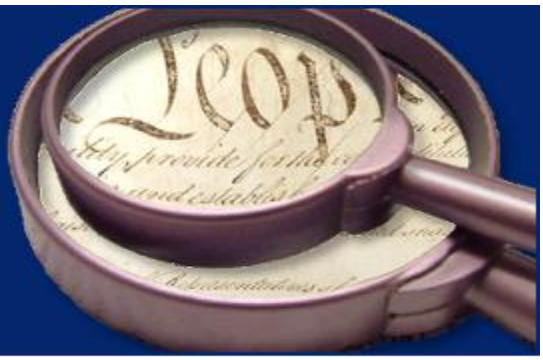
AMERICAN CONSTITUTION SOCIETY FOR LAW AND POLICY

Issue Brief



# The Crisis in Fourth Amendment Jurisprudence

**By Jay Stanley**

**May 2010**



American Constitution Society | 1333 H Street, NW, 11th Floor | Washington, DC 20005

# The Crisis in Fourth Amendment Jurisprudence

Jay Stanley*

## I. Introduction

As the rolling revolution in information technology continues to reshape American life, we need robust rules of the road more than ever to protect the privacy that Americans have always taken for granted. Unfortunately, when it comes to the constitutional amendment that most directly protects our privacy, the Fourth Amendment, federal jurisprudence has gone badly off track. The result is that we are unprepared for an onslaught of new technologies that will leave our privacy more vulnerable than ever in the years ahead.

We are rapidly moving into a new world dominated by biometrics, location tracking, social networks, pervasive surveillance cameras, data mining, cloud computing, ambient intelligence and the "Internet of things," and a trend away from individual, case-by-case surveillance and toward wholesale, automated mass surveillance. The Fourth Amendment as currently interpreted was created largely in the 1970s by men born between 1898 and 1924. It is an edifice that is now, and will increasingly be, put under enormous stress, yet it is not structurally sound.

In part, the problem is simply the fact that the law moves slowly, while technology does not. Given the reality of abrupt, almost discontinuous technological change, our incremental, evolutionary system of jurisprudence sometimes seems simply overwhelmed. In the time it takes a case to go from initial complaint to Supreme Court ruling, entire sectors of the tech industry can rise and fall. In addition, even given the slow rate at which the gears of justice grind, our courts are particularly slow in adapting our traditions to new technologies. It took almost 40 years for the Supreme Court to recognize that the Constitution should apply to the wiretapping of telephone conversations.[1]

But the problem is also that our jurisprudence has gone badly off track and is need of reform. Most commentators identify two principal problems with the Fourth Amendment as it has been interpreted by the Supreme Court: (1) the "third party doctrine," under which information shared with any third party loses all Fourth Amendment protection; and (2) the emergence of a circular standard of "reasonable expectation of privacy."

In some areas, such as communications, Congress has done more than the courts to protect privacy, and some commentators make persuasive arguments that we should invest our hopes in Congress rather than the courts.[2] Of course, advocates should push forward on *all*

---

*Jay Stanley is Senior Policy Analyst at the American Civil Liberties Union's Speech, Privacy and Technology Program. The author would like to thank former ACLU legal intern Jeremy Wolff for his excellent research on the Fourth Amendment jurisprudence in the states.

[1] In 1967, the Supreme Court finally recognized the right to privacy in telephone conversations in *Katz v. United States*, 389 U.S. 347 (1967), reversing the 1928 decision in *Olmstead v. United States*, 277 U.S. 438 (1928).

[2] *See* JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 143-157, 203-216 (2004).

fronts in attempting to defend our privacy. But ultimately, constitutional protection is needed. Like free speech, privacy needs constitutional protection because it is susceptible to "tyranny of the majority" – for example when a security panic leads to calls for suspect minority groups to be stripped of their privacy, or for other unreasonable privacy-invasive security measures. There is also a problem of collective action in privacy: for the individual, it may actually seem rational to rely on the "protection of the herd" because the chances of any one person becoming a subject of abuses by law enforcement or the national security state are usually small, especially for a person not part of a targeted minority or political group. But once such powers can be wielded at will by the authorities, there will be (1) no telling where it will stop, and (2) the inevitable creation of an atmosphere of pervasive insecurity that will affect everyone and chill the community as a whole.

In addition, of course, privacy must be protected constitutionally because the Constitution says it must. But the broken state of our jurisprudence is a serious problem, and poses a substantial risk that advancing technology will leave privacy law in a dysfunctional state and the Fourth Amendment an empty shell. In Section II of this Issue Brief, I examine how our current privacy jurisprudence is broken, and how advancing technology in particular is bringing things to a crisis point by highlighting gaps in the current law and sharpening contradictions in the status quo.

Fortunately, there are reasons to be optimistic about the possibility of reinvigorating the Fourth Amendment, as I discuss in Section III. Those reasons include: (1) the awakening of First Amendment rights in the first half of the 20th century, which serves as a reminder that, when necessary, our judiciary is capable of giving substance and definition to previously weak and vague rights; (2) a line of vigorous dissents in the cases establishing our current jurisprudence, which show that the doctrines were far from self-evident, and provide raw material for judicial reevaluation; (3) the potential for common ground among liberal and conservative jurists, who have both been critical of various aspects of privacy law; and (4) alternative paths taken on privacy by state courts, which both reflect the weakness of current doctrine and lay the groundwork for its repair.

