Justice Action Center
Student Capstone Journal
Project No. 11/12-02

The Third Party Doctrine in the Digital Age

John P. Collins
New York Law School
Class of 2012

The Third Party Doctrine in the Digital Age

By John P. Collins

I. Introduction

The digital age is upon us. Information is our most valued commodity, and communications occur electronically in real time. A side effect is that those digital communications are copied, transferred, and stored by any number of intermediaries that handle those communications between point A and point B. Cellular phone companies, internet service providers, cable providers, and an untold number of websites collect and store information about their users. Under the third party doctrine, those users have no "reasonable expectation of privacy"[1] in the information their service providers collect. The third party doctrine, a controversial exception to the Fourth Amendment's warrant requirement, is an oft-criticized but highly influential doctrine that has shaped the evolution of privacy rights over the last forty years. But the march of technology has taken this doctrine beyond its use. Further, the continued adherence to the third party doctrine poses an immediate threat to the right of the American people to be free from government intrusion. The Supreme Court has opened the door for a challenge to the third party doctrine. At the same time, Congress is developing legislation to further entrench the fruits of that doctrine into law. The Fourth Amendment now stands upon a precipice, whereby an exception may swallow its protections whole. If the people are to retain their right to security in their houses, persons, papers and effects, then the third party doctrine must be replaced with a more realistic approach to the Fourth Amendment.

[1] United States v. Miller, 425 U.S. 435 (1976).

The Supreme Court's recent decision in *United States v. Jones* brought the third party doctrine back into the spotlight.[2] The defendant in *Jones* challenged the constitutionality of attaching a GPS tracking device to an automobile for an extended period of time without a warrant.[3] While the Court ultimately decided that the GPS device constituted a trespass, the third party doctrine loomed large in the background.[4] GPS tracking information, of course, is relayed to many types of modern technology, including OnStar, vehicle GPS map tools, and many cellular phones. Under the third party doctrine, the government could obtain the same information via subpoena that the court barred them from obtaining through an attached GPS device. Justice Sotomayor, concurring in the court's judgment, addressed this issue, and indicated an opportunity to reconsider the third party doctrine:

> 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 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. Perhaps, as JUSTICE ALITO notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," and perhaps not. 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 prerequisite 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.[5]

---

[2] United States v. Jones, 565 U.S. ___, Docket no. 10-1259 (2012).
[3] *Id.*
[4] *Id.*
[5] United States v. Jones, 565 U.S. _, Docket no. 10-1259 (2012) (Sotomayor, J., concurring).

This eloquent summation identifies many of the issues regarding the third party doctrine in modern society. This first part of this paper will explain the origins of the Fourth Amendment and the third party doctrine. The second part will identify the key ways in which the doctrine violates the rights enshrined in the Fourth Amendment. The third part will explore the proposed solutions to the modern problems facing the third party doctrine, and why those solutions are inadequate to meet the issue at hand. Finally, this paper will suggest alternative approaches to restore the substantive guarantees of the Fourth Amendment, and assess the practical likelihood of each.

II. Background/Origin

To properly understand the third party doctrine, we start with the origins the Fourth Amendment, ratified as part of the original bill of rights in 1791.[6] While English common law recognized what we now refer to as the "castle doctrine,"[7] even this narrow protection was often disregarded in the colonies, where general warrants were the norm.[8] In the period leading up to the American Revolution, British taxation of the colonies was often a source of controversy, and the colonists went to great lengths to avoid the duties and excises on imported goods through smuggling.[9] To combat this growing problem, the British passed the Excise Act of 1754, which granted customs officials sweeping powers of interrogation and inspection under a writ of assistance.[10] Essentially, this allowed customs inspectors to investigate and seize untaxed goods

[6] *See Bill of Rights is Finally Ratified*, HISTORY.COM, http://www.history.com/this-day-in-history/bill-of-rights-is-finally-ratified (last visited June 18, 2012).
[7] *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH.L. REV 547, 642 (1999).
[8] *See* James Otis, *Against Writs of Assistance*, NAT'L HUMANITIES INST., http://www.nhinet.org/ccs/docs/writs.htm (last visited June 18, 2012).
[9] *See* George H. Smith, *Americans with Attitudes: Smuggling in Colonial America*, LIBERTARIANISM.ORG (Dec. 6, 2011), http://www.libertarianism.org/publications/essays/excursions/americans-attitudes-smuggling-colonial-america.
[10] Paul Boyer, *Borrowed Rhetoric: The Massachusetts Excise Controversy of 1754, 21* WM. & MARY QUARTERLY 3RD, 328-351 (Jul., 1964), available at http://www.jstor.org/stable/10.2307/1918450.

at will, and it was not long before the colonists became openly hostile to this invasive practice. After unsuccessfully challenging the general warrant practice in court,[11] the colonists took it upon themselves to actively thwart the enforcement of these general warrants.[12] The British government continued to insist upon their validity,[13] an issue that played a key role in the start of the American Revolution.[14]

By 1776, war with Britain was inevitable. Virginia issued its Declaration of Rights, drafted by James Madison and George Mason,[15] which included a particularity requirement and an evidentiary basis for suspicion of criminal activity in order to issue a warrant.[16] In 1780, Massachusetts ratified its own constitution, including a warrant clause that required specificity and evidence supported by an oath, and included the language about "unreasonable searches and seizures" that still permeates our Fourth Amendment jurisprudence today.[17] Following the ratification of the Constitution, the Fourth Amendment was added with the rest of the Bill of Rights in 1791. The text of the Fourth Amendment reads as follows:

> 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.[18]

---

[11] *Id.*; *See* James Otis, *supra* note 8.
[12] In 1765, a group of colonists, later known as the Sons of Liberty, began destroying the homes and threatening the lives of public officials tasked with enforcing taxes. *See* EDMUND S. MORGAN, PROLOGUE TO REVOLUTION 104-126 (University of N.C. Univ. Press 1973) (1959).
[13] *See The Townshend Revenue Act*, U.S. HISTORY.ORG, http://www.ushistory.org/declaration/related/townshend.htm (last visited May 3, 2012).
[14] *See* BERNARD BAILYN, IDEOLOGICAL ORIGINS OF THE AMERICAN REVOLUTION (Harvard Univ. Press 1992).
[15] THE VIRGINIA DECLARATION OF RIGHTS (1776), http://www.constitution.org/bcp/virg_dor.htm (last visited May 3, 2012). It is worth noting that George Mason refused to sign the Constitution because it did not contain a Bill of Rights. Stephen A. Schwartz, *George Mason: Forgotten Founder, he Conceived the Bill of Rights*, SMITHSONIAN MAGAZINE (May 2000), *available at* http://www.smithsonianmag.com/history-archaeology/mason-abstract.html.
[16] *Id.*
[17] MASS. CONST. art. XIV.
[18] U.S. CONST. amend. IV.

