Does the History Behind the Adoption of the Fourth Amendment Demand Abolishing the Third-Party Doctrine?

*Craig Ettinger**

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. – Fourth Amendment, United States Constitution

Introduction

The overarching issues this Article addresses are (1) to what extent the government can extract different categories of internet data from consumers, and (2) how the law can be used to restrict the government's reach in extracting such data. As can be gathered from the text of the Fourth Amendment, cited above, people have the very broad right to be secure in their persons, houses, papers, and effects from unreasonable searches and seizures.[1] Despite the breadth of this right, some courts today incorrectly apply it to individuals when police agencies gather data generated on or through use of the internet.

Regardless of how courts approach which forms of internet communications or uses should be protected, there is still disagreement within the legal community about how Fourth Amendment jurisprudence should handle the problems the internet poses today, and about whether the legal tests employed are obsolete and require an update.[2] Currently, courts seem willing to allow police to obtain evidence from the internet even when the same type of evidence, in non-digital form,

* Craig Ettinger, 2018 *magna cum laude* graduate of Chicago-Kent College of Law; order of the coif inductee.

[1] U.S. Const. amend. IV.

[2] *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 Calif. L. Rev. 805, 807–12 (2016).

would require a warrant.[3] This allowance is not only contrary to the intent of the Fourth Amendment,[4] but it also allows the government to take actions that the Fourth Amendment was expressly adopted to prevent.[5] For example, in England and in the thirteen Colonies, the English government executed general warrants and Writs of Assistance to gather evidence through searches of people's possessions without probable cause.[6] By adopting the Fourth Amendment, the American Framers specifically rejected these approaches, replacing them with the requirement that there be probable cause to suspect that a target was engaged in criminal activity before performing such a search.[7]

Before addressing the reasons why Fourth Amendment jurisprudence should be returned to its roots in *Katz v. United States* and before attempting to apply the Framers' intent to modern-era issues, it is necessary to understand the history of the Fourth Amendment and

---

[3] *See* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 824-26 (2005); Chris Bousquet, *Mining Social Media Data for Policing, the Ethical Way,* DATA-SMART CITY SOLUTIONS (April 26, 2018), https://datasmart.ash.harvard.edu/news/article/mining-social-media-data-policing-ethical-way. *Cf. Ybarra v. Illinois*, 444 U.S. 85, 88, 96 (1979) (finding application of Illinois statute permitting police to detain and search anyone found on premises that are being searched pursuant to a search warrant unconstitutional).

[4] *See, e.g.*, An Old Whig V, INDEP. GAZETTEER (Phila.) Nov. 1, 1787, *reprinted in* 13 THE DOCUMENTARY HISTORY OF THE RATIFICATION OF THE CONSTITUTION 538, 541 (John P. Kaminski et al. eds., 1981) [hereinafter DOCUMENTARY HISTORY] (expressing the view that, without a Bill of Rights, no persons' "houses and papers [would be] free from seizure and search upon general suspicion or general warrants"); *Brutus II*, N.Y.J. (Nov. 1, 1787), *reprinted in* 19 DOCUMENTARY HISTORY 154, 157 (John P. Kaminski & Gaspare J. Saladino eds., 2003) (arguing that a bill of rights was necessary because of the power of the central government of "granting search warrants, and seizing persons, papers, or property"); Patrick Henry, *Debates, The Virginia Convention* (June 16, 1788), in 10 DOCUMENTARY HISTORY 1474-75 (John P. Kaminski & Gaspare J.et al. eds., 1993).

[5] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 737, 745-46 (1979) (permitting the government to install a pen register that tracked the phone numbers defendant dialed from his home did not violate the Fourth Amendment); United States v. Miller, 425 U.S. 435, 442, 444-45 (1976) (finding the federal government's subpoena requesting and obtaining defendant's bank records to not violate the Fourth Amendment); United States v. Lifshitz, 369 F.3d 173, 190 (2d. Cir. 2004) (finding government monitoring of defendant's email on his computer did not violate the Fourth Amendment); United States v. Hambrick, 225 F.3d 656, *4 (4th Cir. 2000) (finding defendant had no Fourth Amendment protection in his name, billing address, IP address, credit card information, and other identifying information he provided to his internet service provider when the government requested and obtained such information through a subpoena); Webb v. Goldstein, 117 F. Supp. 2d 289, 295 (E.D.N.Y. 2000) (finding subpoena requesting to obtain defendant's medical records from a medical institution did not violate the Fourth Amendment).

[6] LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 156-57 (1999); William J. Stuntz, *The Substantive Origins of Criminal Procedure*, YALE L.J. 393, 398-99 (1995).

[7] *See supra* note 4 and accompanying text; U.S. CONST. amend. IV.

how courts have shaped it over time. The periods relevant to this Article stretch from the 1500s to the late 1700s. This is the time period when the English government used general warrants and dreaded Writs of Assistance to invade the lives of Colonial and English citizens at the Crown's will.[8]

From the 1500s through the 1700s, British law allowed the government, based upon "a bare surmise," to enter people's homes to ransack them and the containers within.[9] This allowed the Crown to silence dissenters by using evidence gathered to bolster its legal cases and to deter future criticisms of the Crown by pursuing more criminal charges.[10] Even though United States law explicitly prohibits general warrants,[11] government agents from local and federal law enforcement engage in similar actions when searching and seizing digital evidence.[12]

In today's almost completely interconnected world, police do not need a warrant to search and seize consumers' private data on the internet.[13] Instead, the government can issue a subpoena to a third party to extract desired data,[14] conduct warrantless computer surveillance on its target,[15] get information from internet data recipients

---

8 *See* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 43, 56-58, 96-100, 439-40, 490-91 (2009).

9 *See* EDWARD COKE, THE FOURTH PART OF THE INSTITUTES OF THE LAWS OF ENGLAND: CONCERNING THE JURISDICTION OF COURTS 176-78 (1644); WILLIAM BLACKSTONE, 4 COMMENTARIES ON THE LAWS OF ENGLAND 287 (1769).

10 *See* CUDDIHY, *supra* note 8, at 55-60, 439-44.

11 U.S. CONST. amend. IV ("[N]o 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."); *see also* Groh v. Ramirez, 540 U.S. 551, 572 (2004) (Thomas, J., dissenting) (stating that the Fourth Amendment's history is "clear as to the Amendment's principal target (general warrants)").

12 *See* DOJ v. Utah Dept. of Com., No. 2:16-cv-611-DN-DBP, 2017 WL 3189868, at *9 (D. Utah July 27, 2017) (finding the Department of Justice's subpoena to warrantlessly access a patient's prescription records stored in a secure database to not violate the Fourth Amendment); U.S. DEPT. OF HOMELAND SEC. PRIVACY OFF., 2016 DATA MINING REPORT TO CONGRESS at 31-34; Jessica Guynn, *ACLU: Police used Twitter, Facebook to track protests*, USA TODAY (Oct. 11, 2016, 12:44 PM), "ACLU: Police used Twitter, Facebook to track protests," *USA TODAY*, October 11, 2016, https://www.usatoday.com/story/tech/news/2016/10/11/aclu-police-used-twitter-facebook-data-track-protesters-baltimore-ferguson/91897034/; U.S. Dept. of Homeland Security. Privacy Office. *2016 Data Mining Report to Congress*. Washington, D.C. 2017.

13 *See* Slobogin, *supra* note 3, at 826.

14 *See id.*

15 *See* Bousquet, *supra* note 3.

about incriminating data they receive,[16] or employ other warrantless conduct which suspects and third parties have little recourse to challenge.[17] The Supreme Court granted the government these vast powers through its adoption of the third-party doctrine, which allows the government to obtain any information a person has disclosed to a third party.[18]

With the third-party doctrine being one set of legal tools in a prosecutor's vast arsenal, the right to feel secure in one's person, home, papers, and effects is quickly being chipped away as technology continues to transform the way people do business and participate in society, moving from in-person contacts to internet-based contacts.[19] Given that consumers have little choice but to use the internet to function in today's society, courts need to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[20]

Therefore, based upon the horrific effects of general warrants and Writs of Assistance, and upon how closely those effects parallel the third-party doctrine's effects, the Supreme Court should require probable cause before the government can extract digital evidence for prosecution and should do away with the third-party doctrine. Without such a requirement for seizing people's data, the government is allowed to conduct searches that the Fourth Amendment was adopted to prevent.[21] In today's digitally interconnected world, courts should evaluate on a case-by-case basis whether an individual has an objective expectation of privacy when "society is prepared to recognize [that expectation] as 'reasonable.'"[22] If the Supreme Court does not engage in this normative-based inquiry, the Court is doing exactly what our history teachers taught us not to do: repeating history.

---

16 *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984) (finding that private parties observing evidence and bringing it to the attention of law enforcement was not a search).

17 *See* 18 U.S.C. §§ 3121-3127 (2001); 18 U.S.C. § 2511; 18 U.S.C. § 2701; Melinda J. Caterine, *Privacy of Electronic Communications*, AMERICAN BAR ASSOCIATION, (Dec. 23, 2012), https://www.americanbar.org/content/dam/aba/administrative/labor_law/meetings/2009/2009_err_008.authcheckdam.pdf.

18 *See* United States v. Miller, 425 U.S. 435, 442-43 (1976); Evan Peters, *The Technology We Exalt Today Is Everyman's Master*, 44 WASH. U. J.L. & POLICY 103, 110-19 (2014).

19 U.S. DEP'T OF COM. U.S. CENSUS BUREAU, QUARTERLY RETAIL E-COMMERCE SALES 4TH QUARTER 2017 (2018).

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

21 *See supra* notes 4-5 and accompanying text.

22 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

I. THE FOURTH AMENDMENT'S HISTORICAL FOUNDATION AND HOW THAT FOUNDATION INFLUENCED THE FOURTH AMENDMENT'S PROTECTIONS OF CITIZENS

In examining the American and English history surrounding the Fourth Amendment's formation, an overarching theme emerges: it is necessary to guard against government use of broad searches and seizures to avoid the harmful effects that such vast power can have on citizens and on society as a whole.[23] A handful of brave lawyers took up their instruments, bearing legal arms against the Crown's abuse of power in using general warrants and Writs of Assistance.[24] The Crown employed both of these measures in different ways to consolidate power[25] while trying to maintain a clean image with its subjects.[26] The Crown was ultimately unsuccessful in achieving its goals, and its failures paved the way for modern Fourth Amendment jurisprudence.[27]

The Fourth Amendment's historical roots show that the protections the Framers included in the Fourth Amendment, and the reasons for those protections, contradict the Supreme Court's adoption of the third-party doctrine. First, in examining English history, the Crown primarily used its broad power to search and seize persons and their property to protect itself politically and economically.[28] The Crown first used general warrants to enforce universal religious belief in Christianity and to censor all heretics and dissenters of the Crown.[29]

---

23 *See* Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1182-83 (2016); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 578-80 (1999).

24 Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 992-1002 (2011).