## II. What Is Wrong With Fourth Amendment Jurisprudence

### A. The Third Party Doctrine

According to the Supreme Court's third party doctrine, personal information, once exposed to any third party, loses all Fourth Amendment protection. Some information exposed to third parties is protected by various statutes, but those can be inconsistent and outdated. The Electronic Communications Privacy Act (ECPA), for example, is notably out of date, leaving privacy protection of technology, as the Ninth Circuit put it, "a confusing and uncertain area of the law."[3] Some privacy interests that are currently unprotected under the Fourth Amendment

[3] Konop v. Hawaiian Airlines, 302 F.3d 868, 874 (9th Cir. 2002).

also receive protection under the First Amendment – but that protection is far from comprehensive.[4]

The origins of the doctrine extend back to 1967 in the pro-privacy case *Katz v. United States.*[5] *Katz* overturned a 1928 precedent and found that a suspect making a telephone call from a phone booth did, in fact, enjoy Fourth Amendment protection against wiretapping. This decision was the culmination of a jurisprudential disentanglement of Fourth Amendment privacy from the law of trespass, property rights, and literal-minded hairsplitting over "constitutionally protected area" – modes of thinking that the telephone had long since rendered obsolete. The Court declared in *Katz* that "the Fourth Amendment protects people, not places."[6]

But the Court also noted that, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[7] Thus, if the defendant had not spoken inside a closed phone booth but had spoken loudly where he could be heard by anyone passing by, he could not expect privacy. This commonsense observation, however, was soon pushed in directions that would drastically undercut privacy.

In 1971, the Court ruled in *United States v. White* that the Fourth Amendment offered no protection for conversations recorded by someone wearing a wire, even in one's own home.[8] The Court reasoned that whenever we communicate with another person, we assume the risk that he or she will remember and repeat what we say, and that actual recording of a conversation does not significantly change that reality.[9] Then, in a 1976, the Court in *United States v. Miller* extended that logic from conversations to information shared with one's bank.[10] The Court held that records of the defendant's financial transactions, which the bank was required by law to maintain, were not his "private papers,"[11] and since he had shared them with his bank, he had lost Fourth Amendment protection.

The Court soon extended the same logic to the numbers dialed to and from a telephone, known as a pen register and trap and trace data, in *Smith v. Maryland.*[12] The Court ruled that:

> When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of

[4] *See, e.g.*, Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004) (ruling that National Security Letters violate the First Amendment right to anonymity and association); *In re* Grand Jury Subpoena to Kramerbooks & Afterwords Inc., 26 Med. L. Rptr. 1599 (D.D.C. 1998) (ruling that government must demonstrate compelling need for grand jury subpoena of book purchase information); NAACP v. Alabama, 357 U.S. 449 (1958) (striking down subpoena for membership records as chilling right to association).
[5] *See Katz*, 389 U.S. at 347.
[6] *Id.* at 351.
[7] *Id.*
[8] United States v. White, 401 U.S. 745 (1971).
[9] *Id*. at 751-54.
[10] United States v. Miller, 425 U.S. 435, 443 (1976).
[11] *Id*. at 440-43.
[12] 442 U.S. 735 (1979).

> business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.[13]

The result of these and other cases is that the current jurisprudence is very inconsistent: courts have found that we retain Fourth Amendment protection in the contents of our telephone calls and sealed postal letters, but not in other information that has been exposed to middlemen, from medical and financial data to our reading habits, whether online or in our local library.[14] Even the status of e-mail remains uncertain.[15] And even for letters and telephone calls, the current Fourth Amendment protects only their contents – the outside of envelopes and the numbers that we dial and that dial us are not protected, because it has been deemed to have been exposed to a third party.[16] The Court has created a distinction, not found in the Constitution, between "addressing" or "transactional" data, and content data, with the former receiving no constitutional protection.

While we may not mind *some* people having access to certain information about us, it is a big step to then conclude that we do not mind or cannot prevent the *government* from having access to that information. As Professor Daniel Solove has pointed out, this approach "assumes that the government stands in the same shoes as everybody else, which is clearly not the case."[17] In that sense, it resembles the formalism of the *Lochner* era, which was built around the fiction that a manual laborer and Standard Oil were two equal legal persons "free" to enter into any contract with each other.

B. Reasonable Expectations

The second principal shortcoming with the Fourth Amendment as it has been interpreted in current law is the doctrine that privacy is only protected where a person has "a reasonable expectation of privacy." Once again, this harmful doctrine emerged out of the pro-privacy decision in *Katz* extending Fourth Amendment protection to telephone conversations. In a concurring opinion, Justice Harlan wrote that Fourth Amendment coverage required "first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[18] This two-part test was taken up in other cases and hardened into the "reasonable expectation" doctrine.