The third party doctrine emerged from the court 180 years later. Cases in the interim often relied on the concept that information revealed to third persons was not considered private. A number of cases explicitly recognized that the Fourth Amendment did not protect information an individual voluntarily disclosed to another person, which came to be called the third party doctrine.[19] Soon after, the court expanded the use of this doctrine in two cases, *United States v. Miller*[20] and *Smith v. Maryland.*[21] These two cases laid the framework for applying the third party doctrine to modern technology.

In *Miller*, the defendant was prosecuted for tax fraud stemming from his whiskey bootlegging operation.[22] The Supreme Court upheld evidence gathered from a financial institution via subpoena under the Bank Secrecy Act, because the defendant had no Fourth Amendment interest in the bank's records.[23] This case is often cited as the source of modern problems with the third party doctrine for a number of reasons. In *Miller*, the Court upheld the government's power to force banks to retain customer information for law enforcement purposes, holding that there was no expectation of privacy for information "voluntarily" revealed to a business entity for a limited purpose. The fact that the bank was compelled to collect and retain that information, and that the defendant was required to disclose it in order to use the bank's services, was irrelevant to the majority.[24] *Miller* was the first case to uphold the practice of mandatory data retention by corporate entities, and by declaring that data outside the purview

[19] *See* Lopez v. United States, 373 U.S. 427 (1963); United States v. White, 385 U.S. 206 (1966); Hoffa v. United States, 385 U.S. 293 (1966).
[20] United States v. Miller, 425 U.S. 435 (1976).
[21] Smith v. Maryland, 442 U.S. 735 (1979).
[22] *Miller*, 425 U.S. at 435.
[23] *Id.*
[24] *Id*.

of the Fourth Amendment, the court took the first step in a series of changes that significantly eroded the privacy protections that American citizens used to enjoy.[25]

Smith v. Maryland dealt with phone company retention of pen registries.[26] The defendant was charged with robbery and making obscene phone calls, and sought to suppress the list of phone calls made from his home, which were recorded without a warrant.[27] The twist in this case related to the fact that the phone company automated the process of recording previously dialed phone numbers. The significance of this decision was not readily apparent, but by expanding the third party doctrine to include information revealed to a machine carrying out a routine task, the court laid a foundation that would drastically expand the reach of the third party doctrine upon the advent of the internet.[28]

The next decades brought a number of statutes that sought to re-assert the right to privacy in recorded information that the court was unwilling to recognize. This includes the Privacy Act of 1974[29] (later amended by the Computer Matching and Privacy Act of 1988[30]), and, in the context of internet communications, the Electronic Communications Privacy Act,[31] a statute that itself has been oft-criticized as unworkable in the context of modern society.[32] While these statutes take steps to protect the privacy of stored information in a number of contexts, they do precious little to protect against government intrusion in the context of law enforcement.[33] There

[25] *Cf.* Boyd v. United States, 116 U.S. 616, 631-632 (1886) ("any compulsory discovery. . .compelling the production of his private books and papers, to convict him of crime, or to forfeit his property, is contrary to the principles of a free government.").
[26] *Smith*, 442 U.S. at 735.
[27] *Id*.
[28] Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581 (2011).
[29] *Id.*
[30] *Id.*
[31] 18 U.S.C. § 2510 (2008).
[32] *See, e.g.*, *ECPA Reform: Why Now?* DIGITALDUEPROCESS.ORG, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.
[33] *Id.*; Tokson, *supra* note 28.

are significant exceptions for law enforcement to obtain this otherwise protected information, and those procedures do not necessarily require a warrant.[34] On a more fundamental level, however, the fact remains that whatever privacy rights an individual might have in their electronic documents are granted via statute, rather than guaranteed by the Constitution. These rights can be modified, repealed, or circumvented in any number of ways, and as a result the protections they offer are mostly illusory. More importantly, this approach raises questions about the remedy when law enforcement violates these rights. The Court often takes the position that suppressing this evidence is unnecessary and the proper remedy can be found in a civil suit.[35]

While the Supreme Court has generally upheld the current framework, whereby any privacy interests in electronic data are of a statutory nature and not subject to Fourth Amendment protection, that approach not universal. Eleven states have explicitly rejected the third party doctrine, and a number of others have indicated their willingness to part from such reasoning.[36] Additionally, the Sixth Circuit recently upheld the reasonable expectation of privacy in the case of *United States v. Warshak*.[37] In *Warshak*, the court suppressed the substantive content of emails revealed to the police under the Stored Communications Act (SCA).[38] The court distinguished between information transferred to the intended recipient from the intermediary who delivers it, thereby avoiding the third party doctrine and applying the traditional *Katz* reasonable expectation of privacy test.[39] The court further held that the SCA is unconstitutional to the extent that it allows ISPs to reveal e-mail content to law enforcement on any standard

[34] *See* 18 U.S.C. § 2703 (2008).
[35] *See*, *e.g.*, United States v. Banks, 540 U.S. 31 (2003).
[36] Stephen Henderson, *The Timely Demise of the Third Party Doctrine*, 96 IOWA L.REV. BULLETIN 39 (2011), *available at* http://www.uiowa.edu/~ilr/bulletin/ILRB_96_Henderson.pdf (last visited May 3, 2012).
[37] United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
[38] *Id.*
[39] Katz v. United States, 389 U.S. 347 (1967).

lower than the probable cause requirement of a warrant.[40] The *Warshak* case was the first instance of a federal appeals court recognizing a legitimate expectation of privacy in e-mail. While it would have been preferable to overturn *Miller* (or in the author's opinion, *Smith*), the mere application of Fourth Amendment analysis to an email retrieved from an internet service provider marked a significant change from the traditional third party doctrine approach, and opened the door for the court to re-establish the Fourth Amendment's substantive protections in the digital world.