25 *See* Donohue, *supra* note 23, at 1209-11 (Queen Elizabeth I used general warrants to silence her dissenters).

26 *See id.* at 1199-1201 (The Crown published a pro-government publication called "The Briton" and Crown dissidents published their own writings which were seized after publication through issuing general warrants).

27 *See* Clancy, *supra* note 24, at 1011-12 (John Adams, one of the framers of the Fourth Amendment, knew of the English citizens' plights and congratulated John Wilkes, a member of Parliament, on his legal victory against the Crown).

28 *See* CUDDIHY, *supra* note 8, at 85 (King James I used general warrants to uncover the "Gunpowder Plot" which was a scheme to blow up the House of Parliament, along with the King, in order install the King's nine-year-old daughter as a Catholic monarch).

29 *Id*. at 56-57 (discussing Queen Mary I's use of general warrants to reestablish the Catholic Church).

In the early 1500s, church and state were not separate.[30] The Crown used religion to strengthen its power, including its power over its Colonial subjects.[31]

In fact, Queen Elizabeth I laid the legally oppressive groundwork necessary to protect state-controlled religion through the use of general warrants. In 1559, Elizabeth I formed a High Commission for the purpose of quieting "seditious and slanderous persons" speaking of "false rumours, tales and seditious slanders" against the Queen "and the said good laws and statutes."[32] Unfortunately for the Crown's subjects, when King James I came to power, he expanded the High Commission's reach to search and seize any persons or property that related to religious matters or to the Crown's public image.[33] James I gave the Commission the power to find any materials or documents that were "offensive to the state" and to persecute anyone involved in the materials' release to the public.[34] This included authors, publishers, and even people who merely printed words on manuscripts.[35] As time progressed, Parliament passed statutes to broaden the Crown's power.[36] With this broadening of power came awareness of the concern that if "every dissolute agent of the [High] [C]ommission by a warrant under the handes of the Commissioners, shall enter into mens howses, break vpp their chestes and chambers, . . . carry away what they list, and afterward *pick matter to arrest and commit them*[,]" then where does this power end?[37]

Sir Edward Coke first sought to address this concern, as he too became a victim of the Crown because of his continual criticism of the

---

[30] *See* An Acte for the Uniformitie of Common Prayoure and Dyvyne Service in the Churche, and the Administration of the Sacramentes, 1 Eliz, ch 2 (1559), in 4 Statutes of the Realm 355, 355 (laying out the prayers to be included in the Book of Common Prayer); An Acte Restoring to the Crowne Thaucyent Jurisdiction over the State Ecclesiasticall and Spuall, and Abolyshing All Forreine Power Repugnaunt to the Same, 1 Eliz, ch 1 (1559), in 4 Statutes of the Realm 350, 351-52 (reviving the statutes withdrawn by Mary I and reestablishing the monarch as the Supreme Governor of the Church of England).

[31] *See* Establishment of the Court of High Commission (1559) *reprinted in* SELECT DOCUMENTS OF ENGLISH CONSTITUTIONAL HISTORY, 310-314 (George Burton Adams & H. Morse Stephens, eds., 1935).

[32] *Id.* at 310.

[33] Donohue, *supra* note 23, at 1209.

[34] *See* CUDDIHY, *supra* note 8, at 58 (quoting a Commission report from June 21, 1614).

[35] *See id.* (quoting a Commission report from August 29, 1611).

[36] *See id.* at 69-101.

[37] *Id*. at 114 (internal quotation marks omitted) (emphasis added).

Crown's tyrannical use of power.[38] In 1621, James I issued a general warrant to seize Coke and to search his home.[39] The warrant ordered the King's officers "to make dilligent search for all such papers and writeings as doe anie way concerne his Majestie's service" and "to open all such studies, clossetts, chests, trunkes, deskes or boxes, where you shall understaund or probably conceave anie such papers . . . ."[40]

As the Crown's former Attorney General, Coke had been forced to exact onto others the same wrongs he eventually experienced himself.[41] Coke's experience galvanized his fight against the Crown.[42] In 1628, Coke gave a speech to the House of Commons regarding the Petition of Right of 1628.[43] In that speech, Coke used the confiscation of his manuscripts and his interrogation to argue that the Petition of Right should include a clause requiring that cause be shown before a man could be imprisoned against his will.[44] Coke stated that, during that day in 1621, he was "committed to [prison]" and all of his "books and study searched, and 37 manuscripts were taken away . . . ."[45] He further made the point that enshrining this clause within the Petition of Right was necessary because, if a person's house could be searched while he was confined without being told the cause, "they will find cause enough"—that is, they will find something incriminating.[46] This concern of Coke's parallels problems manifest in the modern world, as sifting and searching through a person's internet data, without having cause in advance, will allow police investigators to "find cause enough."[47] In March of 1628, Coke provided the materials that created the foundation for modern Fourth Amendment jurisprudence when he proclaimed to Parliament, "No free man ought to be committed but the cause must be showed *in particular*."[48]

---

38 *See* Donohue, *supra* note 23, at 1211.

39 3 SIR EDWARD COKE, THE SELECTED WRITINGS AND SPEECHES OF SIR EDWARD COKE, 1329-30 (Steve Sheppard, ed., 2003).

40 *Id.* at 1330.

41 *See* CUDDIHY, *supra* note 8, at 140.

42 *See* COKE, *supra* note 39, at 1270-71; Donohue, *supra* note 23, at 1211.

43 COKE, *supra* note 39, at 1270.

44 CUDDIHY, *supra* note 8, at 141.

45 COKE, *supra* note 39, at 1271.

46 CUDDIHY, *supra* note 8, at 141 (Coke is quoted from a House of Commons debate transcript recorded on April 29, 1628).

47 *Id.*

48 COKE, *supra* note 39, at 1234 (emphasis added).

Following King Charles's seizure of Coke's writings, other English legal scholars began to cite Coke in their own treatises and essentially established that Coke's thoughts should be universal law.[49] In the "Historia Placitorum Coronae" ("History of the Pleas of the Crown"), one English legal scholar's language also shows the parallel between English history and modern-day internet use.[50] In this piece, the author proclaimed:

> [A] general warrant to search in all suspected places is not good, but only to search in such particular places, where the [government] assigns before the justice his suspicion and the probable cause thereof, for these warrants are judicial acts, and must be granted upon examination of the fact[s]. . . . [T]herefore I take those general warrants . . . are not justifiable, for it makes the [government] to be in effect the judge; and therefore searches made by pretense of such general warrants give no more power to the [government], than what they may do by law without them.[51]

The second sentence quoted from *Historia* should ring true as applied to the concern that police can abuse the knowledge they may have of a person's specific uses of the internet. Consequently, the third-party doctrine and the scope of warrants to search a person's electronic device content enact a sort of general warrant that gives the police the power "to be in effect the judge."[52]

The writings of these legal dissenters sowed the seeds of the American Framers' reasoning for rejecting general warrants altogether in the language of the Fourth Amendment.[53] Then, three seminal English cases continued to shape Fourth Amendment jurisprudence.

---

[49] *See, e.g.*, 2 WILLIAM HAWKINS, A TREATISE OF PLEAS OF THE CROWN 140 (1795); 1 JOSEPH SHAW, THE PRACTICAL JUSTICE OF PEACE: OR A TREATISE SHOWING THE PRESENT POWER OF THAT OFFICER IN ALL THE BRANCHES OF HIS DUTY 261-62 (1728); 2 MATTHEW HALE, HISTORIA PLACITORUM CORONAE 107, 113-14 (1736).

[50] *See* HALE *supra* note 49, at 150.

[51] *Id.*

[52] STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FRIST CENTURY 35 (2012) (quoting SIR MATTHEW HALE, 2 HISTORY OF THE PLEAS OF THE CROWN 150 (Sollom Emlyn ed., 1800)).

[53] *See* Clancy, *supra* note 24, at 1013 (showing that John Adams collected treatises from several English legal scholars who wrote about search and seizure principles including: William Blackstone, Sir Edward Coke, Sir Matthew Hale, William Hawkins, Michael Dalton, and Richard Burn).

A. *Three English Cases Leading to the Framers' Adoption of the Fourth Amendment*

England's encounters with general warrants and the Colonies' encounters with Writs of Assistance are intertwined.[54] Writs of Assistance greatly resembled general warrants, but writs granted more power to their holders than did general warrants.[55] The following table illustrates the similarities and differences between the two tools of enforcing tyranny:

General Warrants	Writs of Assistance
• The Crown or the Secretary of State could generally issue general warrants, without any justifications to support their issuance, giving officials wide latitude to search and seize anyone and anything.[56] • English common law required a warrant to intrude into someone's home, and it had to be based upon a "bare surmise" that the home contained stolen goods or felons subject to search and seizure; but, exceptions existed that justified warrantless intrusions.[57] • To subvert the common law, statutory measures were passed to give power to wielders of general warrants to search homes under broad pretenses.[58]	• The Crown gave the writ-holder the power to search anywhere and anything he believed held condemned goods at any time, including the home.[59] • This power was effective for as long as the King was alive.[60] • All officers and able-bodied common people were mandated by the writ to help the holder make his search.[61] • If the writ-holder caused damage to a person's property in the execution of his search, he would not be liable for any damage caused and was permitted to cause such damage to find contraband.[62]

54 *See* Robert J. McWhirter, *Molasses and the Sticky Origins of the 4th Amendment A Pictorial History*, 43 ARIZ. ATT'Y 16, 27-31 (June 2007) (English general warrant litigation began in 1763 and the Colonial Writs of Assistance case began in 1761).

55 Clancy, *supra* note 24, at 991 (quoting JACOB W. LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT: A STUDY IN CONSTITUTIONAL INTERPRETATION, 31 (1966)) (citing Berger v. New York, 388 U.S. 41, 58 (1967) (equating Writs of Assistance with general warrants)).

56 *See* SCHULHOFER, *supra* note 52, at 24.

From 1761 to 1780, the American Colonies and England both faced the tyrannical powers of the Crown.[63] This time period in the Colonies and in England was the catalyst for the Fourth Amendment's adoption.[64] Starting in 1761, the Colonies began to challenge Writs of Assistance on the grounds that they were mirror images of general warrants, and should be struck down and amended to reflect the common law requirements of probable cause and particularity for search warrants.[65] James Otis and John Adams were at the forefront of the challenges to these over-expansive writs.[66]

Shortly after the Writs of Assistance challenges, a series of general warrants were litigated in England.[67] These seminal cases shaped the American Framers' ideology in creating the text necessary to combat general warrants and to regulate other search and seizure activities in the late eighteenth century and in the nineteenth century.[68] John Adams proclaimed that James Otis's arguments against Writs of Assistance in Massachusetts marked the point where "the child Independence was born."[69] John Entick, in his case against the Crown, first spurred the idea to prohibit the execution of general warrants in England.

---

[57] *Id.* (quoting COKE, *supra* note 9, at 176-77).

[58] Donohue, *supra* note 23, at 1193, 1195-96.