As a result of this approach, the Fourth Amendment as it is currently interpreted provides no protection against a wide array of intrusive searches. The Court has found no "reasonable expectation of privacy" against aerial video surveillance, for example, even when sunbathing in one's own back yard and surrounded by a tall fence,[19] or against searches of one's household

---

[13] *Id.* at 744.
[14] Again, privacy in these areas is sometimes and inconsistently protected by federal statutes such as the Health Insurance Portability and Accountability Act (HIPAA) and state library confidentiality and financial privacy laws.
[15] *See* Warshak v. United States, 532 F.3d 521 (6th Cir. 2008) (en banc decision vacating panel's finding of Fourth Amendment protection for e-mail as unripe).
[16] Smith v. Maryland, 442 U.S. 735 (1979).
[17] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE DIGITAL AGE 215 (2004).
[18] Katz v. United States, 389 U.S 347, 361 (1967).
[19] California v. Ciraolo, 476 U.S. 207 (1986).

garbage once it is left out on the curb.[20] Or against a wide range of surveillance that takes place in public, even if it is intrusive in ways that, as a factual matter, violate the expectations of most Americans, such as the tracking of a vehicle via an electronic device.[21]

1. The Circularity of "Expectations"

The primary, widely recognized problem with this standard is its circularity: people get only the privacy that they expect to get. Under this standard, even the most reprehensible invasions of privacy might lose constitutional protection if a realistic person is forced to conclude that their privacy will in fact be invaded – much as a realistic person might sadly conclude that, no matter how wrong it is, a diamond ring dropped on a busy sidewalk will not long remain.

In theory, it means the FBI could take out Super Bowl ads announcing deployment of its latest high-tech surveillance technique, and destroy any reasonable expectation that one might have in that area. Or as Professor Laurence Tribe put it, "if you put billboards up saying, 'Big Brother is listening wherever you are,' there goes your expectation of privacy."[22] The effect is to create what one commentator has called a "one-way ratchet against Fourth Amendment protection."[23]

The circularity of the "reasonable expectation" language may not have been a problem if the Court had simply adopted the word "desire" or "intention," instead of "expectation," when enunciating this test – and to have done so would have barely altered Harlan's original point, which was simply that people who publicly flaunt something obviously cannot be extended protection for their privacy.[24]

The word "expectation" is circular because it bases law and practice on the subject's understanding of law and practice. If we simply substituted "desire for" or "intention to preserve" privacy for "expectation of," the circularity would be eliminated. Under Harlan's test, privacy would then be honored when (1) individuals act as if privacy was desired, and (2) that desire is seen as reasonable by the community.

---

[20] California v. Greenwood, 486 U.S. 35 (1988).

[21] *See* United States v. Knotts, 460 U.S. 276, 281-82 (1983).

[22] Laurence H. Tribe, Freedom of Speech and Press in the 21st Century: New Technology Meets Old Constitutionalism, Remarks at the Progress & Freedom Foundation's Aspen Summit (Aug. 21, 2007), *available at* http://www.pff.org/issues-pubs/pops/pop14.19tribetranscript.pdf.

[23] Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U.L. REV. 1381, 1389 (2008).

[24] After describing his two-part test, Harlan gave several examples showing that this is what he had in mind:

> Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected," because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.

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

2. Unrealistic "Expectations"

Another significant problem with both the "reasonable expectation" criterion and the third party doctrine is that they are legal fictions that are very fictional indeed. In reality, rightly or (more often) wrongly, most people do in fact have a belief – an *expectation* – that information they share with many third parties – their bank, their doctor, their Internet service provider – will be kept private.[25]

The current "reasonable expectation" doctrine could only make sense in an era of relatively gradual change in privacy-invading technologies. In an era of gradual change, the circular nature of the doctrine would be much less of a problem, because "expectations" in such contexts could refer to deeply rooted cultural understandings of the boundaries between the public and the private. This would be a reasonable criterion for the Court to lean upon, since privacy is in some (but not all) respects, a culturally relative value. But when changes are as rapid as they are today, that reflexivity becomes intolerable and unworkable. In that context, the "expectation" language makes our rights dependent on up-to-the-minute reevaluations of reality at a time when perpetual technological change leaves us in an extremely fluid, practically revolutionary situation, and when we need stability of expectations regarding our privacy more than ever.

C. The Technology Revolution Exacerbates the Problem

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects" except when the government obtains a warrant based on probable cause.[26] Our privacy interest in our papers and effects has not diminished, but today we store these things in different forms and in different places than the Founders did. The "papers and effects" of someone like, say, Thomas Jefferson – his correspondence, financial and medical records, and so forth – were likely to be stored in his library. In fact, not just his records but most of his actual financial and medical life itself took place within the boundaries of Monticello. Today, our lives have moved outward: our records are just as likely to be stored on the servers of international corporations as in our home. Our medical care is mostly performed in doctor's offices and hospitals outside the home, our money is held by banks and brokerages – and of course, our verbal conversations are no longer necessarily confined within the walls where they take place, while our written correspondence is often transported and stored electronically by numerous third-party middlemen. Yet we have just as much need for fundamental privacy protections as did Jefferson and his contemporaries.