III. Problems with the Third Party Doctrine

At this point it is important to draw a distinction between the types of parties with access to electronic communications in the context of the third party doctrine. The most common distinction, advanced by Professor Henderson and the Sixth Circuit Court of Appeals, is to distinguish between courier and intended recipient.[41] Others, such as Professor Kerr, distinguish between "secret agents" and "business records."[42] I contend that the proper approach is to distinguish between information revealed to natural third persons, and information revealed to an automated electronic intermediary. The latter portion of the third party doctrine is the real concern of the digital age, and this author concedes that attempting to enforce privacy rights in information revealed to natural third persons is both unworkable and outside the purview of the Fourth Amendment.[43] The *Smith* case held that there was no significance to the fact that the process was automated, as the same information would have been disclosed to a human operator

[40] *Warshak*, 631 F.2d 266.
[41] Henderson, *supra* note 36.
[42] Orrin Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 563 (2008).
[43] Professor Erin Murphy is a critic who advocates for a total repeal of the third party doctrine and would allow individuals to assert a Fourth Amendment right in information disclosed to natural third parties, and suggests alternating theories of third party waiver, sliding scale protections, and heightened standards of voluntariness. While interesting, these solutions are unworkable in practice, and would likely result in *less* Fourth Amendment protection, as qualified immunity will shield officers who violate these complex and hazy classifications. *See* Erin Murphy, *The Case Against the Case for the Third Party Doctrine*, 24 BERKELEY TECH.L.J. 1239 (2009).

absent the automated process.[44] Whatever credence one might put in such logic, it is clearly inapplicable in today's digital society, wherein both the quantity and depth of information provided via electronic means place such electronic communications well outside the scope of any human ability at retention. In other words, the would-be telephone operator in *Smith* may have been able to recall the phone numbers dialed by the defendant had the process not been automated, but there is no human equivalent in the context of the internet. These electronic communications would not be manually transferred by human beings absent automation; without an automated process, these communications would be impossible. Ultimately, the point is that whether it was a wax seal, a closed envelope, or a beheading after delivery, the messenger had never been privy to the message before the advent of digital technology. But because information revealed to the third parties carries no expectation of privacy (regardless of whether the third party is a human being or a machine), and because modern intermediaries necessarily copy the information in the process of transferring it to its recipient, the net effect is that an electronic intermediary has the right, and in some cases the duty, to record and store the contents of communications and disclose them law enforcement upon request.[45]

The fact that email systems automatically copy the content of the communications they transfer does not require providers to store those communications indefinitely. For a time, technology acted as a self-referencing check upon such data, as the cost and impossibility of storing such information made discoverable evidence limited. The SCA itself provides different standards depending on how long the information has been stored, affording less protection for information an ISP retained for more than 180 days.[46] Today, the existence of such a distinction

[44] Smith v. Maryland, 442 U.S. 735 (1979).
[45] Kerr, *supra* note 42.
[46] 17 U.S.C. § 2701.

should be *prima facie* evidence that the statute has outlived its usefulness. Ever-expanding data storage capacity, combined with increased efficiency (lower prices), results in ISPs that can essentially store electronic data indefinitely. It has become so inexpensive to store this data that the digital information industry has made a push toward "cloud computing." Here, information is retained by the provider on its own private servers, and is only transferred to the user when it is necessary.[47] As remote data storage becomes the norm, it is time to question whether the third party doctrine and the SCA approach to electronic data communications remains workable.

Another set of issues raised by the evolution of this doctrine are the awkward distinctions the court now relies on to decide cases. For example, the SCA distinguishes between intercepted data and data retrieved from storage,[48] a remnant of a prior incarnation of wiretap and pen registry cases in the context of telephones. This same holdover reasoning from an earlier technology distinguishes between content and destination information.[49] While the content of the website you visit may be protected, the web address you enter into your browser to reach that website is not, just as a phone conversation may be protected while the phone number dialed is not. Such distinctions seem arbitrary and poorly thought out, and with good reason, as they are antiquated distinctions from an antiquated technology, and no longer carry any relevance.

The practical concerns stemming from this theoretical boondoggle have important real world implications. Whatever logical justification the government may have for its current approach to electronic information, the result is a standing general warrant for every American citizen. That includes bank and tax records, electronic data, web browsing history, cellular phone contents, medical records, and any number of categories of otherwise private information

[47] *See* Rivka Tadjer, *What is Cloud Computing?*, PC MAGAZINE ONLINE, http://www.pcmag.com/article2/0,2817,2372163,00.asp (Last visited June 18, 2012).
[48] O'Brien v. O'Brien, 66 N.Y.2d 576 (1985).
[49] *Id.*

that, through either legal mandate or functional necessity, are stored and maintained in electronic records by government and private entities alike. Today, 230 years after Virginia passed its Declaration of Rights, we have effectively returned to the writ of general assistance, whereby a government authority may obtain an impossibly broad amount of information on nothing more than a subpoena. While under *Warshak*, viewing the content of emails may require a warrant, it is hard to imagine a scenario where the destination of the communication will not be sufficient to establish probable cause to sustain a warrant for its content. This reduces the warrant requirement to a mere procedural hurdle, rather than a substantive protection of individual rights.