[59] Clancy, *supra* note 24, at 991 (quoting LANDYNSKI, *supra* note 55, at 31; TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION, 26 (1969); NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION, 263-64 (1937)).

[60] LASSON, *supra* note 59, at 263-64.

[61] *See* M.H. SMITH, THE WRITS OF ASSISTANCE CASE, 29 (1978); SAMUEL DASH, THE INTRUDERS: UNREASONABLE SEARCHES AND SEIZURES FROM KING JOHN TO JOHN ASHCROFT 36 (2004).

[62] *See* Clancy, *supra* note 24, at 1000-01 (referring to James Otis's arguments as to why the Writs of Assistance should be unlawful) (quoting CHARLES FRANCIS ADAMS, 2 THE WORKS OF JOHN ADAMS, SECOND PRESIDENT OF THE UNITED STATES 524-25 (Charles C. Little & James Brown eds., 1850).

[63] *See* McWhirter *supra*, note 54 at 30-31; Clancy, *supra* note 24, at 989.

[64] *See* Clancy, *supra* note 24, at 989.

[65] *Id.* at 992-1002; *see also* Gerstein v. Pugh, 420 U.S. 103, 116 n.17 (1975).

[66] *See* McWhirter, *supra* note 54, at 30-31.

[67] *Id.* at 20, 30-31.

[68] *See, e.g.*, Stanford v. Texas, 379 U.S. 476, 484 (1965) (describing the Wilkes opinion as "a wellspring of the rights now protected by the Fourth Amendment"); Boyd v. United States, 116 U.S. 616, 626-27 (1886) (maintaining that it can be "confidently asserted" that the Wilkes case and its results "were in the minds of those who framed the Fourth Amendment"); *see also* Clancy, *supra* note 24, at 1010 n.182.

[69] LASSON *supra* note 59, at 59.

1. *Entick v. Carrington* (1765)

In 1755, John Entick and his associates began their challenge to hold the Crown and its officials accountable for actions that they deemed irreconcilable with the freedoms entitled to the people.[70] With his associates, Entick launched a weekly essay paper, *The Monitor*, to "commend good men and good measures, and to censure bad ones."[71] Their goal was to awaken "that spirit of LIBERTY AND LOYALTY, for which the *British* nation was *anciently* distinguished," and to use that spirit against the Crown's tyrannical practices.[72] *The Monitor*'s treatment of the political elite did not go unnoticed. On November 6, 1762, the second Earl of Halifax, George Montague Dunk, signed a general warrant that denounced *The Monitor*'s "gross and scandalous reflections and invectives upon his majesty's government, and upon both houses of parliament."[73]

Following the Crown's intrusions, Entick brought a civil suit against the Crown and the Earl of Halifax for trespass, on the grounds that he ought to be secure in his home against unreasonable governmental intrusion.[74] Charles Pratt, the Chief Justice of the Common Pleas, ruled against the Crown and found the search's illegality began the moment the King's messengers entered Entick's home.[75] Interestingly, Chief Justice Pratt's words about the seizing of Entick's papers just as easily addresses modern concerns about governmental internet searches. Regarding Entick's papers, Chief Justice Pratt declared the following in his ruling:

> Papers are the owner's goods and chattels. They are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect.

---

70 Donohue, *supra* note 23, at 1196-97.

71 1 THE MONITOR: OR, BRITISH FREEHOLDER, THE DEDICATION *1 (J. Scott, 3d ed. 1760).

72 *Id.* at *1-2.

73 Donohue, *supra* note 23, at 1197 n.64 (quoting Entick v. Carrington, 19 How. St. Tr. 1029, 1034 (CP 1765)).

74 *Entick*, 19 How. St. Tr. at 1032.

75 *Id.* at 1066 (finding that "every invasion of private property, be it ever so minute, is a trespass"); *see also Boyd*, 116 U.S. at 630 (noting that Chief Justice Pratt, referred to as "Lord CAMDEN," laid down the Fourth Amendment's basic principles).

> Where is the written law that gives any magistrate such a power? I can safely answer, there is none; and therefore it is too much for us without such authority to pronounce a practice legal, which would be subversive of all the comforts of society.[76]

Chief Justice Pratt was concerned with a person's right of privacy in his home and in his chattels.[77] If general warrants could be used to circumvent the common law requirements of a specific warrant, then "such a power would be more pernicious to the innocent than useful to the public."[78]

2. *Wilkes v. Wood* (1763)

The Colonies paid the most attention to a subsequent case, *Wilkes v. Wood*, and revered it as the search and seizure case having the most influence on the path of today's Fourth Amendment jurisprudence.[79] John Wilkes was a Member of Parliament and the publisher of *The North Briton*, a political magazine that mocked the government.[80] *The North Briton*'s purpose was specifically to irritate King George III.[81] *The North Briton No. 45* more than accomplished that goal, as this edition mocked King George's speech to Parliament with regard to his comments about the public benefits of the Treaty of Paris, the end of the Seven Years' War, and the Treaty itself.[82] Wilkes urged the people to resist the King and to resort to rebellion if necessary.[83] He supported this sentiment by questioning how there could be peace between the Crown and its subject when "private houses are now made liable to be entered and searched at pleasure?"[84]

The King soon reached the end of his tether. Following *The North Briton No. 45*'s publication, a warrant was issued calling on its executors "to make strict and diligent search for the authors, printers

---

76 *Entick*, 19 How. St. Tr. at 1066.

77 *See id.* at 1073.

78 *Id.*

79 Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 772 (1994).

80 McWhirter, *supra* note 54, at 18.

81 *See* DASH, *supra* note 61, at 27.

82 *See id.*; ARTHUR H. CASH, JOHN WILKES, THE SCANDALOUS FATHER OF CIVIL LIBERTY 100 (2006); John Wilkes, *North Briton No. 25*, in 2 *The North Briton* 136, 136-37 (printed for John Mitchell and James Williams 1764).

83 *See* CASH, *supra* note 82, at 100.

84 LASSON, *supra* note 59, at 43 n.108 (quoting the *North Briton No. 45*).

and publishers of a seditious and treasonable paper, intitled, The North Briton," and "to apprehend and seize [them], together with their papers, and to bring in safe custody before me, to be examined."[85] The King's messengers carried out the warrant by entering Wilkes's home and rummaging through every nook, cranny, chest, drawer, and closet.[86] Wilkes was arrested, along with 48 other people.[87]

Shortly thereafter, Wilkes filed a lawsuit for trespass and false imprisonment against John Wood, the official who oversaw the search and seizure of Wilkes's chattels and papers.[88] In Wilkes's trial, as in many others, the Crown's lawyers relied upon the fact that these general warrants were customary and, therefore, not illegal.[89] Moreover, the excessive searches and seizures of papers were justified considering the level of treason *No. 45* had committed.[90]

Ultimately, the jury found in favor of Wilkes and awarded him "exemplary damages" to deter similar future conduct by the Crown.[91] Chief Justice Pratt, who oversaw the trial, criticized the warrants for not specifying the persons to be seized by name and for giving the messengers far too much discretion to search wherever they believed "libelous" material existed.[92] Chief Justice Pratt declared that if the power to issue these kinds of warrants existed, "it certainly may affect the person and property of every man in this kingdom, and [be] totally subversive of the liberty of the subject."[93]

3. *Leach v. Money* (1765)

The invasion of Dryden Leach's rights arose out of the same general warrant that invaded Wilkes's rights.[94] Leach was the publisher of

---

85 *The Case of John Wilkes, esq. on a Habeas Corpus, Common Pleas*, Easter Term: 3 George III. (1763) *in* 19 A COMPLETE COLLECTION OF STATE TRIALS AND PROCEEDINGS FOR HIGH TREASON AND OTHER CRIMES AND MISDEMEANORS FROM THE EARLIEST PERIOD TO THE PRESENT TIME 1753-1771 981-82 (T.B. Howell, ed., 1813).

86 *See* Wilkes v. Wood, 98 E.R. 489, 491 (1763).

87 McWhirter, *supra* note 54, at 20 (citing LASSON, *supra* note 59, at 44).

88 *Wilkes*, 98 E.R. at 489.

89 *See* CUDDIHY, *supra* note 8, at 444 n.22.

90 *Id.*

91 *Wilkes*, 98 E.R. at 498-99.

92 *Id.* at 498.

93 *Id.*

94 Leach v. Money, 19 How. St. Tr. 1001, 1003-04 (KB 1765).

previous issues of *The North Briton*, but did not publish *No. 45*.[95] During Leach's legal proceedings, his counsel, John Dunning, rebutted the Crown's justifications for the general warrant by citing the cautions articulated by Sir Matthew Hale and another English legal scholar, stating that "to ransack private studies *in order to search for evidence*, and even without a previous charge on oath, is contrary to natural justice, as well as the liberty of the subject."[96] Attacking the legality of the warrant, Dunning proclaimed:

> If "Author, Printer, and Publisher" without naming any particular Person, be sufficient in such a Warrant as this; it would be equally so, to issue a warrant generally, "to take up the Robber or murderer of such a One." This is no Description of the Person; but only of the Offence: It is making the Officer to be Judge of the Matter, in the Place of the Person who issues the Warrant. Such a Power would be extremely mischievous and might be productive of great Oppression.[97]

The trial court's ruling, that the warrant was illegal and void, was affirmed.[98]

These three seminal English cases, along with a Writs of Assistance case commonly referred to as Paxton's case, most influenced the American Framers' thoughts regarding search and seizure practices prior to adopting the Fourth Amendment.[99] The Colonial press reported on these cases thoroughly and framed them to help the colonists understand the oppressive nature of general warrants.[100] John Adams owned a book containing one of the *Wilkes* cases, and Adams even wrote Wilkes a letter showing his support and admiration of Wilkes's feats of justice.[101] Not by coincidence, it was John Adams who primarily helped craft the Fourth Amendment's language.[102] Adams did not accomplish this feat alone, however, as the Writs of Assistance case argued by James Otis provided Adams with the

---

95 *See* Clancy, *supra* note 24, at 1008.

96 *Leach*, 19 How. St. Tr. at 1024 (emphasis added).

97 Clancy, *supra* note 24, at 1009 (citing *Leach*, 97 Eng. Rep. at 1762).

98 *Leach*, 19 How. St. Tr. at 1028.

99 *See* Clancy, *supra* note 24, at 1006 n.151 & 1010 n.182.