From the standpoint of an individual seeking privacy in today's high-tech world, it is highly arbitrary that postal letters handed over to a third party and electrical fluctuations transmitted over wires owned and controlled by a third party (*i.e.*, telephone calls) are protected by the Fourth Amendment, but telephone digits that similarly pulse through telecom wires are not. It would be absurd for e-mail not to be protected, yet all e-mail is exposed to third parties as

[25] Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at 'Understandings Recognized and Permitted by Society,'* 42 DUKE L.J. 727 (1993); CHRISTOPHER SLOBOGIN, PRIVACY AT RISK 33-35, 110-113, 183-186 (2007).
[26] U.S. Const. amend. IV.

it passes through the network of servers that make up the Internet, and when it arrives it is stored by the recipient's Internet service provider. When it comes to the computers that we carry with us (*i.e.*, mobile phones), our voice conversations are protected, but that is an increasingly small portion of what we use our phones for. Web surfing, chat, music downloading, and GPS location sensing make up the rest – and as with e-mail, the courts are having a hard time providing clear protection for these activities because of the Supreme Court's broken doctrine.

The status quo will become only more dysfunctional as the information revolution unfolds. To take just one example, industry and government are currently working on implementing a concept called "the smart grid," which involves putting computer intelligence into the electricity system – both into the utilities' distribution systems, and into customers' appliances within the home.[27] This promises many advantages in terms of energy efficiency and the environment. By pricing electricity differently at different times, for example, it could smooth out demand cycles and reduce the need for utilities to invest in the generation capacity required to handle occasional spikes in demand. Appliances would communicate with each other and with the grid in order to shift electricity use to cheaper times, and to provide feedback to homeowners about their electricity use.

The result, however, could be that relatively detailed information about activities inside the home will be transmitted to utilities, third-party service providers, or others. And under the third party doctrine, that information flowing out from the home could be found to lose constitutional protection. Not only information about "at what hour each night the lady of the house takes her daily sauna and bath" (which the Supreme Court has used as an example of protected information[28]) but far more besides, would become available. Unfortunately, anyone who wants to retain constitutional protection for the privacy of activities in their home would be well advised to steer clear of many smart grid applications until the current doctrine is fixed.

1. Our Papers, Ourselves

The increasing embrace of "cloud computing" may, as much as any trend, intensify the arbitrary effects of current jurisprudence. Cloud computing is the trend toward creating and storing data (such as calendars, address books, photos, and documents) not on individuals' private computers, but on third-party servers that provide convenient access from a browser anywhere on the Internet. To the modern computer user, the difference between a letter created and stored on his or her hard drive, and a letter stored or composed on a Google server, is nearly

[27] For more on the privacy implications of the Smart Grid, *see, e.g.*, ELECTRONIC PRIVACY INFORMATION CENTER ET AL., COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER TO THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Dec. 1, 2009), *available at* http://epic.org/privacy/smartgrid/EPIC_Smart_Grid-Cybersecurity_12-01-09.2.pdf; FUTURE OF PRIVACY FORUM ET AL., SMARTPRIVACY FOR THE SMART GRID: EMBEDDING PRIVACY INTO THE DESIGN OF ELECTRICITY CONSERVATION (Nov. 2009); *available at* http://www.futureofprivacy.org/wp-content/uploads/2009/11/smartprivacy-for-the-smart-grid.pdf.

[28] Kyllo v. United States, 533 U.S. 27, 38 (2001).

invisible. But the third party doctrine makes the difference highly relevant, and ultimately, threatens to make the Fourth Amendment a hollow shell.[29]

Although our documents may be stored on distant servers, they can be as personal as ever, and perhaps even more so. Technology affects not just how we externally handle our "papers and effects" – it also affects the very way that we think and communicate. People today are discovering that a telephone conversation between two people sitting at their respective computers can be a different kind of conversation, as both parties seamlessly integrate on-the-fly Internet searches into the discussion. And our computers are increasingly becoming an integral part of how we think. From ancient times through the Renaissance, memory was the single most highly valued mental skill.[30] Today, however, when we all have access to libraries full of books and computers that can store and retrieve more raw data than our minds will ever match, that faculty has been devalued and is derided as "mere memorization." With the de-emphasis of memorization skills, our minds have evolved to function around the written word – and as computers have made manipulation of words more fluid than ever, many people today find they have trouble arranging their thoughts without laying them out on a word processor. In effect, for many people, the computer has become an extension of their mind.

Ironically, in the past this continuity of private writings and private thoughts was better recognized in the law than it is today. Until relatively recently, private papers were regarded as immune to seizure. For centuries, English law did not permit the government to access private papers in civil or criminal cases, even with a valid warrant.[31] Behind this rule was a belief that using a person's papers as evidence against him was akin to forcing him to testify against himself. As an anonymous 1763 pamphlet on this issue put it:

> A man's WRITINGS lying in his closet, NOT PUBLISHED, are no more than his thoughts, hardly brought forth even in his own account, and, to all the rest of the world, the same as if they yet remained in embrio in his breast.[32]

This seizure of private papers was at the center of heated public controversy over several high-profile (and ultimately successful) lawsuits against the English government.[33] Among those galvanized by the issue were the American colonists, who later wrote protections against both unreasonable searches and seizures and self-incrimination into the Constitution.[34] A century later, in 1886, the protection for private papers was upheld by the Supreme Court in *Boyd v. United States.*[35] The Court cited the English precedent, said that it was the Founders' undoubted