Finally, there remains the fundamental flaw of the reasoning in *Miller*. Information disclosed to a bank, internet service provider, or a cellular phone carrier, as a prerequisite to obtain those services, is considered to be disclosed "voluntarily" under *Miller* and its progeny. But as society and government increasingly rely on these intermediaries to transact day-to-day business, the argument that these disclosures can be avoided by simply not utilizing the related services loses whatever credibility it once had. One could, theoretically, never hold a bank account or own a cellular phone, never purchase a television, and only access the internet from public places, and have a reasonable chance of maintaining privacy. But for anyone born in the last fifty years, such an approach is functionally impossible. Without a credit score, email address, or cellular phone, it is impossible to access most government services, to say nothing of a job or an education. Continuing to label these transactions as "voluntary" may serve the orderly administration of justice (and make life easier on both law enforcement and the courts), but they offer cold comfort to a new generation of Americans who today find their Fourth Amendment right to privacy mutually exclusive to their Fifth Amendment rights to life, liberty and property. There was a time when the Court thought these rights to be hopelessly

intertwined,[50] but today's court presents us with a Morton's fork, as we must sacrifice our privacy rights to meaningfully participate in society.[51]

Perhaps the greatest problem posed by this interpretation of the Fourth Amendment is the advantage prosecutors may gain during the plea bargaining process in criminal cases. Because the Constitution guarantees a trial but not a plea offer, these agreements are offered at the discretion of the prosecutor. If that prosecutor has access to a broad range of private, personal data about the accused, there is no reason to believe that the information will not be used as leverage in the plea bargaining process, regardless of the relationship between the information and the alleged crime. Because of this, society should consider exactly how much power the third party doctrine vests in the prosecutor. For example, what might one plead to in order to prevent the disclosure of their sexual orientation? We recently saw a young man, barely 20 years old, commit suicide over the public disclosure of his homosexually.[52] An extramarital affair? The John Edwards trial provided ample evidence of the lengths people will go to keep such information a secret.[53] An embarrassing act? Eight members of the secret service were dismissed solely based on the fear of potential extortion arising out of their interactions with prostitutes in Columbia, when such conduct was not even illegal there.[54] It is not hard to imagine a defendant pleading guilty to a crime he did not commit because the prosecutor threatens to reveal sensitive information during the trial. While people like Professor Kerr may

---

[50] Boyd v. United States, 116 U.S. 616 (1886).

[51] A "Morton's fork" is a choice between two equally unpleasant alternatives. The term originated with John Morton, who collected taxes on behalf of Henry VII. *Morton's Fork Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/morton's+fork.

[52] *See* Geoff Mulvihill, *Ex-Rutgers Student Convicted of Hate Crime, Invasion of Privacy in Webcam Spying Case*, HUFFINGTON POST (Mar. 17, 2012), http://www.huffingtonpost.com/2012/03/16/ex-rutgers-student-convic_n_1353591.html.

[53] *See* Kim Severson, *Edwards Trial on Campaign Finance Begins*, N.Y. TIMES (Apr. 23, 2012) http://www.nytimes.com/2012/04/24/us/jury-selection-in-john-edwards-trial-set-to-begin.html.

[54] *See* Laurie Kellman, *Washington delicate about Secret Service Scandal*, BOSTON.COM (Apr. 23, 2012) http://articles.boston.com/2012-04-24/news/31393548_1_secret-service-military-personnel-prostitutes.

argue that there is no reason to believe the prosecutor will use information such as this in an inappropriate manner, others would respond that anyone who trusts the apparatus of criminal law enforcement to exercise self-restraint has never been on the receiving end of its scrutiny. The founders were keenly aware of that scrutiny, and we ignore them at our peril.[55]

IV. Proposed Solutions – and Why They Won't Work

As society grows more dependent on digital communications in daily life, the third party doctrine has received a great deal of criticism.[56] While not without its supporters,[57] the flawed logic of the third party doctrine draws the ire of many scholars, just as the flawed results it produces draws the ire of the general public. The problem is a complicated one, and the proposed solutions to the third party doctrine create problems of their own, both in theory and in practice. Additionally, there is always the problem of the proper remedy, even if the Fourth Amendment applies to information revealed to automated third parties in the future. Whatever compromise is ultimately reached, the solutions proposed thus far are all fatally flawed, and for one reason or another are unlikely to correct problems with the third party doctrine.

For example, professor Orren Kerr, an outspoken proponent of the third party doctrine, believes the problem is a theoretical one, and that if the third party doctrine was viewed as a search with consent instead of a non-search, whatever problems remained would be self-

[55] Warden Md. Penitentiary v. Hayden, 387 U.S. 294, 316 (1967) ("A List of Infringements and Violations of Rights' drawn up by the Boston town meeting late in 1772 alluded to a number of personal rights which had allegedly been violated by agents of the crown. The list included complaints against the writs of assistance which had been employed by royal officers in their searches for contraband. The Bostonians complained that 'our houses and even our bed chambers are exposed to be ransacked, our boxes, chests, and trunks broke open, ravaged and plundered by wretches, whom no prudent man would venture to employ even as menial servants."(quoting ROBERT RUTLAND, THE BIRTH OF THE BILL OF RIGHTS 25 (Collier Books, 3rd ed., 1955)).
[56] Henderson, *supra* note 36.
[57] Kerr, *supra* note 42.

correcting.[58] Kerr further argues that other legal protections such as entrapment, the First Amendment, internal governmental agency regulations and statutory protections offer adequate privacy protections in the absence of the Fourth Amendment.[59] But this argument misses the underlying point, and evinces the shortcomings of an academic approach to such a practical doctrine. The Fourth Amendment is a substantive, fundamental right to security in the house, person, papers, and effects of each citizen.[60] By reducing these fundamental rights to a series of situational statutory guarantees, it leaves the right to privacy subject to the will of the legislature, rather than outside of its purview. The idea that "internal agency regulations"[61] are an adequate substitute for an inalienable right guaranteed by the Constitution should be so self-evidently flawed as to not require elaboration. These alternatives only exist as long as Congress deems them to be wise policy, whereas recognizing the right to privacy for what it is, a fundamental right guaranteed by the Constitution since the adoption of the Bill of Rights, ensures these protections in perpetuity.

Professor Stephen Henderson and other opponents of the third party doctrine, fail to address the fundamental issues that surround this doctrine in the modern world. Professor Henderson, in announcing the demise of the third party doctrine,[62] designs a four-part test as a substitute for today's third party doctrine:

> (1) The initial transfer of the information from the person to a third party is reasonably necessary to participate meaningfully in society or is socially beneficial, including to freedom of speech and association;
> (2) The information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma if disclosed, and

[58] *Id.* at 589.
[59] *Id.*
[60] U.S. CONST. amend. IV.
[61] Kerr, *supra* note 42 at 594.
[62] Henderson, *supra* note 36.

