uses a telephone within the United States, not on the basis of suspicion, but in order to generate suspicion.

General warrants also were condemned because they authorized searches which were not carefully circumscribed. They did not specify the things to be seized, but instead left unbridled discretion to the executing officer of what could be taken from the person who was the target of the search. They gave officers a roving commission to seize any and all property and engage in a fishing expedition.[212] As the anonymous writer "Candor" wrote on the ransacking of papers at issue in the *Wilkes* case, general warrants "would lead to the seizing of a man and his papers for a libel, against whom there was no proof, merely slight suspicion, under a hope that, among the private papers of his bureau, some proof might be found which would answer the end. It is a fishing for evidence, to the disquiet of all men, and to the violation of every private right; and is the most odious and infamous act, of the worst sort of inquisitions, by the worst sort of men, in the most enslaved counties[.]"[213] With this history in mind, the Supreme Court has established that the Fourth Amendment's search and seizure clause does not permit an "indiscriminate rummaging"[214] through the records or belongings of individuals.

The mass seizure of telephony metadata under the order is indistinguishable from the supposedly forbidden general warrants of yore. "As with general warrants, blanket seizure programs subject the private papers of innocent people to the risk of search and exposure, without their knowledge and with no realistic prospect of a remedy."[215] The kind of "mass dataveillance" authorized by the order at issue here possess the same dangers the Framers meant to prohibit by adopting the Fourth Amendment, i.e., general warrants under which the government is allowed to commit intrusions "in search of suspicious information without particularized suspicion and without limitations on its use."[216]

---

[211] Rosen, *supra*, 46 Ariz. L. Rev. at 611.
[212] *Berger*, 388 U.S. at 58-59.
[213] Donald A. Dripps, *"Dearest Property": Digital Evidence and the History oif Private "Papers" as Special Objects of Search and* Seizure, 103 J. Crim. L. & Criminology 49, 70 (2013) (quoting Candor, *A Letter from Candor to the Public Advertiser* (London, J. Almon 1764)).
[214] *California Bankers Assoc. v. Shultz*, 416 U.S. 21, 62 (1974).
[215] Randy E. Barnett & Jim Harper, *Why NSA's Bulk Data Seizures Are Illegal and Unconstitutional*, The Federalist Society October 21 2013 (available at http://www.fed-soc.org/publications/detail/why-nsas-bulk-data-seizures-are-illegal-and-unconstitutional).
[216] Rosen, *supra*, 46 Ariz. L. Rev. at 611.

The NSA's Section 215 collection program entails an invasion of privacy far beyond what the Founding Fathers could have imagined. As the President's own Privacy and Civil Liberties Oversight Board noted, the bulk collection of telephone metadata can reveal intimate details about a person's life, especially when combined with other information and subjected to sophisticated computer analysis. While the NSA emphasizes that it does not listen to actual conversations, the circumstances of a particular call, revealed by the metadata, can be highly suggestive of the content of a phone call. Moreover, the invasion of privacy is magnified by the bulk collection and five-year storage of all phone calls since this can reveal information far beyond that which can be obtained from a single telephone call.[217] The technological innovations that allow such vast collection and analysis far exceed anything human senses are capable of alone, squarely implicating the Court's concerns in *United States v. Jones*. As the Justices in that case noted, a violation of the Fourth Amendment may occur when technological advances allow the collection and analysis of information in a manner beyond the abilities of law enforcement at the time of the Fourth Amendment's ratification, even if it is the same type of information that may be gathered through human observation alone. An individual's reasonable expectation of privacy is formed in part by the limitations on police resources and priorities, so while the police's use of a pen register on a single individual's telephone for two days as part of an investigation into a specific crime may be constitutional, the unending collection of metadata for virtually every single telephone call involving any American without connection to any specific investigation is likely to run afoul of the reasonable expectation of privacy test set forth in *United States v. Jones*. Law enforcement in the 1790s obviously lacked the ability to gather information on this scope, and even if they did, they would not have used it to investigate potential or speculative crimes in the nature of international terrorism. The NSA's reliance on *Smith* without the limitations placed on that holding by the majority in *Jones* means that its analysis of constitutionality of the Section 215 program is incomplete at best. Given a complete and proper constitutional framework, the bulk collection of telephone metadata under Section 215 more likely violates the reasonable expectation of privacy of every American who makes or receives a telephone call and thus is not permissible under the Fourth Amendment. In 1792, American citizens had the reasonable expectation that they could regularly communicate via mail—the antecedent of today's phone calls—without identifying to the government either the sender or the receiver.

VII. Conclusion

Under the required historical standard, the NSA's Section 215 telephone metadata collection program violates the Fourth Amendment to the United States Constitution. The program simply does not accord Americans the same reasonable expectation of privacy as they had in 1792. The NSA has argued that its program is compatible with Supreme Court Fourth

[217] PCLOB Report at 12.

Amendment jurisprudence, citing *Smith v. Maryland*'s distinction between actual telephone conversations and the information necessarily provided to telephone companies in order to complete the call. However, the NSA has given insufficient weight to post-*Smith* case law that calls into serious question its suitability as a legal basis for the Section 215 program. In particular, the Court's decision in *United States v. Jones* means that government surveillance that is constitutional when done on a limited basis might violate the Constitution if done on a massive, technologically-enabled scale. The Court has suggested several means to formulate when government actions cross this threshold, including examining law enforcement resources available in 1792. The Court has also previously and repeatedly identified the postal service as a suitable comparison point for the telephone system in Fourth Amendment analysis. An examination of 1792 law enforcement resources and the concurrent privacy expectations regarding postal communications leaves no doubt that law enforcement could not have maintained anything approaching the NSA's Section 215 program nor would any such program, if based on the postal service, have been consistent with the Fourth Amendment's guarantee of a reasonable expectation of privacy. Therefore, the telephone metadata program violates the Fourth Amendment and is unconstitutional.