---

[29] *See* ACLU OF NORTHERN CALIFORNIA, CLOUD COMPUTING: STORM WARNING FOR PRIVACY? (Jan. 2010); *available at* http://www.dotrights.org/sites/default/files/Cloud%20Computing%20Issue%20Paper.pdf.
[30] *See* F.A. YATES, THE ART OF MEMORY (1966); MARY CARRUTHERS, THE BOOK OF MEMORY: A STUDY OF MEMORY IN MEDIEVAL CULTURE (1990).
[31] *See* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 26-53 (2000). My account of the law in this area comes from Rosen, as well as Eric Schnapper, *Unreasonable Searches and Seizures of Private Papers*, 71 VA. L. REV. 869 (1985), upon which Rosen also relies.
[32] ROSEN, *supra* note 31, at 29.
[33] *Id.* at 27-31.
[34] *Id.* at 27.
[35] 116 U.S. 661 (1886).

intention to incorporate it into the Constitution, and ruled that subpoenaing a person's private papers violated not only the Fourth Amendment but also the Fifth. "The seizure of a man's private books and papers to be used in evidence against him" is not "substantially different from compelling him to be a witness against himself," the Court found.[36]

The *Boyd* case actually had to do not with revealing personal letters or a diary, but with business records. In this, the Court unfortunately overreached, and its precedent was eroded as regulation of business expanded in the 20th century. And in doing so the courts never drew a line between business records and personal records to preserve privacy protection for the latter. Although the Supreme Court has never explicitly repudiated the distinction, in relatively recent times the right to the privacy of personal records through subpoena has effectively been destroyed. In 1994, for example, Senator Bob Packwood lost an effort to fight a subpoena of his diaries, which were subsequently made public and mockingly and humiliatingly excerpted in the *Washington Post*,[37] and Monica Lewinsky's drafts of unsent love letters to President Clinton were acquired by Independent Counsel Kenneth Starr and published.[38]

As Americans make use of all the advantages of new technologies and increasingly commit not only their communications, purchases, and research to electronic media, but often their very thoughts, they should not have to worry that changes in the mere technology used for the fundamental activities of life will leave them without privacy for their thoughts, communications, papers, and effects.

2. Wholesale Surveillance

Current jurisprudence has another disturbing implication. *White*, *Miller*, and *Smith* all contributed to a significant decline in protection for privacy in America during the 1970s. But in one respect their impact was limited: all involved what has been called "retail," or individually targeted surveillance, as opposed to the "wholesale" kind of mass monitoring that is increasingly becoming possible. The ruling in *White*, for example, addresses cases where people are recruited to betray others by wearing a wire. Human beings are expensive and time-consuming, and arranging to place them in such situations is a complex, labor-intensive, and often dangerous matter. *Miller* and *Smith* similarly involved attempts by the police to obtain information about specific individuals that they already had in their sights.

But the *White* Court's blithe equivalence of electronic and non-electronic eavesdropping, the *Miller* Court's placement of personal financial records outside Fourth Amendment protection, and the content/non-content distinction invented by the *Smith* Court, have paved the way for large-scale privacy invasions that were not technologically possible when those opinions were written.

For example, the Bank Secrecy Act[39] and the Patriot Act,[40] combined with modern electronic communications and the third party doctrine, have permitted the emergence of a

[36] *Id.* at 633.
[37] ROSEN, *supra* note 31, at 31-33.
[38] *Id.* at 26.
[39] 31 C.F.R. § 103.

system in which the Treasury Department's Financial Crimes Enforcement Network (FinCEN) routinely gathers a vast amount of information about financial transactions. The information it collects includes any transactions over $3,000 involving cash, checks, or commercial paper,[41] a broadly defined set of other "suspicious" transactions,[42] all cash transactions of $10,000 or more not just by banks but by anyone engaged in any "trade or business,"[43] and all international wire transfers of $3,000 or more.[44] FinCEN then sifts through that information (*i.e.*, data mines it) in an effort to spot wrongdoing.[45]

Similar mass data mining is now taking place with regard to Americans' international telephone and email communications. This was done first under the National Security Agency's (NSA) illegal warrantless wiretapping program, and now under cover of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008,[46] which effectively approved of such activity by allowing extremely broad searches with no requirement of specificity, no limits on the storage and use of collected information, and little judicial oversight.

All of this is a violation of the time-honored principle in the Anglo-American legal tradition that the government does not watch everyone in an attempt to spot illegal activity, but must have particularized suspicion before it begins looking over people's shoulders. Unless the Constitution is there to protect us, it is to be expected that this kind of routine wholesale surveillance will expand into ever more areas.

In short, today's technology revolution is creating a crisis in Fourth Amendment law. There is no functionalist magic to guarantee that the legal system will adapt, and that we will not simply find ourselves with a greatly diminished right of privacy. However, there are reasons to believe that reform is possible, and Section III of this Issue Brief will look at those reasons.