> whether outside of the initial transfer to a third party it is typically disclosed only within one's close social network, if at all;
> (3) The information is accessible to and accessed by nongovernment persons outside the institution; and
> (4) Existing law restricts or allows access to and dissemination of the information or similar information.[63]

The flaws of this test are readily apparent. The first factor relies on a reasonability assessment; the second upon a judge's estimation of how likely certain information is to be disclosed outside of one's "close social network"; the third factor is a restatement of the inevitability exception to the warrant requirement, and the fourth factor makes the Fourth Amendment contingent upon statutory law. In short, Henderson proposes that we eliminate the third party doctrine entirely, and replace it with a watered down version of the *Katz* test. Even as he declares the third party doctrine's demise, he seeks to replace one form of judicial discretion with another.[64] While every fundamental right is, at some level, subject to the whims of the judge interpreting that right at a given time, there is little security in rendering that right dependent on a judge's estimate of the likelihood that one might disclose certain information outside of their "close social network," regardless of how that term may be defined.

Matthew Tokson, another opponent of the third party doctrine who is willing to distinguish between disclosing information to human beings and machines, also accepts without question the concept of a "reasonableness" assessment based on societal expectations of privacy.[65] As *Katz* and its progeny illustrate, in practice, the "societal expectations of privacy" means whatever five Supreme Court justices decide society expects.[66] But society is not made

---

[63] *Id.* at 50.
[64] *Id.*
[65] Tokson, *supra* note 28.
[66] For example, squeezing a bag to determine its contents violates the Fourth Amendment, United States v. Bond, 529 U.S. 334 (2000), but if it contains garbage it does not, Ca. v. Greenwood, 486 U.S. 35 (1988). Smelling a bag to determine its contents does not violate the Fourth Amendment, which is apparently how officers make that distinction prior to searching the bag. Ill. v. Caballes, 543 U.S. 405 (2005). One man's junk is another man's

up of sixty-six year old graduates of Harvard and Yale Law School. It is hard to imagine a group of people less able to estimate the "reasonable expectations of society" than the members of the Supreme Court; the very fact that they sit upon the Supreme Court should be evidence enough that they have long since parted ways with the average American citizen. While the justification for this reasonableness test is judicial flexibility, there is a notorious absence of holdings that find a once unreasonable expectation has become reasonable, though there are numerous cases that reach the opposite result.

In essence, these commentators suggest either continuing on the current path, or removing the third party doctrine and reverting to some version of the *Katz* test for reasonableness. But the third party doctrine is merely shorthand for the premise that society will not recognize a reasonable expectation of privacy in information disclosed to third parties. Whether unreasonable as a matter of law or unreasonable after a *Katz* analysis, whatever changes these proposals might garner will be found in the body of the decision rather than the outcome of the case. Unless we recognize the Fourth Amendment for what it is, a substantive guarantee of security in a citizen's house, person, papers and effects,[67] the end result of any of these proposed solutions is that the guarantees of the Fourth Amendment are determined at the discretion of the court. On a theoretical level, if such a right was intended to be in the hands of the government, there would be no need to enumerate it in the Bill of Rights. On a practical level, the right to privacy should not be left in the sole discretion of the government, both because they will not, and because they cannot, protect it.

---

treasure, but society only recognizes privacy in the treasure. Pottinger v. City of Miami, 810 F.Supp. 1551, 1556 (S.D.Fl. 1992). And while it is unreasonable for people to assume they are secure from aerial surveillance on their property due to the prevalence of commercial flight, CA v. Ciraolo, 476 U.S. 207 (1986), the populace can rest assured that the Constitution prevents the government from learning what time the lady of the house takes her bath. Kyllo v. United States, 533 U.S. 37 (2001). This parade of horribles continues *ad infinum* throughout our Fourth Amendment jurisprudence.

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

Who will protect the right to privacy? The judiciary has no reason to do so—it only makes their jobs more difficult. Heavy enough is the weight of overseeing a criminal trial. Judges are loathe to suppress otherwise relevant evidence due to a procedural fault in the investigation process.[68] The Supreme Court has repeatedly held that civil claims are the proper remedy for violations of the Fourth Amendment.[69] Even Justice Scalia, the great advocate of Originalism,[70] feels that a remedy for Fourth Amendment violations should not be suppression.[71] Instead, the Justice tells us, the appropriate remedy for the violation of a fundamental right enshrined in 1791,[72] is a civil claim under a statute enacted in 1871,[73] as long as the qualified immunities of a 1960s-era statute do not interfere.[74] In Scalia's world, the police may violate a suspect's Fourth Amendment rights at their convenience, and can remedy those violations by crediting that suspect's prison commissary after sentencing. While this approach may be appealing for its efficiency, it offers little freedom from unreasonable searches and seizures. One wonders what happened to the Scalia who once declared of our criminal justice system, "it has never been efficient, but it has always been free."[75]

The suppression of evidence as a remedy raises a serious problem for judges, as the result of a Fourth Amendment suppression hearing is often outcome determinative. There is simply no motivation for a judge to suppress otherwise relevant evidence, Fourth Amendment or not. This is not an accusation of bad faith on the part of the judiciary; in fact, it is their misplaced

[68] *See* Hudson v. Michigan, 547 U.S. 586 (2006).
[69] *See e.g,.* Wilson v. Arkansas, 514 U.S. 497 (1995).
[70] Justice Scalia does not believe that exclusion is a proper remedy for violations of the Fourth Amendment, and believes that suppression is a judicially created remedy. For a detailed history of Fourth Amendment remedies, see Roger Roots, *The Originalist Case for the Fourth Amendment Exclusionary Rule*, 45 GONZ. L. REV. 1 (2010).
[71] *See, e.g.,* David Oscar Markus, *"Why don't we just abolish the exclusionary rule?"*, SOUTHERN DISTRICT OF FLORIDA BLOG (Mar. 21, 2011), http://sdfla.blogspot.com/2011/03/why-dont-we-just-abolish-exclusionary.html.
[72] U.S. CONST. amend. IV.
[73] 42 U.S.C. § 1983.
[74] *See* Ashcroft v. Al-Kidd, 131 S. Ct. 2074 (2011) (government officials entitled to qualified immunity as long as they do not violate clearly established law).
[75] Apprendi v. New Jersey, 530 U.S. 466 (2000) (Scalia, J., concurring).