100 Clancy, *supra* note 24, at 1011 n.184 (citing CUDDIHY, *supra* note 8, at 538-40, 847-50).

101 Clancy, *supra* note 24, at 1011-12 and accompanying text.

102 *Id.* at 1029.

ammunition he needed to protect privacy from the powerful eyes of the government.[103]

B. *Colonial History*

From 1761 to 1791, many events in the Colonies influenced the Framers to adopt the current text of the Fourth Amendment.[104] Because England could not risk the colonists funding England's enemies in an ongoing war, new Writs of Assistance were requested in 1761 to enforce the 1733 Molasses Act, which required the colonists to purchase molasses and other goods from England.[105] However, England soon ran into a roadblock in the form of a group of Boston merchants and James Otis, who petitioned for a hearing to impede the writs' issuance.[106] It was Otis's arguments that inspired John Adams's creation of the structure of the modern Fourth Amendment.[107]

"The key issue" in the *Writs* case "was whether the Superior Court [of Massachusetts] should continue to grant [Writs of Assistance] in general and open-ended form, or whether it should limit the writs to "a single occasion based on particularized information given under oath."[108] In his legal arguments, Otis argued that English common law dictated that these general warrants, disguised as writs, were illegal and that specific and particular warrants were required instead to recover smuggled or stolen goods.[109] Specific warrants required their proponents to appear before a Justice of the Peace and state, under oath, the basis for the belief that smuggled goods would be found in a specific place.[110] If "probable cause was established, the justice would issue a warrant authorizing [the warrant proponent] to go with a constable to the specified place and, if the goods were found, to return [with] the goods and suspected felon before the justice, for . . . disposition of the matter."[111] Otis argued that, with writs, anyone

---

103 *See id.* at 1052.

104 *Id.* at 980-81.

105 McWhirter, *supra* note 54, at 27-30.

106 *Id.* at 30.

107 *See* Clancy, *supra* note 24, at 992-1006.

108 *Id.* at 992 (citing JOSIAH QUINCY, JR., REPORTS OF CASES ARGUED AND ADJUDGED IN THE SUPERIOR COURT OF JUDICATURE OF THE PROVINCE OF MASSACHUSETTS BAY, BETWEEN 1761 AND 1772 531-32 (1865)).

109 Clancy, *supra* note 24, at 993 n.88 (citing THOMAS HUTCHINSON, THE HISTORY OF THE PROVINCE OF MASSACHUSETTS BAY, FROM 1749 TO 1774 93-94 (1828)).

110 *See id.* at 993.

111 *See id.* at 990-91 (citing ADAMS, *supra* note 62, at 525).

"may enter [houses], may break locks, bars, and every thing in their way; and whether they break through malice or revenge, no man, no court, [could] inquire. Bare suspicion without oath [was] sufficient."[112]

Otis did not win the case, but his efforts were not in vain, as Otis's arguments encouraged those who opposed the government and illuminated the incompatibility of the Crown's practices with basic concepts of liberty.[113] Not only did Otis's arguments resonate with the common people, but they also resonated heavily with Otis's co-counsel, and the ultimate creator of the Fourth Amendment, John Adams.[114]

Years after the *Writs* case concluded, John Adams revived Otis's arguments against Writs of Assistance.[115] Adams used the precise language that Otis employed—in arguing that the Writs of Assistance should only be issued if they mirrored specific warrants—as the base of his draft of Article 14 of the Massachusetts Declaration of Rights, which preceded the Massachusetts Constitution.[116] Article 14 stated:

> Every subject has a right to be secure from all unreasonable searches, and seizures, of his person, his house, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.[117]

Not only did Article 14 prohibit general warrants, it also represented the first time a state constitution guaranteed citizens the right to be secure against unreasonable searches.[118] Clearly, Adams was con-

---

112 Clancy, *supra* note 24, at 1000.

113 *Id.* at 1002 (citing HUTCHINSON, *supra* note 109, at 94-95).

114 *See id.* at 1004 (quoting 3 DIARY AND AUTOBIOGRAPHY OF JOHN ADAMS 276 (L.H. Butterfield ed., 1961)).

115 *See id.* 992-1007.

116 *See* QUINCY, *supra* note 108, at 489 n.6; *Petition of Lechmere, Editorial Note*, in 2 LEGAL PAPERS OF JOHN ADAMS 125-32 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965).

117 MASS. DECLARATION OF RIGHTS OF 1780, art. XIV.

118 *See* Clancy, *supra* note 24, at 1027-29.

cerned not only with general warrants, but also with the scope of any search or seizure, with or without a warrant.

Adams's model eventually became the preferred format for the right to be protected from government intrusions, for the level of proof and the procedural requirements needed for a warrant to be legal, and for the phrasing of the Fourth Amendment's verbiage.[119] Although the historical records surrounding the Framers' and Colonies' adoption of the Fourth Amendment are fragmented and buried beneath deep discussions about the substance of the proposed Constitution, many state legislatures ratifying the Constitution were concerned not only with general warrants, but also with the broad power associated with unjustified searches and seizures, the unlimited power of new officers, and the protection of the home.[120]

Patrick Henry chiefly influenced including the Fourth Amendment in the Bill of Rights.[121] Regarding general warrants and searches without a warrant, Henry was concerned about tax collectors and other federal officers having the unrestrained ability to "go into your cellars and rooms, and search, ransack and measure, every thing you eat, drink and wear."[122] Henry argued that government officers "ought to be restrained within proper bounds."[123] Henry was also concerned that, pursuant to general warrants, "any man may be seized; any property may be taken, in the most arbitrary manner, without any evidence or reason. Every thing the most sacred, may be searched and ransacked by the strong hand of power."[124] James Madison, the drafter of the Fourth Amendment, aired similar concerns about general warrants, as the Necessary and Proper Clause could give Congress wide latitude to enforce general warrants in order to collect tax revenue or to enforce federal laws in general.[125]

Madison was also concerned with a citizen's right to be secure from unreasonable searches and seizures, in general; in his initial draft of the Fourth Amendment, he copied the structure and language that Adams used in Article 14 of the Massachusetts Declaration of

---

119 *Id.* at 1029.

120 *Id.* at 1031-33 nn.344-45, 347.

121 *See id.* at 1038-40.

122 *Id.* at 1039 (quoting Henry, *supra* note 4, at 1331-32).

123 *Id.*

124 *See* Clancy, *supra* note 24, at 1040 (quoting Henry, *supra* note 4, at 1474-75).

125 *See id.* at 1045-46 (quoting James Madison, Speech at the First Congress, First Session "Amendments to the Constitution" (June 8, 1789), *in* 5 THE WRITINGS OF JAMES MADISON 383-84 (Gaillard Hunt ed., 1904)).

Rights.[126] Eventually, the language of Madison's Fourth Amendment draft was modified, and later ratified by the thirteen Colonies, but Adams's structure of the Fourth Amendment remained intact.[127] Although the historical record is absent with respect to Madison's and other Framers' responses to the general right to be secure from unreasonable searches and seizures, the ratification of Madison's final draft of the Fourth Amendment gives rise to the inference that the Framers did, indeed, intend to supply protections against numerous broad acts of search and seizure. This inference is further supported by the fact that Madison's initial draft of the Fourth Amendment went through the Congressional Committee of Eleven,[128] which inadvertently omitted the right to be secure against unreasonable searches and seizures, and then was changed back to reflect its original language and structure.[129]

As the Fourth Amendment's historical roots show, the Amendment's adoption arose from the government's broad power to unjustifiably intrude into English and Colonial citizens' homes, persons, papers, and lives in general. James Otis, John Adams, James Madison, and many other Fourth Amendment influencers sought to protect against all types of general warrants and against all unjustified, warrantless intrusions into people's lives.[130] Unfortunately, this protection has not been carried out fully in today's world, as a new kind of general warrant currently exists in the form of the third-party doctrine.

Clearly, the Framers could not have foreseen the digitally interconnected world that modern citizens live in, with use of the internet,

---

126 *Compare* LASSON, *supra* note 59, at 100 n.77 (quoting 1 ANNALS OF CONG. 452 (1789)), *with* MASS. DECLARATION OF RIGHTS OF 1780, art. XIV. Madison's draft included the following: "The rights of the people to be secured in their persons, their houses, their papers, and their other property from all unreasonable searches and seizures, shall not be violated by warrants issued without probable cause, supported by oath or affirmation, or not particularly describing the places to be searched, or the persons or things to be searched."

127 *Compare* U.S. CONST. amend. IV., *with* MASS. DECLARATION OF RIGHTS OF 1780, art. XIV; *see also* Clancy, *supra* note 24, at 1047-48 (explaining that Madison changed Adams's employed new language and a different order of phrasing that language because Adams's model was a bit archaic).

128 Clancy, *supra* note 24, at 1047-48 (citing LASSON, *supra* note 59, at 100). The Committee of Eleven was the Committee that was made up of one member represented in Congress at the time as not all of the Thirteen Colonies had ratified the Constitution at this time.

129 *Id.* at 1047-48 (quoting and referring to 1 ANNALS OF CONG. 754 (1789) (Aug. 17, 1789 comments and motion of Mr. Gerry)).

130 *See* Clancy, *supra* note 24, at 980, 982, 1044-61.

social media, and other electronic communications. However, if the Framers were alive today, and were aware of the third-party doctrine's effects and the lack of prerequisites to its use, they would likely be taken aback, as the doctrine gives the government almost complete and unchecked power to gather information about a citizen upon the mere disclosure of information to a third party. In effect, the third-party doctrine is the modern-day equivalent of a general warrant. Therefore, history admonishes that this doctrine must be extinguished, and Fourth Amendment jurisprudence must revert back to its original roots, as established in *Katz v. United States*.[131]

II. WHAT IS THE THIRD-PARTY DOCTRINE, AND HOW DID IT COME TO FRUITION?

The third-party doctrine is a prophylactic rule of law created by the Supreme Court that prohibits a citizen from asserting an expectation of privacy in information voluntarily disclosed to a third party.[132] Under these circumstances, a government invasion of a person's privacy can never be found under the two-pronged *Katz* test[133] because, to find such an invasion of privacy, the second prong of the *Katz* test requires that society recognize an individual's subjectively exhibited expectation of privacy as "'reasonable.'"[134] In prior decisions, the Supreme Court has firmly stated "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[135] Thus, an unreasonable search cannot be found under the third-party doctrine because the Supreme Court merged the analysis of *Katz*'s second prong with the third-party doctrine.[136]

Regarding the policy supporting this broad and powerful doctrine, the Court has stated that people voluntarily disclosing such information "assume the risk" that the third party will share the dis-

131 389 U.S. 347 (1967).

132 *See* Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 985 (2016); Orin Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

133 *See* Orin Kerr, *supra* note 132, at 563.

134 *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

135 *See Smith*, 442 U.S. at 743-44 (citing United States v. Miller, 425 U.S. 435, 442-44 (1975)); Couch v. United States, 409 U.S. 322, 335-36 (1973); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Hoffa v. United States, 385 U.S. 293, 303 (1966); Lopez v. United States, 373 U.S. 427, 438 (1963)).