## III. Potential Sources of Reform

### A. The Emergence of Free Speech

The kind of broad repair of Fourth Amendment jurisprudence that we so badly need today actually took place in First Amendment law early in the 20th century. Before World War I, free speech was generally recognized as an American value, but when that all-American value came into conflict with other all-American values (such as "support your country in a time of war") or with viewpoints that struck a community as "simply beyond the pale," it lost out. Free expression was broadly exercised in America through such traditions as a boisterous and partisan press, loud criticisms of political figures, and postal subsidies for periodicals of all persuasions. But radicals, labor organizers, and purveyors of material that was deemed socially

---

[40] Pub. L. No. 107-56, 115 Stat. 272 (2001).
[41] 31 C.F.R. § 103.29.
[42] 31 C.F.R. § 103.15-103.21.
[43] 31 C.F.R. § 103.30.
[44] 31 C.F.R. § 103.33.
[45] "Through robust data mining capabilities, FinCEN can analyze SAR filings for a particular financial institution, type of activity, or geographic area." *Suspicious Activity Reports: Not Just for Law Enforcement*, THE SAR ACTIVITY REV., May 2007, at 41; *available at* http://www.fincen.gov/sarreviewissue11.pdf.
[46] Pub. L. No. 110-261, 122 Stat. 2436 (2008).

"harmful," such as anything that ran afoul of Victorian moral sensibilities (including for example any information whatsoever about birth control) received virtually no protection in the courts.[47]

In fact, there was widespread hostility to free speech claims in the courts – especially in the Supreme Court, which rarely generated even a dissenting opinion in such cases.[48] In 1907, for example, the Court found in *Patterson v. Colorado* that while the First Amendment prohibited the prior restraint of speech, the punishment of speech that "may be deemed contrary to the public welfare" was perfectly constitutional.[49] Freedom of Speech was an ethos – but an ethos was all that it was. In this it was in much the same position as privacy today.

However, in the following decades, First Amendment jurisprudence underwent a startling transformation. During the war, anti-war sentiment was vigorously repressed, including through the Espionage Act of 1917 and the Sedition Act of 1918. Americans were thrown in jail for such activities as writing letters to the editor protesting U.S. participation the war. Enforcement of these laws was highly selective, targeted almost exclusively against socialists and radicals but not other opponents of the war.[50]

In three separate cases decided in March 1919, the Supreme Court repeatedly rejected First Amendment defenses by socialists convicted of speaking out against the war.[51] Justice Oliver Wendell Holmes wrote all three decisions, and Justice Louis Brandeis joined the unanimous opinions. But just eight months later, both justices seemed to have a change of heart and dissented in another free speech case, *Abrams v. United States*.[52] From this start, Supreme Court protection of free expression flowered. Justices Holmes and Brandeis remained primarily as dissenters on free speech throughout the 1920s, but increasingly their position won out. In 1925 the Court applied the First Amendment to the states via the Fourteenth Amendment,[53] in 1927 it ruled in favor of a radical for the first time in a free speech case,[54] and in 1931 the Court first invalidated a state law as a violation of the First Amendment.[55] In subsequent decades, the Court fully embraced the robust reading of the First Amendment that holds sway today, and eventually the United States came to offer what may well be the broadest protections for free speech in the world.

Of course, legal shifts do not take place in a historical vacuum. Justices Holmes and Brandeis's particular shift on free speech is often attributed to the influence of widely read

---

[47] PAUL STARR, THE CREATION OF THE MEDIA: POLITICAL ORIGINS OF MODERN COMMUNICATIONS 267-94 (2004); DAVID M. RABBAN, FREE SPEECH IN ITS FORGOTTEN YEARS, 1870-1920 (1997); SAMUEL WALKER, IN DEFENSE OF AMERICAN LIBERTIES: A HISTORY OF THE ACLU 11-26 (1990).
[48] RABBAN, *supra* note 47, at 131; STARR, *supra* note 47, at 268.
[49] Paterson v. Colorado, 205 U.S. 454, 462 (1907).
[50] STARR, *supra* note 47, at 277-278. Selective enforcement was not an accidental, additional problem to the repression of speech, of course – it is virtually inevitable when certain people are allowed to decide which speech is acceptable and which is not.
[51] Schenck v. United States, 249 U.S. 47 (1919); Debs v. United States, 249 U.S. 211 (1919); Frohwerk v. United States, 249 U.S. 204 (1919).
[52] 250 U.S. 616 (1919).
[53] Gitlow v. New York, 268 U.S. 652 (1925).
[54] Stromberg v. California, 283 U.S. 359 (1931).
[55] Near v. Minnesota, 283 U.S. 697 (1931).

articles by Harvard law professor Zechariah Chafee.[56] But the justices, as well as Professor Chafee, were also part of a broader community of statist and pro-war Progressives disillusioned by the domestic abuses of World War I and newly appreciative of individual rights. As affluent elites, they had been insulated from restrictions on free speech, which they had previously associated heavily with pro-business laissez-faire forces, and what that could mean. In 1919 in particular, when Justices Holmes and Brandeis made their switch, Progressives were horrified by the Red Scare, dismayed by intense labor violence and repression, and newly disgusted by the war as a result of the Versailles Treaty.[57] Such dismay sparked among other things the formation in 1920 of the ACLU, which went on to push for broader free speech rights, in court and out.[58]

Adding to the trend was a simultaneous growth in cultural liberalization and cosmopolitanism that made Victorian censorship of sexual material via state and federal Comstock laws increasingly seem provincial and narrow-minded.[59] And even more fundamental was the fact that the United States was turning from a set of largely isolated "island communities" into more of a single, larger community, confronting many Americans with questions of diversity they had not before faced.[60]

But World War I brought these trends to a head and functioned as the "generative crisis" of free speech.[61] It intensified the contradiction between the latent and diffuse American cultural respect for diversity of opinion on the one hand, and on the other, the willingness to tolerate legal suppression of opinions that lay outside certain boundaries. The extreme pressures of war and the "extreme" reactions provoked by that war pushed the judiciary and society to resolve that contradiction in favor of expression.