good faith that drives the denial of this right. Judges seek to decide cases fairly and accurately, and that task is hard enough when considering all relevant information. Suppression makes the judge's job more difficult, and makes the outcome of the case less accurate. Why would the court ever enforce the Fourth Amendment in the face of such a Hobson's choice? Any judge fool enough to consider enforcing the Fourth Amendment in the face of an otherwise guilty defendant need look no further than Justice Harold Baer to see what fate awaits them if they try.[76]

The legislature presents similar hurdles. Congress is tasked with the regulation of commerce and collecting taxes, and that task is often directly at odds with the right to privacy. The Fourth Amendment was born out of resentment over the overzealous tools of the tax man, and it makes little difference whether the tax collector is from the federal government or the British Empire.[77] When given the choice between carrying out their duties and respecting the Fourth Amendment, it is foolish to expect Congress to choose the latter, which is why the Fourth Amendment was written.[78] The Supreme Court explicitly (though inadvertently) acknowledges as much in *Couch v. United States,* which holds that tax records provided to an accountant carry no expectation of privacy. In finding the Fourth Amendment inapplicable to the accountant's records, Justice Powell tells us that the Fourth Amendment does not protect the people from the

[76] In a rare act of bi-partisanship, both political parties called for Justice Baer's ouster after he suppressed evidence in a high profile drug case, holding that the police lacked reasonable suspicion to stop the vehicle. United States v. Bayless, 201 F.3d 116 (2000); *see* Don Van Natta, *Judge Takes Himself Off Drug* Case, N.Y. TIMES, May 17, 1966 at 1.

[77] The disdain for general warrants was so prevalent during the founding period that it was the only specific example used by James Madison to prove the necessity of adding the bill of rights to the Constitution. James Madison, Speech Introducing the Bill of Rights (June 8, 1789), *available at* http://teachingamericanhistory.org/library /index.asp?document=111.

[78] Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 316 (1967) ("'The officers of Congress may come upon you now, fortified with all the terrors of paramount federal authority. Excisemen may come in multitudes; for the limitation of their numbers no man knows. They may, unless the general government be restrained by a bill of rights, or some similar restriction, go into your cellars and rooms, and search, ransack, and measure, everything you eat, drink, and wear. They ought to be restrained within proper bounds.'" (Quoting Patrick Henry)).

tax collector, because it would interfere with the system Congress developed for "collection of the revenues."[79]

The executive branch is tasked with enforcing the criminal law, and no further explanation for its disdain for the Fourth Amendment is necessary. Skeptics need to look no further than the National Security Agency (NSA), who recently refused to tell the Senate how many Americans have been monitored under the Foreign Intelligence Surveillance Act. Inspector General Charles McCullough refused to investigate the query, claiming that disclosing the scope of NSA surveillance "would itself violate the privacy of U.S. persons."[80]

The Fourth Amendment highlights a flaw in our system of checks and balances. Of the three branches of government, no single branch has a reason to enforce the rights the guaranteed by the Fourth Amendment, nor does any branch have a reason to check the infringement of the Fourth Amendment by another. And why would they? These are the same public officials who are under intense media scrutiny, and the Fourth Amendment does not operate on the journalists who investigate them. Whatever privacy elected officials retain is protected by state secrets, statutory immunity, and various other laws applicable only to government officials. They do not rely on the Fourth Amendment, and experience shows that they cannot be relied upon to protect the privacy of American citizens.

Perhaps this is a symptom of a deeper problem, often cited by proponents of digital privacy: the legislators writing these laws, and the judges enforcing them, simply do not understand the technology they are dealing with. From Senator Ted Steven's famous quote

[79] Couch v. United States, 409 U.S. 322, 336 (1973).
[80] Spencer Ackerman, *NSA: It Would Violate Your Privacy to Say if we Spied on You*, WIRED (June 18, 2012, 6:29 PM), http://www.wired.com/dangerroom/2012/06/nsa-spied/.

about a "series of tubes,"[81] to the Supreme Court's reliance on doctrines of trespass to decide *Jones*, it is unclear whether public officials understand the technology they are addressing, the long term effects of their decisions, or the stakes involved when those decisions are made. Even Clarence Thomas, who steadfastly proclaimed at his confirmation hearing, "I will not allow this committee or anyone else to probe into my private life. This is not what America is all about"[82] has consistently rejected privacy claims under the Fourth Amendment.[83] Ironically, the same man who was indignant when accused of abusing his station for sexual gratification stood alone in holding that it was reasonable for a school administrator to strip-search a student at the age of sexual maturity, based solely on another student's confidential accusation that she was distributing contraband ibuprofen.[84] Worst of all may be Justice Posner of the Seventh Circuit, who tells us that some Fourth Amendment violations, such as searching the numbers in a cellular phone, are so "minimally intrusive" that they are not entitled to a remedy.[85] If these are the stalwarts of our Fourth Amendment privacy rights, then it is no wonder the people are seeking extra-judicial remedies to restore the right to privacy.

The United States was founded on the principle that the people must take it upon themselves to enforce their natural rights when the government fails to do so, in what John

---

[81] *See Series of Tubes*, WIKIPEDIA (last visited May 3, 2012), http://en.wikipedia.org/wiki/Series_of_tubes.
[82] CLARENCE THOMAS, MY GRANDFATHER'S SON 264 (Harper Collins 2007).
[83] *See* Board of Education v. Earls, 536 U.S. 822 (2002); Samson v. California, 547 U.S. 843 (2006); City of Indianapolis v. Edmond, 531 U.S. 32 (2000).
[84] Safford v. Redding, 557 U.S. 364 (2009) (Thomas, J., dissenting); *cf.* CLARENCE THOMAS, MY GRANDFATHER'S SON 270 (Harper Collins 2007) ("How would any member on this committee, or any person in this room, or any person in this country like sleaze said about him or her in this fashion, or this dirt dredged up, and this gossip and these lies displayed in this manner?").
[85] United States v. Flores-Lopez, No. 10-3803, 2012 U.S. App. LEXIS 4078 (7th Cir. Feb. 29, 2012). Judge Posner also tells us that the probable cause standard only applies to warrants, whereas warrantless searches only need be reasonable, in a breathtaking display of revisionist history that assume the power to search without a warrant is the historical rule, rather than a mid-20th century judicially created exception to the warrant requirement. This is the same Judge Posner who decries the use of the "judicial remedy" of exclusion because it is inconsistent with our Constitution's history. *See* RICHARD POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN TIME OF EMERGENCY 171 (Oxford Univ. Press 2006).