136 *See White*, 401 U.S. at 751-53.

closed information with the police or others.[137] Moreover, in its application, the doctrine does not distinguish how or through what intermediary a person discloses information to a third party; the mere act of disclosing information to a third party is sufficient to eviscerate any reasonable expectation of privacy a person has in his information, even if the information was disclosed in reliance upon it not being shared with anyone other than the recipient.[138] Once a person has disclosed information to a third party, regardless of the medium employed, the government can extract that information with almost complete impunity.[139] Therefore, under the *Katz* test, any collection of information disclosed to a third party could not be the subject of an unreasonable search under the Fourth Amendment.[140]

Regarding citizens' use of smartphones, social media, and other forms of electronic communication to convey private information to entrusted third parties in today's digitally interconnected world, this doctrine is extremely troublesome, as "any property may be taken, in the most arbitrary manner, without any evidence or reason. Every thing the most sacred, may be searched and ransacked by the strong hand of power."[141] To illustrate the third-party doctrine's oppressive effect, suppose that Megan used Facebook Messenger to send her friend, Alex, a message containing information meant for Alex's eyes only. Despite Megan's intent that her message be seen only by Alex, Megan's disclosure to Alex and, inadvertently, to Facebook renders

---

137 *E.g., Smith*, 442 U.S. at 744; *Hoffa*, 385 U.S. at 303; *Lopez*, 373 U.S. at 438.

138 Issacharoff, *supra* note 132, at 993-94, 1042-43 (citing Kerr, *supra* note 132, at 579-81).

139 *See* Slobogin, *supra* note 3, at 805-06 nn.5-8, 808-09 (explaining that document subpoenas are extremely easy to enforce because both subpoenas duces tecum and administrative subpoenas are subject to challenges of privilege, burdensomeness, and irrelevance). A challenge that succeeds based upon attorney-client privilege and the Fifth Amendment privilege against self-incrimination is rare because they're both usually unavailable. Succeeding based upon a relevance challenge is also rare because the standard of proof to enforce subpoenas duces tecum and administrative subpoenas are very broad. For example, in the federal grand jury context, subpoenas are quashed under irrelevance only if "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation." United States v. R. Enterprises, Inc., 498 U.S. 292, 301 (1991). Burdensome challenges asserting that assembling the records demanded by the subpoena is too expensive or laboring also "are almost always doomed to failure." WAYNE R. LAFAVE ET. AL., 3 CRIMINAL PROCEDURE 135 (2d ed. 1999). Fourth Amendment challenges rarely succeed as well because the *Miller* Court found that defendants cannot challenge governmental access to personal information possessed by third-party record holders due to the third-party doctrine. 425 U.S. at 444.

140 *See, e.g.*, *Miller*, 425 U.S. at 442-43; *Smith*, 442 U.S. at 743-44.

141 Clancy, *supra* note 24, at 1040 (quoting Henry, *supra* note 4, at 1474-75).

her expectation of privacy in that information extinguished.[142] Because Facebook has "seen" the Facebook message, the government can compel Facebook to disclose Megan's message because Megan has lost her privacy interest.[143]

The same logic can be extended to compel Megan's internet service provider (ISP) to disclose the message as well, even though the ISP's personnel have probably not examined the message, and the ISP is a mere conduit of information.[144] If Megan were subjected to a criminal trial, and the government sought to introduce evidence of this Facebook message to Alex, Megan would not have standing to challenge the message's admission because she forfeited her expectation of privacy.[145]

This "all-or-nothing" approach did not arrive overnight through Supreme Court precedent. The third-party doctrine's roots began with cases involving policemen who personally participated in a conversation with a suspect or indirectly participated through a "false friend" or third party.[146] "False friends" may use technology, like wires, to document and record conversations for the government to use in prosecuting suspects.[147]

The Supreme Court case, *On Lee v. United States*, was the first case in which the Court found that a conversation a suspect had with his former employee, which was simultaneously being listened to by a government agent, was not a search under the Fourth Amendment.[148] The Court supported its holding by finding that the suspect voluntarily gave information to a third party and, thereby, assumed the risk of that information being revealed to the police.[149] One succeeding

---

142 Peters, *supra* note 18, at 119-20.

143 *See* Rakas v. Illinois, 439 U.S. 128, 134 (1978) (holding that a defendant has standing under the Fourth Amendment to challenge government attempts to introduce evidence only when that defendant has a recognized expectation of privacy in the evidence seized); Slobogin, *supra* note 3, at 806 nn.5-8, 808-09.

144 Peters, *supra* note 18, at 119-20.

145 *See Rakas*, 439 U.S. at 133-38; Andrew J, DeFilippis, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1102 n.62 (2006); *see generally* Stephen P. Jones, *Reasonable Expectations of Privacy: Searches, Seizures, and the Concept of Fourth Amendment Standing*, 27 U. MEM. L. REV. 907, 909-12 (1997) (describing Fourth Amendment standing).

146 *See, e.g.*, On Lee v. United States, 343 U.S. 747, 753, 757 (1952); *Hoffa*, 385 U.S. at 302; *Lopez*, 373 U.S. at 438.

147 *See On Lee*, 343 U.S. at 753-54, 757.

148 *Id.* at 751.

149 *Id.* at 753-54.

"false friends" case before the Supreme Court was *Lopez v. United States*, in which the Court continued *On Lee*'s line of reasoning.[150] The Court found that an undercover agent's use of tape-recording equipment, which recorded a suspect's conversation with him, was also not a search because the information was voluntarily disclosed.[151] *Hoffa v. United States* continued this logic and broadly noted that "[n]either this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[152]

Katz v. United States came approximately a year after *Hoffa* was decided, and drastically changed the landscape of Fourth Amendment search jurisprudence.[153] In *Katz*, the suspect was making a phone call to his bookie in a public phone booth with the door closed.[154] The government attached an electronic recording device outside the booth to listen to the suspect's conversations with his bookie.[155] In downplaying the importance of physically trespassing on a constitutionally protected area, and focusing on the privacy interests of the individual, the majority opinion provided that "the Fourth Amendment protects people, not places . . . what a person . . . seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[156]

Although this broad holding recognized citizens' general entitlements to Fourth Amendment protection of their privacy in private or public areas, Justice Harlan's concurring opinion formed the test that determines what privacy interests deserve Fourth Amendment protection in public areas.[157] Justice Harlan's test requires that, to find a protected search, first "a person [must] have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be

---

150 *Id.* at 437-38.

151 *Id.* at 436, 439.

152 *Hoffa*, 385 U.S. at 302.

153 Peters, *supra* note 18, at 108 (citing Caren Myers Morrison, *The Drug Dealer, The Narc, and The Very Tiny Constable: Reflections on United States v. Jones*, 3 CALIF. L. REV. CIR. 113, 116 (2012); Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 827-28 (1994)).

154 *See* 389 U.S. at 348, 352.

155 *Id.*

156 *Id.* at 351.

157 *See id.* at 360-61 (Harlan, J., concurring).

one that society is prepared to recognize as 'reasonable.'"[158] Essentially, Justice Harlan's test requires an examination of whether a person subjectively intended to keep information private, and then whether societal norms would agree that the person's subjective intent was reasonable under the circumstances.[159]

In applying this test to the facts of *Katz*, Justice Harlan concluded that the suspect's act of shutting the phone booth door behind him, and thus closing the interior of the phone booth off to the public, exhibited a subjective expectation of privacy.[160] Society would also recognize this subjective expectation of privacy to be reasonable because, temporarily, the closed booth becomes a private place where a person should be able to assume that no one will intrude on his private conversations.[161] Although Justice Harlan's test was revolutionary at the time, it is slowly losing its power to protect citizens' privacy interests in a world of ever-emerging technology.[162] Following *Katz*, the Court had to deal with squaring the two-pronged *Katz* test with cases like *On Lee*, *Lopez*, and *Hoffa*, where suspects did not receive Fourth Amendment protection because they assumed the risk that their disclosed information could now be revealed to others.[163]

III. THE THIRD-PARTY DOCTRINE'S IMPACT ON THE *KATZ* TEST AFTER *WHITE V. UNITED STATES*

In *White v. United States*, the Supreme Court provided the steppingstone that merged the third-party doctrine in *On Lee*, *Lopez*, and *Hoffa* with the two-pronged *Katz* test.[164] *White* was another "false friends" case in which a suspect gave information to a third party who was recording their conversation.[165] However, this case was analyzed under the *Katz* test, and the Court did not find that the test was satisfied such that the recording could be considered a search.[166] The Court reasoned as it did in the prior "false friends" cases, and merged

158 *Id.* at 361.

159 *See id.*

160 Katz v. United States, 389 U.S. 347, 361 (1967).

161 *See id.*

162 *See, e.g.*, *Smith*, 442 U.S. at 741; *Miller*, 425 U.S. at 442; *White*, 401 U.S. at 747.

163 *Hoffa*, 385 U.S. at 302; *see also Lopez*, 373 U.S. at 436; *On Lee*, 343 U.S. at 753-54.

164 *See White*, 401 U.S. at 749 (quoting *Hoffa*, 385 U.S. at 302).

165 *Id.* at 746-47.

166 *See id.* at 748-49.

the policy supporting those decisions with the *Katz* test, stating the following:

> [H]owever strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent regularly communicating with the authorities. In these circumstances, no interest legitimately protected by the Fourth Amendment is involved, for that amendment affords no protection to a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.[167]

The reasoning in *White* set the Court on a path toward broadening the scope of the third-party doctrine to other disclosures to third parties. The Court did just that in *United States v. Miller*.

In *Miller*, the defendant was indicted on charges of tax fraud, among others, and the government attempted to admit his bank records as evidence.[168] The government subpoenaed Miller's banking institution to turn over his records, and Miller challenged the admission on the basis that his Fourth Amendment rights were being violated through the government's seizure of his private records.[169] In citing *White*, *Lopez*, and *Hoffa*, the Court found that, under the second prong of the *Katz* test, Miller had lost his expectation of privacy in the contents of those records by virtue of his disclosure to the bank.[170] The Court's broad statement solidified the third-party doctrine's vast power:

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[171]

---

167 *Id.* at 749 (quoting *Hoffa*, 385 U.S. at 302) (internal quotation marks omitted).
168 *See Miller*, 425 U.S. at 436.
169 *Id.* at 437, 442.
170 *Id.* at 443.
171 *Id.*

The Supreme Court employed this broad mandate again in *Smith v. Maryland*.[172] There, a pen register was installed at a phone company's office to identify who was calling the victim of a robbery and harassing her.[173] The pen register recorded the numbers that the suspect dialed at his home.[174] The Court limited its inquiry to whether the police violated the defendant's Fourth Amendment rights by gathering information from the phone numbers he dialed through the third-party phone company.[175] Under the *Katz* test, the Court found that society does not recognize a reasonable expectation of privacy in the phone numbers people dial.[176] In reaching its conclusion, the Court used *Miller* as support and stated, "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[177]

Following *Miller* and *Smith*, the third-party doctrine has become a "zero-sum game for citizens."[178] Citizens ultimately have two choices that dictate whether their private information is actually kept private from the powerful eyes of the government. Citizens can either keep their information completely to themselves or they can use a third-party servicer and, therefore, give up all Fourth Amendment rights to the information.[179] Through the third-party doctrine, the government does not need to follow any prerequisites in obtaining information conveyed through electronic transmission.[180] The government does not have to apply for a warrant, nor convince a magistrate to approve the issuance and execution of a warrant.[181] The government has free rein in taking any person's information, criminally charged or not, merely upon his usage of the internet.[182]

In this technological world, where consumers have little to no choice but to use technology to meaningfully participate in society, "consumers will be increasingly forced to waive their Fourth Amend-

---

172 *See Smith*, 442 U.S. at 744.
173 *Id.* at 737.
174 *Id.*
175 *See id.* at 742.
176 *See id.* at 742-44.
177 *Id.* at 743-44.
178 Peters, *supra* note 18, at 118.
179 *See id.* at 118-20
180 *See id.*
181 *See id.*
182 *See id.*

ment rights in order to obtain vital goods and services."[183] In the current technological climate, with the inevitable progression of further connecting people through third-party technology, and with the third-party doctrine flying in the face of the reasons the Fourth Amendment was originally adopted, the Supreme Court needs to abandon the third-party doctrine in its entirety and revive the *Katz* test to make case-by-case determinations regarding whether a person has exhibited an expectation of privacy, subjectively, and whether society would regard that expectation as reasonable.