With free speech, historical circumstances brought latent contradictions within American life to a boiling point, leading to a revolution in First Amendment law. Today we may well be facing a similar generative crisis in Fourth Amendment law – one sharpened not by war but by technology. We have on the one hand a set of less-than-robust Fourth Amendment doctrines that originated largely in the post-Warren, Nixonian context of the 1970s, when questions of crime and disorder loomed large politically (and were a major factor in the disintegration of the New Deal political coalition that had ruled America since 1932). On the other hand, we have an ongoing technological revolution that is exposing the weakness of those legal doctrines and bringing them into growing conflict with Americans' sense of what is and should be private.

B. Privacy Dissents

There is a rich body of intellectual work that has been highly critical of the Supreme Court's Fourth Amendment law and that might provide raw material for a way out of the current

[56] RABBAN, *supra* note 47, at 342; WALKER, *supra* note 47, at 27.
[57] STARR, *supra* note 47, at 284-85.
[58] *Id*. at 281, 285.
[59] RABBAN, *supra* note 47, at 351-352; WALKER, *supra* note 47, at 30-45; STARR, *supra* note 47, at 268-274.
[60] WALKER, *supra* note 47, at 29.
[61] STARR, *supra* note 47, at 274.

quagmire in this area. In addition to work by a variety of legal scholars,[62] there is a line of vigorous dissents to the big post-Warren Court privacy cases that established the current broken doctrines. Unlike free speech, where decisions against expression were long unanimous, in the privacy area there have been strong dissenters all along, including especially Justices William J. Brennan, John Marshall Harlan, and Thurgood Marshall. These dissenters spurned the Court's third party doctrine and in some cases its emphasis on or application of the "reasonable expectation" criterion. Instead, they emphasized the need for protection of the substance of privacy and the practical loss of privacy entailed by these decisions. They also pointed out the involuntary nature of the disclosures at issue in these cases, such as the necessity in modern life of dialing phone numbers and maintaining bank accounts. These dissents demonstrate that the law as it has developed was far from self-evident, and provide raw material for the creation of new lines of jurisprudence.

We might look to Justice Harlan's dissent in *United States v. White*, the 1971 case about the use of an informant wearing a wire. Justice Harlan rejected the "expectations approach of *Katz*" and pointed the way toward a broader, more substantive, and non-circular standard for privacy.[63] "We should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society," he wrote, arguing that the question before the Court must "be answered by assessing the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement."[64] He then evaluated the actual substantive effect of wearing a wire upon Americans' privacy:

> The impact of the practice of third-party bugging, must, I think, be considered such as to undermine that confidence and sense of security in dealing with one another that is characteristic of individual relationships between citizens in a free society . . . . Words would be measured a good deal more carefully and communication inhibited if one suspected his conversations were being transmitted and transcribed. Were third-party bugging a prevalent practice, it might well smother that spontaneity – reflected in frivolous, impetuous, sacrilegious, and defiant discourse that liberates daily life.[65]

Similarly, in a dissent in *Smith*, Justice Marshall argued that constitutional protections should not depend on a person's subjective privacy expectations, but "on the risks he should be forced to assume in a free and open society."[66] Justice Marshall also thought that the underlying

---

[62] For critiques of Fourth Amendment jurisprudence, *see, e.g.*, SLOBOGIN, *supra* note 25; SOLOVE, *supra* note 17; Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 293-96 (2005); ROSEN, *supra* note 31; Harper, *supra* note 23; WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT (1978).

[63] United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

[64] *Id.*

[65] *Id.* at 787; Jeffrey Rosen points to this dissent in THE NAKED CROWD, *supra* note 2, at 204-206.

[66] *Smith*, 442 U.S. at 750 (Marshall, J., dissenting); *see also* ROSEN, *supra* note 31, at 64.

statute in that case, the Bank Secrecy Act, which imposed recordkeeping requirements on banks, represented an unconstitutional warrantless seizure of customers' financial records.[67]

In *Miller*, Justice Brennan cited the full substantive privacy interest that individuals hold in their bank records, and their lack of choice or control over them:

> [I]t is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography.[68]

Justice Brennan compared the invasion of bank privacy in the *Miller* case to the intrusion into an individual's privacy that results from "violent searches and invasions" of a person's dwelling, adding that high-tech privacy violations could be "equally devastating":

> Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently, judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new devices.[69]

The original pro-privacy decision in *Katz* also contains raw material for new directions in Fourth Amendment jurisprudence. Brushing aside government arguments that the defendant had no privacy because his telephone booth was made of glass, and that therefore he was in public and had no privacy, the Court wrote:

> But what [Katz] sought to exclude when he entered the booth was not the intruding eye – it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen . . . . To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[70]

The Court thus recognized, first, that it matters when particular communications facilities come to play a "vital role" in private communication – an observation that should be extended today to all manner of electronic communication. Second, the court recognized that being "in public" is not a binary state – that is, one can be exposed to the public in some respects but not in others. This is another increasingly important observation as all manner of novel technological

[67] California Bankers Ass'n v. Shultz, 416 U.S. 21 (1974) (Marshall, J., dissenting).
[68] United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting) (quoting Burrows v. Superior Court of San Bernardino County, 529 P.2d 590, 596 (Cal. 1974)).
[69] *Id.* (quoting *Burrows*, 529 P.2d at 593-596).
[70] Katz v. United States, 389 U.S. 347, 352 (1967).

invasions of privacy – from pervasive video surveillance to thermal imagers to remote pulse-measurement devices to tracking devices – are justified through the too-simple observation that "when you're in public you have no expectation of privacy."