Locke described as an appeal to heaven.[86] The hacker collective Anonymous, and various other actors who seek to steal, pervert, compromise, and otherwise destroy stored data, may represent the first steps toward such an appeal—a modern-day Sons of Liberty.[87] Active resistance to new laws, such as the Stop Online Privacy Act (SOPA), reveal a populace motivated to protect its privacy rights.[88] But this is no match for a motivated Congress. It took only a month for Congress to pass an alternate bill granting largely the same powers, under the guise of "cyber security" rather than copyright infringement.[89]

Rather than address the fundamental privacy concerns that SOPA raised, the Cyber Intelligence Sharing and Protection Act (CISPA) simply grants immunity to ISPs for the negative effects of their information sharing.[90] On receiving immunity, large companies like Facebook and Google either fell in line or fell silent, and the bill easily passed in the House of Representatives.[91] While the President has promised to veto the bill, it remains to be seen if he will follow through on that promise; those familiar with the controversial NDAA legislation passed in January know this promise is far from reliable.[92] Even if CISPA does not make it out of the Senate, Congress is committed to legislating on this subject, and it will eventually find the votes to get it done. These legislative efforts make it clear that Congress has no interest in protecting privacy, regardless of the will of the people. It remains to be seen if the current

---

[86] "Whenever any form of Government becomes destructive of these ends, it is the Right of the People to alter or abolish it." THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776); *see also* John Locke, *Second Treatise of Civil Government*, (1690) *available at* http://www.constitution.org/jl/2ndtreat.htm.
[87] Otis, *supra* note 8.
[88] Larry Magid, *SOPA and PIPA Defeat: People Power or Corporate Clout?,* FORBES (Jan. 31, 2012, 10:40 AM), http://www.forbes.com/sites/larrymagid/2012/01/31/sopa-and-pipa-defeat-peoples-power-or-corporate-clout/.
[89] Violet Blue, *Say Hello to CISPA, it Will Remind You of SOPA*, CNET NEWS (Apr. 13, 2012, 7:35 AM), http://news.cnet.com/8301-1023_3-57413627-93/say-hello-to-cispa-it-will-remind-you-of-sopa/.
[90] *Id.*
[91] Louis Peitzman, *CISPA Passes House*, GAWKER (Apr. 26, 2012) http://gawker.com/5905584/cispa-passes-house.
[92] Erik Kain, *President Obama signed the National Defense Authorization Act – Now What?*, FORBES (Jan 2, 2012), http://www.forbes.com/sites/erikkain/2012/01/02/president-obama-signed-the-national-defense-authorization-act-now-what/.

American populace is willing to take the same steps to protect their rights that the founding generation took to obtain them.

Unsurprisingly, the government, and the large ISPs tasked with monitoring the internet for "security threats," may prove the greatest threat of all. According to former US cyber security chief Richard Clarke, every major US company has been compromised and raided for their protected data.[93] Clarke's statements, and events like the theft of six weeks' worth of emails from the U.S. Chamber of Commerce in 2010,[94] make it clear that the government lacks the ability to protect our privacy, even if they had the desire to do so. One must question the wisdom of granting private corporations carte blanche powers to monitor and share this sensitive information with the government, when all of these entities have proven incapable of protecting that information.

V. Alternative Approaches

The obvious solution to this problem to is simply to restore the substantive guarantees of the Fourth Amendment. As Professor Kerr tells us, one of the greatest benefits to the third party doctrine is its simplicity as a bright line rule.[95] But the Fourth Amendment also provides a bright line rule; the government needs a warrant in order to search or seize the "houses, persons, papers and effects" of the general populace. By recognizing electronic communications as "papers" and sensitive personal information such as social security, banking and other business records as "effects," the Supreme Court would take great steps toward restoring the privacy protections of

---

[93] Chris Nerney, *Former cybersecurity czar: Every major U.S. company has been hacked by China*, IT WORLD (MAR. 27, 2012) http://www.itworld.com/security/262616/former-cybersecurity-czar-every-major-us-company-has-been-hacked-china.

[94] Nicole Perlroth, *Traveling Light in a Time of Digital Thievery*, N.Y. TIMES, Feb. 11, 2012, at A_1.

[95] Kerr, *supra* note 42.

sensitive information, regardless of who owns the server on which it is stored. At the same time, the Court could preserve the power to effectively investigate and prevent crime by preserving the third party doctrine for actual human beings. In essence, the Court should adopt the reasoning advanced in *Warshak*, and expand it to include all the information collected by machines over the internet. To put it another way, the third party doctrine should apply to people, and the Fourth Amendment should apply to machines. By repealing the automation logic of *Smith*, the Court could return us to the Constitutional starting point of privacy protection, and avoid the implicit absurdity that accompanies applying *Smith* to the internet where, unlike in the case of the telephone company, the automated functions of a web browser are not "merely the modern counterpart of an operator" who would otherwise manually perform the same tasks.[96] While the digital age may necessitate the erosion of privacy rights, as Justice Alito suggests,[97] the default position should be an assumption of privacy, rather than an assumption of public disclosure.

An alternative is to reconsider the concepts of "limited purpose" and "voluntariness" addressed in *Miller*.[98] When *Miller* was decided, using a bank to conduct financial affairs may not have been voluntary, but that is simply no longer the case.[99] Commercial regulation has drastically altered the landscape of society, and mandatory disclosure of all sorts of personal information is now required to receive the basic services necessary for survival. Without delving too deeply into the subject, I will simply point out that at the time the third party doctrine was

---

[96] Smith v. Maryland, 442 U.S. 735 (1979) ("The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber." Implicit in every case that relies on Smith, then, is the idea that somewhere in some vast library beneath Time Warner headquarters, someone is manually executing google searches by hand).