If the Court does not adopt this test, or mandate sufficient safeguards to better protect consumers' data revealed to third parties, then the Court will continue to allow the government and police agencies to employ the modern-day equivalent of a general warrant. The Court will be repeating history. The history behind the adoption of the Fourth Amendment supports abolishing the third-party doctrine and its current application. Many dissenting Supreme Court opinions provide the insight necessary to do so.

IV. IS THE THIRD-PARTY DOCTRINE THE MODERN-DAY EQUIVALENT OF A GENERAL WARRANT?

The history of the Fourth Amendment's adoption, and many dissenting opinions penned by Supreme Court Justices, heavily support reviving the second prong of the *Katz* test and abandoning the third-party doctrine in its entirety.[184] The basic premise behind the Framers' adoption of the Fourth Amendment was to give citizens a broad

---

183 *Id.* at 118 (quoting Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 245-46 (2006)).

184 *See, e.g.*, *Smith*, 442 U.S. at 749-51 (Marshall, J., dissenting) (finding that "it does not follow that [a person] expect[s] [phone numbers dialed from his or her home] to be made available to the public in general or the government in particular" and fearing that the unrestricted application of the third-party doctrine will lead to "unregulated governmental monitoring"); *Miller*, 425 U.S. at 451 (Brennan, J., dissenting) (finding that because every person essentially needs a bank account, banks could give access to every person's bank information, which "opens the door to a vast and unlimited ranger of very real abuses of police power"); *White*, 401 U.S. at 756, 760-62 (Douglas, J., dissenting) (finding that electronic surveillance must be subject to its own Fourth Amendment search limits because "[e]lectronic surveillance is the greatest leveler of human privacy ever known," and the "use of electronic surveillance . . . uncontrolled, promises to lead us into a police state"); Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) ("[O]ur contemplation [of how to comport the Fourth Amendment with new technology] cannot be only of what has been, but of what may be. The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping") (internal quotation marks omitted).

right to be secure from all unreasonable searches and seizures.[185] Only when a governmental policing body met all the warrant requirements could that body have the constitutional authority to invade citizens' privacy and conduct searches and seizures of persons, property, and effects.[186] Although there are exceptions to these warrant requirements, the Framers designed the Fourth Amendment to prevent the use of general warrants against citizens of the United States and to give citizens minimum protections against arbitrary uses of police power.[187]

Throughout English and Colonial history, citizens fought against the Crown's enforcement of general warrants and Writs of Assistance.[188] Citizens and lawyers alike were enraged with the effects of executing these instruments, the intent to use them as ways around the English common law rule requiring a specific warrant in order to legally enter a person's home, and the power the Crown had to circumvent the procedure of obtaining a warrant.[189] The third-party doctrine's effects today parallel these warrants' effects in the past. These parallel effects are evident in the juxtaposition of Sir Edward Coke's fears about general warrants and modern concerns related to the National Security Agency's (NSA) telephony metadata collection program.

A. *The NSA's Metadata Collection Program's Relation to General Warrants*

In the 1600s, Coke feared the vast power that general warrants granted the Crown in allowing it to search a man's house without probable cause and then, through that search, find "cause enough" to incriminate him.[190] This is what the third-party doctrine currently allows, and what government and local police agencies do, through the expanses of the internet.[191] In 2001, President George W. Bush authorized the NSA to engage in a surveillance effort that amassed vast collections of data from millions of phone users to combat terror-

185 *See supra* notes 125-128 and accompanying text.

186 *See* U.S. CONST. amend. IV.

187 *See supra* note 185.

188 *See supra* notes 71-112 and accompanying text.

189 *See supra* notes 38-62 and accompanying text.

190 CUDDIHY, *supra* note 8, at 141 n.56 (Coke is quoted from a House of Commons debate transcript recorded on April 29, 1628).

191 *See infra* notes 192-278.

ism efforts, both domestically and abroad.[192] The NSA collected data similar to the pen register used in *Smith*, in that it collected the telephone numbers people dialed and the start time and duration of phone calls they made.[193] However, there is one large distinction between this NSA program and the pen register in *Smith*.[194]

The ongoing NSA program collects telephony metadata.[195] This data is collected from all phone calls made to and from United States numbers, and includes "telephone calling card numbers, trunk identifiers, International Mobile Subscriber Identity (IMSI) numbers, and comprehensive communication routing information."[196] Presumably, cell site location data—data determining the nearest cell tower a phone has been connected to—also falls under "telephony metadata."[197] Despite the depth and breadth of this data collection, few criminal indictments have resulted, according to current public information.[198] However, the case of *U.S. v. Moalin*[199] illustrates why

---

192 *See* Ellen Nakashima, *NSA's bulk collection of Americans' phone records ends Sunday*, WASH. POST (Nov. 27, 2015), https://www.washingtonpost.com/world/national-security/nsas-bulk-collection-of-americans-phone-records-ends-sunday/2015/11/27/75dc62e2-9546-11e5-a2d6-f57908580b1f_story.html?utm_term=.eebaf49c6d54.

193 *See* John Villasenor, *What You Need to Know about the Third-Party Doctrine*, THE ATLANTIC (Dec 30, 2013), http://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/.

194 *See infra* notes 195-197.

195 *See* Devin Coldewey, *NSA triples metadata collection numbers, sucking up over 500 million call records in 2017*, TECHCRUNCH (May 4, 2018), https://techcrunch.com/2018/05/04/nsa-triples-metadata-collection-numbers-sucking-up-over-500-million-call-records-in-2017/.

196 *See* Glen Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

197 *See id.*; United States v. Carpenter, 819 F.3d 880, 887-90 (finding that the government's collection of defendants' cell-site locational data was not a search under *Smith*).

198 *See* Marshall Erwin, *Connecting the Dots: Analysis of the Effectiveness of Bulk Phone Records Collection*, HOOVER INSTITUTE PRESS (Jan. 13, 2014), https://www.judiciary.senate.gov/imo/media/doc/011413RecordSub-Leahy.pdf; According to the New York Times, the NSA program generated thousands of tips in the months following 9/11 but virtually none panned out. Lowell Bergman, et al, *Domestic Surveillance: The Program; Spy Agency Data after Sept. 11 Led F.B.I. to Dead Ends*, N.Y. TIMES (Jan 17, 2006), at A1 (reporting how the NSA flooded the FBI with tips, virtually all of which were "dead ends or innocent Americans"). Seisint, a commercial data broker, claimed to have generated a list of 120,000 names with "High Terrorist Factor" (HTF) scores and that "scores of arrests" were made based on this information. The validity of these arrests, assuming they occurred, has not been corroborated, and the HTF feature was reportedly dropped because of concerns about privacy abuses. Brian Bergstein, *Database Measured "Terrorism Quotient*," AP (May 20, 2004), https://www.wfmynews2.com/article/news/ap-database-measured-terrorism-quotient/83-402381415.

199 United States v. Moalin, No. 10CR4246-JM, 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013).

Coke's fears about general warrants are still applicable and well founded today.

The facts in *U.S. v. Moalin* that gave rise to Basaaly Moalin's criminal indictment are sparse because that information is "classified" and "under seal" according to the Southern District of California.[200] However, the indictment indicates that Moalin was charged with conspiracy to provide money to al-Shabaab, a violent and brutal militia group in Somalia designated by the United States Department of State as a foreign terrorist organization.[201] From late 2007 to early 2008, Moalin was in direct telephone contact with Aden Hashi Ayrow, a prominent military leader of al-Shabaab.[202] This information came to light through the NSA program.[203] Ayrow requested money from Moalin, and Moalin then coordinated fund-raising efforts and money transfers with three other co-defendants in the case.[204] The defendants were charged with crimes relating to aiding terrorist organizations.[205]

Although the defendants were convicted and had convincing evidence presented against them,[206] Coke's fears still materialized in this case. Moalin's telephony data was seized and compiled under the NSA program, and that search was found to be lawful under the Fourth Amendment through the application of the third-party doctrine.[207] After searching his telephone records, the government did "find cause enough" in that Moalin had direct telephone communications with the leader of a terrorist organization.[208] This fact likely allowed the government to pry into the contents of those phone calls and to find the following piece of evidence: "On or about April 12, 2008, Ayrow told defendant MOALIN by telephone that 'it is the time to finance the jihad.'"[209] In effect, the third-party doctrine allowed

---

200 *See id.* at *1-4.

201 Second Superseding Indictment, United States v. Moalin, No. 10CR4246-JM, 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013), at *1-2, *6-7 (June 6, 2012) [Hereinafter *Indictment*].

202 *Id.* at *6-7.

203 *Moalin*, 2013 WL 6079518 at *3.

204 *Indictment*, *supra* note 201, at *7.

205 *Id.* at *3, *8-11.

206 *See* Moalin, 2013 WL 6079518, at*1-3.

207 *Id.* at *5-6.

208 *Id.* at *3.

209 *Indictment*, *supra* note 201, at 7.

the government to access all of Moalin's telephony metadata, without a warrant, and to then use it against him.[210]

Although it can be argued that the use of the NSA's program was justified in *Moalin*, the bigger concern is that the NSA can access telephony metadata from *anyone* in the United States and abroad for an *indefinite* period of time, and it can store innocent people's information to potentially use it against them later.[211] Using this data, the government can go on a fishing expedition and make assumptions about a person based upon who that person called, how long that person spoke on the phone, and where the listener was located.[212]

A study conducted by the Privacy and Civil Liberties Oversight Board in 2014 found that the NSA could retrieve "billions of records per day" before Edward Snowden revealed the program's existence in 2013.[213] Despite congressional action taken to curb the NSA's vast power in collecting this metadata, the Agency was still able to collect 151 million phone records in 2016.[214] Moreover, the amount of telephony metadata collected by the NSA is vast compared to the number of known indictments arising from the metadata, which suggests that the program does more harm to citizens' privacy than it does to combat terrorism and other crimes.[215]

Justice Sotomayor's concurring opinion in *United States v. Jones* highlights the pervasive and perverse effects that the government's collection of this type of data can have on citizens' privacy.[216] In the context of the government placing a GPS tracking device on an automobile over a four-week period, Justice Sotomayor's fears about the collection of information through GPS and other technology also speak to the data the NSA has been collecting for over a decade.[217]

---

210 *See Moalin*, 2013 WL 6079518 at *4-8.

211 *See supra*, notes 192-209 and accompanying text.

212 *See* Lori Andrews & Jake Meyer, *NSA Spying Violates First and Fourth Amendments*, ON THE EDGES OF SCIENCE AND LAW, (June 11, 2013), http://blogs.kentlaw.iit.edu/islat/2013/06/11/nsa-spying-violates-first-and-fourth-amendments/.

213 *See* James Vincent, *NSA collected 151 million phone records in 2016, despite surveillance law changes*, THE VERGE (May 3, 2017, 4:22 AM), https://www.theverge.com/2017/5/3/15527882/nsa-collecting-phone-records-us-citizen-metadata (citing PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *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*, (Jan. 23, 2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf).

214 Andrews, *supra* note 212.

215 *See supra*, notes 195, 198, 212 and accompanying text.

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

217 *See id.*

Justice Sotomayor's concerns in *United States v. Jones* were expressed in 2012, even before Edward Snowden revealed the existence of the NSA's program in 2013.[218] In the third paragraph, Justice Sotomayor begins her opinion, widely cited in support of dismantling the third-party doctrine, by criticizing the long-term monitoring of suspects.[219] She states, "'longer term . . . monitoring in most investigations of most offenses impinges on expectations of privacy.'"[220] Similar to the data collected by the NSA, Sotomayor stated about GPS data, "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations . . . The Government can store such records and efficiently mine them for information years into the future."[221] The NSA has engaged in such conduct and continues to do so today.[222]

Justice Sotomayor articulates her distrust of the government's vast surveillance power by stating:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."[223]

Chief Justice Pratt's opinions in *Entick v. Carrington* and in *Wilkes v. Wood* expressed similar concerns about governmental practices associated with general warrants, as he feared that "such a power would be more pernicious to the innocent than useful to the public."[224] He

---

218 *See* Barton Gellman, Aaron Blake, & Greg Miller*, Edward Snowden comes forward as source of NSA leaks*, WASH. POST (June 9, 2013), https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?utm_term=.ba77a5055518.

219 *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

220 *Id.* (quoting 565 U.S. at 430 (Alito, J., concurring).

221 *Id.*

222 *See* Vincent, *supra* note 213.

223 *See Jones*, 565 U.S. at 416 (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

224 *See Entick*, 19 How. St. Tr. at 1073; *Wilkes*, 98 Eng. Rep. at 498.

also asserted "it is too much for [magistrates] without such authority to pronounce [the issuing and execution of a general warrant] legal, which would be *subversive of all the comforts of society*."[225] Chief Justice Pratt pronounced that if the power to issue general warrants continued to exist, then "it certainly [may] affect the person and property of every man in this kingdom, and is *totally subversive of the liberty of the subject*."[226]

In her concurring opinion, Justice Sotomayor did not stop at explaining her fears about the government's employment of technological surveillance techniques.[227] She continued by stating that she would

> take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the *sum of one's public movements* . . . whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.[228]

Paralleling English and Colonial fears of the Crown employing general warrants, Justice Sotomayor continued,

> I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power and prevent "a too permeating police surveillance."[229]

Regarding the third-party doctrine, and relating even more closely to the NSA's metadata program, Justice Sotomayor opined:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to

---

225 *Entick*, 19 How. St. Tr. at 1066 (emphasis added).

226 *Wilkes*, 98 Eng. Rep. at 498 (emphasis added).

227 *See Jones*, 565 U.S. at 416.

228 *Id.*

229 *Compare id.* at 416-17 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)), *with* Vincent *supra*, note 213 (showing that the NSA continued to collect records about Americans' phone calls despite the USA Freedom Act, which was intended to curb bulk surveillance).

> the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a perquisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[230]

Before the Supreme Court granted *certiorari* in *Jones*, the D.C. Circuit Court of Appeals examined the case—then called *United States v. Maynard*—and took a different approach known as the "mosaic theory."[231]

The mosaic theory considers that "[d]isparate items of information, though individually of limited or no utility to their possessor, can take on added significance *when combined with other items of information*."[232] The *Maynard* court found that "[w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene,"—i.e., the government.[233] Exactly in line with Justice Sotomayor's fears, the *Maynard* court noted that from the knowledge attained from this broad picture of people's private data, "all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, . . . an unfaithful husband, . . . an associate of particular individuals or political groups—and not just one such fact about a person, *but all such facts*."[234] These expressions from the *Maynard* court,

---

230 *Jones*, 565 U.S. at 417-18 (Sotomayor, J., concurring) (internal citations omitted).

231 *See* United States v. Maynard, 615 F.3d 544, 561-62 (2010) (showing that the mosaic theory is the theory that the aggregation of data creates a "mosaic," or broad picture, in which the whole of the data examined from a broad view reveals more than the sum of its parts).

232 Issacharoff, *supra* note 132, at 1000 (quoting David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act,* 115 YALE L.J. 628, 630 (2005)).

233 *See Maynard*, 615 F.3d at 562 (quoting CIA v. Sims, 471 U.S. 159, 178 (1985)).

234 *Compare id.* at 562 (emphasis added), *with Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

from Justice Sotomayor, and from the historical fears of general warrants are sharpened not only by the NSA's program, but also by the police's use of a method aimed at deterring future crime called data mining.

B. *Data Mining's Relation to General Warrants*

Data mining is a process by which governmental agencies and private entities discover patterns in large data sets through intelligence methods that utilize machine learning, statistics, and database systems.[235] The overall goal of data mining is to extract information from a data set and transform it into an understandable structure for further use, primarily by both law enforcement agencies and the government.[236] In addition to being analyzed, the information is stored in a database and subject to data management aspects, data pre-processing, model and inference considerations, gauges for the level of interest in the information, visualization, and online updating of information.[237] Calling this process "data mining" is misleading because the overall goal is recording patterns and extracting knowledge from large amounts of data, not the mining of the data itself.[238]

The actual data mining task involves the semi-automatic or automatic analysis of larger quantities of data to extract previously unknown, notable patterns—such as groups of data records, unusual records, and dependencies of targets.[239] These patterns are considered a summary of the data inputted and are then used in subsequent analysis for tasks such as machine learning or, more importantly, predictive analytics.[240] To illustrate, the data mining stage may identify multiple groups of people in the data. The groups can then be used to obtain more accurate predictions of people's behaviors by a computer predicting what types of behaviors these people specifically, or as a group, may engage in next.[241] In all, data mining is a task that compiles information from commercial and public sector resources—

---

235 *See* Liane Colonna, *A Taxonomy and Classification of Data Mining*, 16 SMU SCI. & TECH. L. REV. 309, 309-14 (2013).

236 *See* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 312-23 (2008).

237 *See* Colonna, *supra* note 235, at 315-17.

238 *See id.* at 310-11.

239 *See id.* at 318-19.

240 *See id.* at 320-21.

241 *See* Slobogin, *supra* note 236, at 317-23.

banking and financial intuitions, real estate accounts, education details, retail sales information, social services information, transportation, use of the mail system, and hospitality and lodging transactions—to optimize the collection, analysis, and sharing of information on individuals to predict their next mode of behavior.[242]

Local police departments and governmental agencies around the country have been employing data mining methods to predict future instances of crime since the early 2000s, and the third-party doctrine permits this technique.[243] However, this practice has been met with stern opposition from the American Civil Liberties Union (ACLU) and many others because it not only accesses citizens' private information, but it also chills First Amendment rights to free speech and discriminatorily targets minority groups.[244] For example, in 2014, 2015, and 2016, the Boston Police Department (BPD) utilized a data mining program called Geofeedia in an effort that, it claimed, would help deter future crime stemming from "public unrest" in Baltimore and from the Black Lives Matter protests in Ferguson, Missouri.[245]

According to a 2016 ACLU study on the document requests relating to the BPD's use of Geofeedia, and 62 other departments' use of similar technology, the BPD used this system primarily to target black and Muslim protestors and gathered thousands of posts about political and social activism, religious issues, and other personal matters irrelevant to criminal investigatory matters.[246] The BPD was not the only police department to employ Geofeedia's or similar providers' services, as a report by the Brennan Center for Justice at the NYU School of Law showed that nearly all large cities, and many

---

242 *See id.* at 323.

243 *See id.* at 317-19, 329-31.

244 *See, e.g.*, Natasha Singer, *Data Privacy, Put to the Test*, *N.Y. Times* (Apr. 30, 2011), https://www.nytimes.com/2011/05/01/business/01stream.html; Dell Cameron, *Dozens of police-spying tools remain after Facebook, Twitter crack down on Geofeedia*, THE DAILY DOT (Oct. 11, 2016, 1:33 PM), https://www.dailydot.com/layer8/geofeedia-twitter-facebook-instagram-social-media-surveillance/; Bousquet, *supra* note 3); Nasser Eledroos & Kade Crockford, *Social Media Monitoring in Boston: Free Speech in the Crosshairs*, PRIVACY SOS, https://privacysos.org/social-media-monitoring-boston-free-speech-crosshairs/; Chris Perez, *Boston Cops used social media to spy on black, Muslim protestors: ACLU*, N.Y. POST, (Feb. 7, 2018, 7:58 PM), https://nypost.com/2018/02/07/boston-cops-used-social-media-to-spy-on-black-muslim-protesters-aclu/; Guynn, *supra* note 12.

245 *See id*; Eledroos, *supra* note 244.

246 *See* Guynn, *supra* note 12; Eledroos, *supra* note 244 (*citing* City of Boston Purchase Order, PRIVACY SOS, https://privacysos.org/geofeedia-files-boston-police-social-media-surveillance/ (last visited Aug. 26, 2018).

smaller ones, have significantly invested in social media monitoring tools like Geofeedia.[247]

Not only did Geofeedia (and other similar programs) gather posts made publicly, but it also collected the locations of social media users, generally, and gathered when they made specific posts;[248] targeted hashtags like #MuslimLivesMatter, #DontShoot, and #blacklivesmatter;[249] targeted posts with the key words "ISIS" or "Ferguson" when the contexts of those posts were jokes, criticisms of policing efforts, or discussions about current events;[250] and even successfully circumvented Facebook's privacy settings to gather the content of private posts and the locations of their authors.[251] Specifically, Geofeedia encouraged police departments to make dummy Facebook or Twitter accounts that were, in reality, fake profiles depicting provocative pictures of attractive women to lure in suspects as friends or followers.[252] This, in turn, enabled police to track social media users' locations across social media sites, regardless of whether their location was publicly or privately revealed.[253]

Snaptrends is another program that made promises to circumvent Twitter users' efforts to hide their locations.[254] By the summer of 2014, hundreds of federal and local law enforcement agencies were using this program as well.[255] A crime analyst from the Phoenix Police Department in Arizona claimed that Snaptrends sent the analyst an email promising that the program has "exclusive access to Twitter back end[.]"[256] Lexis Nexis, a popular legal database, offered a similar program called "Digital Stakeout."[257] Regarding Digital Stakeout,

247 Bousquet, *supra* note 3 (citing *Maps: Social Media Monitoring by Police Departments, Cities, and Counties*, BRENNAN CENTER FOR JUSTICE (Apr. 5, 2017), https://www.brennancenter.org/analysis/map-social-media-monitoring-police-departments-cities-and-counties).