[97] United States v. Jones, 565 U.S. ___, Docket no. 10-1259 (2012) (Alito, J., concurring).

[98] Unites States v. Miller, 425 U.S. 435 (1976); *see* Henderson, *supra* note 36.

[99] *Miller*, 425 U.S. at 451("the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account." (Brennan, J., dissenting)).

invented, the government was still claiming that Social Security numbers would not be used for identification purposes. Today, Social Security numbers are the most effective tool for criminals to use to engage in identity theft, and are almost universally required for a range of both public and private services. It is time for the Court to acknowledge these changes, and the manner in which they undermine the logic of the holdings defining the third party doctrine. Citizens routinely disclose information to third parties for a limited purpose, and are often required by law to do so. For the Court to continue to hold that such mandatory, limited purpose disclosures are voluntary in the eyes of the law undermines the credibility of the judiciary, and casts further doubt on the premise that the Supreme Court is competent to decide what expectations of privacy society deems reasonable.

A third approach is a conceptual shift in the analysis of privacy. As in *Jones*, the court has often reverted to concepts of property law to decide Fourth Amendment cases. But electronic communications and the nature of the internet are ill-suited to this analysis. The court should consider borrowing from concepts of intellectual property, rather than tangible property, when considering the right to privacy. After all, we are talking about whether corporations have the right to read, reproduce, and disseminate the private information of their customers without their knowledge or permission. If the court is willing to recognize that private citizens, no less than corporate media outlets, have inherent ownership rights in the information they disseminate on a limited basis, it will be a significant step toward restoring the balance of privacy in American society. In doing so, the court will have to enforce these rights as inalienable, lest the Fourth Amendment be subject to the drafting preferences of a terms of service agreement.

The author's preferred approach would be to adopt a self-executing check on government power. A simple solution would be to recognize that any information that the government

requires us to disclose carries a reasonable expectation of privacy. It appears axiomatic that if the government must compel citizens to disclose information, then the government has inherently recognized a reasonable expectation of privacy in that information. After all, if the information was not private, then people would not need to be forced to disclose it under threat of penalty. However, this solution seems unlikely to be applied, as the unintended effects would cause chaos in the administration of justice, and the court is unlikely to sanction such a sweeping change for the sake of suppressing relevant evidence.

Whether these or other solutions will prove workable in practice depends in large part on the will of the government officials enforcing them. The problem is large, it is systemic, and it is only going to get worse as electronic communications grow more ubiquitous in American society. At the same time, the logic behind decisions such as *Miller* and *Smith* grows more and more detached from reality, and the public's confidence in the courts is threatened as they continue to rely on outdated concepts to render their decisions. Are we to believe, as Justice Scalia suggests, that it is the physical intrusion of the GPS device placed on a car, rather than the information that the device collects, that is relevant to the security guaranteed in the Fourth Amendment?[100] Are we concerned with police officers learning what time the lady of the house draws her bath, or is it the act of a government official monitoring the temperature of our homes that threatens our security?[101] If we concede that the Supreme Court's goal is "the preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted,"[102] then surely the Supreme Court, which often relies on the text of the Federalist Papers, must recognize that Publius had an expectation of privacy that the founding generation

[100] United States v. Jones, 565 U.S. ___, Docket no. 10-1259 (2012).
[101] Kyllo v. United States, 533 U.S. 27 (2001).
[102] *Jones*, 565 U.S. ___ (Alito, J., concurring).

would recognize as reasonable. But under today's Supreme Court jurisprudence, Hamilton, Madison and Jay could be monitored, unmasked and investigated for the threat they posed to the government chartered by the Articles of Confederation. This cannot be the way.

VI. Conclusion

Technological advances have brought privacy to the forefront of American consciousness once again. As issues in the war on drugs, the war on terror, and the internet's influence on interstate commerce continue to clash with the privacy expectations of American citizens, it seems inevitable that a long term solution must be reached. While the Supreme Court avoided the question in *Jones*, the time will come when theories of trespass will be inadequate, and the court will have to face the question squarely. Some people hope that technology will self-correct, and that new advances in encryption technology will determine the answer for us, rendering it outside the government's power to monitor and aggregate our private information, even if it remains within their legal right to do so.[103] But our current systemic approach to privacy makes this nothing more than a pipe dream, as Congress can require developers of encryption software to retain decryption keys, and allow the police to subpoena them. The problem originated in the legislature and the courts, and that is where it must be solved.

Justice Sotomayor has opened the door to reconsider the third party doctrine, but Congress moved to slam it shut with CISPA. Once private entities are granted the power to monitor electronic data for "security threats" and exchange that information with the government, the opportunity to restore some semblance of privacy will likely be lost forever. It is imperative to seize this opportunity to limit the third party doctrine to information that was

[103] John Matson, *Bits of the Future: First Universal Quantum Network Prototype Links 2 Separate Labs*, SCIENTIFIC AMERICAN ONLINE (Apr. 11, 2012), http://www.scientificamerican.com/article.cfm?id=universal-quantum-network.

truly disclosed voluntarily to a natural person. Should the powers the government seeks under CISPA be granted, then the Fourth Amendment will become a dead letter—another rule swallowed by a shortsighted exception. While some commentators believe this issue is *sui generis*, history makes clear that while the medium of communication may change, the threat posed by government intrusion today is no different from the threats this country has faced since its inception.[104] I leave you with a piece of wisdom from the founding generation:

"Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety." – Benjamin Franklin[105]

[104] *See generally* JAMES MORTON SMITH, FREEDOM'S FETTERS: THE ALIEN AND SEDITION LAWS AND AMERICAN CIVIL LIBERTIES (Cornell Univ. Press 1966); JIM VANDER & WARD CHURCHILL, THE COINTELPRO PAPERS: DOCUMENTS FROM THE FBI'S SECRET WARS AGAINST DISSENT IN THE UNITED STATES (South End Press 1990); Louis D. Brandeis & Samuel Warren, *The Right to Privacy*, 4 HARV. L.REV. 193 (1890).
[105] Benjamin Franklin, *Pennsylvania Legislature: Reply to the Governor* (Nov 11, 1765), http://www.ushistory.org/franklin/quotable/quote04.htm.