248 *See* Bousquet, *supra* note 3.

249 *See id.*

250 *See id.*; Eledroos, *supra* note 244.

251 *See* Cameron, *supra* note 244 (discussing how Geofeedia's goal was to bypass the privacy services, particularly those involving locational data, offered by social media sites like Facebook).

252 *See* Bousquet, *supra* note 3.

253 *Id.*

254 *See id.* (explaining that Snaptrends, a tool similar to Geofeedia, creates fake profiles to track social media site users' location regardless of if the users publicly geotag their posts).

255 *See* Cameron, *supra* note 244.

256 *See id.*

257 *Id.*

one police officer from Osceola County, Florida said that he was sold on this service because of its "ability to monitor your undercover accounts."[258] However, he admitted that he and his department "did not expect the amount of data [they] would get," adding that "the amount of data . . . [was] overwhelming and we don't have an analyst specifically assigned to do social media only."[259]

The ACLU's report found no evidence that the social media mining led to any arrests or prompted further investigations.[260] However, the report did find that records received from the BPD about Geofeedia in particular showed "that police social media surveillance systems, operated in the dark without any public scrutiny, [were] likely to treat people as inherently suspicious based on their race, religion, or ethnicity, or because they are politically active, without advancing public safety or criminal investigations."[261] Exactly this happened to a man named Robert McDaniel in Chicago in 2013.[262]

Using a similar kind of data mining technique as Geofeedia, the Chicago Police Department (CPD) generated a "heat list," or "an index of the roughly 400 people in the city of Chicago supposedly most likely to be involved in violent crime."[263] Information contained within the CPD's crime database—including that about crime "hotspots" where crimes have occurred in the past, disturbance calls and calls regarding suspicious persons, arrest and conviction records, and relationships to other violent people—informs this list.[264] From this information, the CPD's partnership with a predictive analytics group from the Illinois Institute of Technology (IIT) in Chicago allows the group to "generate crime maps that highlight neighborhoods of the city that might soon be at risk of an uptick in crime."[265] This practice triggers the mosaic theory concerns from Justice Sotomayor's concurring opinion in *Jones*, and the *Maynard* court's concerns in that same

---

258 *Id.* (internal quotation marks omitted).

259 *Id.* (internal quotation marks omitted).

260 *See* Crockford, *supra* note 244.

261 *Id.*

262 *See* Matt Stroud, *The Minority Report: Chicago's New Police Computer Predicts Crime, But is it Racist?* THE VERGE (Feb. 19, 2014), https://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist.

263 *See id.*

264 *See id.*

265 *See id.*

case, because the map reveals intimate details to police regarding targets and makes assumptions that may be improper.[266]

In Robert McDaniel's case, although he had never been convicted of a violent crime and had not interacted with a police officer recently before his visit from police, he lived in a neighborhood well known for violence.[267] As a result, he fit within the parameters of the CPD's crime map and heat list algorithms.[268] Mr. McDaniel received a visit from a CPD police commander at his front door with the following message: "if you commit any crimes, there will be major consequences. *We're watching you*."[269]

What goes into these algorithms, besides the information indicated above, and how they make assumptions about who should be included within the crime map and heat list, is currently unknown.[270] This raises concerns similar to those surrounding Geofeedia and the like.[271] Do these roughly 400 people appear on this heat list because they live in violent parts of Chicago? Can being arrested or picked up in violent areas for nonviolent crimes put a person on this list when he, perhaps, should not be on the list? Does a person appear there because of her race or ethnicity? Or just because she is friends with violent, or potentially violent, people? The IIT team's leader said that the algorithm also "ranks" people based upon "their chance of becoming involved in a shooting or homicide."[272] Commander Steven Caluris of the CPD made it clear, though, that "[i]f you end up on that list, there's a reason you're there."[273]

---

266 *Compare* Stroud, *supra* note 262 ("But the jury's still out about whether Chicago's heat list and its other predictive policing experiments are worth the invasions of privacy they might cause and the unfair profiling they could blatantly encourage"), *with Jones*, 565 U.S. at 416 (Sotomayor, S., concurring) ("The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society'").

267 *See* Stroud, *supra* note 262.

268 *See id.*

269 *See id.*

270 *See id.* ("*The Verge* filed a Freedom of Information Act request with the CPD to obtain the heat list itself and attempt to use that list as a way to independently answer some . . . questions. The request was denied because sharing that information could 'endanger the life or physical safety of law enforcement personnel or any other person,' according to a letter from the CPD's Office of Legal Affairs.").

271 *Compare* Stroud, *supra* note 262, *with* Bousquet, *supra* note 3.

272 *See* Bousquet, *supra* note 3.

273 *Id.*

To calm fears that this algorithm perpetuates and intensifies racial profiling by police, the IIT team's leader expressed that their predictive analysis is novel and that his team is "attempting to evaluate the risk of violence in an unbiased, quantitative way."[274] However, with what has been revealed about Geofeedia's similar practices, the CPD and IIT team's attempt to evaluate the risk of violence in Chicago is likely not unbiased.[275]

In response to the ACLU's 2016 report, Facebook, Instagram, and Twitter promised to cut off social media mining companies, like Geofeedia and Snaptrends, from access to their websites' back-end data.[276] However, regardless of Facebook, Instagram, and Twitter cracking down on Geofeedia and Snaptrends, other similar police spying tools still remain in police possession.[277] Therefore, it is reasonable to conclude that the third-party doctrine's existence, and police departments' ability to apply it to prevent crime, remain alive and well.

Before the general public knew data mining and similar police spying tools existed, legal scholars feared that, from the Supreme Court's adoption of the third-party doctrine, "it [would] not [be] farfetched for government officials to amass data for use in silencing or attacking enemies, critics, undesirables, or radicals."[278] Some worried the doctrine would prevent courts "from using the Fourth Amendment as a tool to limit government misbehavior."[279] Clearly, these fears have been manifested in data mining and in the NSA's metadata program.[280] Not only have these fears been manifested, but the Crown's purposes in effectuating general warrants, stemming from the 1500s to the 1700s, have resurfaced as well.[281]

---

274 *Id.*

275 *See supra* notes 272, 245.

276 *See* Bousquet, *supra* note 3.

277 *See* Singer, *supra* note 244.

278 *See* Issacharoff, *supra* note 132 (citing Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy,* 75 S. CAL. L. REV. 1083, 1112 (2002)).

279 *See id.* (citing Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent,* 81 MICH. L. REV. 1229, 1272 (1983) ("[The Fourth Amendment] has been restricted so much that it fails to offer innocent citizens the protection to which they should be entitled under the fourth amendment.").

280 *See supra* notes 192-278 and accompanying text.

281 *See supra* notes 38-62 and accompanying text.

Queen Elizabeth's and King James's motives in using general warrants were primarily to silence dissenters.[282] The Crown continued to employ these same warrants and Writs of Assistance in the 1700s to ransack people's homes, to take their most private writings and possessions with impunity, and, in effect, to silence criticisms of the Crown and control its constituents' behavior.[283] The third-party doctrine's allowance of programs like the NSA's metadata collection and data mining have empowered the federal and state governments, along with local municipalities and their police departments, to silence dissenters and to chill rights to free speech—as well as eviscerated people's right to keep private information secure from prying government eyes—just like the Crown's use of general warrants.[284]

Chief Justice Pratt's concerns that general warrants' effects would be "subversive to all comforts of society" and "subversive of the liberty of the subject [of the general warrant]" have also been revived by the third-party doctrine.[285] John Dunning's fears that the power stemming from general warrants was "extremely mischievous" and "productive of great Oppression" ring true as well.[286] And, most importantly, James Otis's and John Adams's reservations about the effects of general warrants have been resurrected, but now in the form of the government being able to "enter" or access a person's private information without any constitutionally-mandated prerequisites.[287] Still, now, as then, "Bare suspicion without oath is sufficient."[288]

CONCLUSION

In effect, by keeping the third-party doctrine alive, the Supreme Court has allowed the United States to repeat history and has allowed the government to employ modern-day general warrants to search and seize any and all content stored on the internet or generated through

---

[282] *See supra* notes 10, 23, 25 and accompanying text.

[283] *See supra* notes 24, 56-62, 70-109, 283 and accompanying text.

[284] *See supra* notes 192-278, 284 and accompanying text.

[285] *Compare Entick*, 19 How. St. Tr. at 1066, *with Wilkes*, 98 Eng. Rep. at 498, *and Jones*, 465 U.S. at 415-18 (Sotomayor, J., concurring).

[286] *Compare Leach*, 19 How. St. Tr. At 1003-04, 108, *with supra* notes 192-278 and accompanying text.

[287] *See supra* notes 109-12, 115-18 and accompanying text.

[288] *Compare supra* note 112, *with supra* notes 167-183 and accompanying text.

the use of technology.[289] Data mining and the NSA's telephony metadata collection program are prime examples of parallel negative effects, as the third-party doctrine currently imposes upon citizens the same abuses that general warrants did in the past.[290] The parallels between the third-party doctrine and general warrants are further highlighted in Patrick Henry's fears that the Constitution did not contain a prohibition against the use of general warrants. Henry wrote that, without such a prohibition, "[A]ny property may be taken, in the most arbitrary manner, without any evidence or reason. Every thing the most sacred, may be searched and ransacked by the strong hand of power."[291]

Thus, as technology continues to transform and strengthen the connections between people and entities, the Supreme Court must establish additional safeguards to prevent the government from being able to search and seize citizens' information kept on the internet or conveyed to third parties for specific purposes. Abolishing the third-party doctrine altogether—and reviving the second prong of the *Katz* test to make case-by-case determinations of reasonable societal expectations of privacy—may be the Court's best solution to this problem. Not all revelations on the internet or to third parties deserve protection under the Fourth Amendment, but the current "all or nothing" effect of applying the third-party doctrine cannot continue to exist in today's digital age. If the Court does not adopt this Article's approach, or impose other limits on the third-party doctrine's reach, then the Court will continue to allow the government to employ the modern-day equivalent of general warrants—and it will continue to repeat history.

---

289 *Compare supra* notes 24-117 and accompanying text, *with supra* notes 167-278 and accompanying text.

290 *Compare supra* notes 24-117 and accompanying text, *with supra* notes 192-278 and accompanying text.

291 *Compare supra* notes 121-124 and accompanying text, *with supra* notes 167-278 and accompanying text.