A footnote in the majority opinion in *Smith* could also serve as fuel for future courts wishing to redirect Fourth Amendment law. "Situations can be imagined," the majority wrote, in which reasonable expectations would be "inadequate" as a constitutional measure.[71] Such situations might include a refugee from a totalitarian nation who expects no rights, or if "the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry."[72]

> In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.[73]

If the Supreme Court were to recognize the technological revolution as one such factor that makes its doctrine "inadequate," that would go a long way toward improving our privacy jurisprudence.

C. Conservatives

It has not only been liberal justices who have been critical of current privacy doctrine. Justice Antonin Scalia authored a majority opinion in the 2001 case *Kyllo v. United States* striking down the use of thermal imagers by the police to identify an in-home marijuana-growing operation via the heat given off by lamps the defendant had installed for his plants.

In *Kyllo*, Justice Scalia acknowledged the problem with the reasonable expectation doctrine, observing that "the *Katz* test – whether the individual has an expectation of privacy that society is prepared to recognize as reasonable – has often been criticized as circular, and hence subjective and unpredictable."[74] Justice Scalia preferred to ground his judgment in the intent of the Founders, and on that basis found that the use of the scanners was a search. Only that position, he said, "assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[75]

That criteria, read broadly, not only dissolves the circularity of "reasonable expectations," but also should dispose of the third party doctrine, which due to changes in technology, as we

[71] *Smith*, 442 U.S. at 741 n.5.
[72] *Id.*
[73] *Id.*
[74] Kyllo v. United States, 533 U.S. 27, 34 (2001).
[75] *Id.*

have seen, most definitely does not "assure preservation that degree of privacy" enjoyed by the Founders.

Justice Scalia's decision is not unlimited in scope – he relied heavily on the "Fourth Amendment sanctity of the home" and it is unclear how far beyond that time-honored boundary he would push his analysis.[76] His opinion also includes a potentially ominous disclaimer about the ruling applying only to those technologies "not in general public use."[77]

But there are other examples of conservative justices supporting privacy. For example, in a concurring opinion on a 2000 case, Justice Clarence Thomas (joined by Scalia), held out the possibility of once again making personal papers immune from seizure as they were once understood to be. Justices Thomas and Scalia suggested their willingness "in a future case" to broaden the Fifth Amendment based on an originalist reading of the meaning of the term "witness," as in the Fifth Amendment's prohibition on forcing a person "to be a witness against himself."[78] Justice Thomas argued that according to "the meaning of the term at the time of the founding," the word referred not just to evidence of a "testimonial character," as current Supreme Court doctrine has it, but *any* evidence, including personal papers and effects.[79]

Although an originalist approach might work pretty well at protecting our privacy in the midst of the technology revolution, we need not embrace Justices Scalia and Thomas's originalist theories of jurisprudence to rescue the Fourth Amendment. It would be enough for the Court to make a broad judgment over which privacy desires our society does, as a matter of fact, regard as reasonable according to the contemporary standards of our culture, in the broadest sense, including our oldest traditions.

But there is potential common ground between originalists and broader judicial visions that look to the substantive privacy needs of fulfilled citizens in a democratic society. Conservatives may want to focus on "that degree of privacy against government that existed when the Fourth Amendment was adopted," while liberals may want to more openly acknowledge the Court's need to impose substantive privacy out of an evaluation of the deep-rooted privacy sensibilities of contemporary society. Happily for privacy, the Founders clearly valued substantive privacy protection, so a substantive approach and an originalist approach have the potential, at least, to dovetail with each other on privacy, and hermeneutical warfare over these approaches can take place on other battlefields.

The unity of the two approaches – substantive and originalist – can be seen in Justice Brandeis's famous dissent to *Olmstead v. United States*, the 1928 decision finding that telephone calls did not enjoy Fourth Amendment protection (later overturned by *Katz*).[80] When the Constitution was written, the violation of individuals' privacy and right against self-

[76] The Court also found that warrantless GPS tracking of a car is impermissible when the vehicle is brought into a private residence. United States v. Karo, 468 U.S. 705 (1984).
[77] *Kyllo*, 533 U.S. at 40. It is already possible to find a fully functional $50 infrared night-vision scope on the shelves of the toy department at Target.
[78] U.S. Const. amend. V.
[79] United States v. Hubbell, 530 U.S. 27, 50 (2000) (Thomas, J., concurring).
[80] *See generally* Olmstead v. United States, 277 U.S. 438 (1928).

incrimination "had been necessarily simple," Brandeis observed.[81] But, "subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government . . . to obtain disclosure in court of what is whispered in the closet."[82] Brandeis protested against "an unduly literal" interpretation of the Fourth Amendment, writing that:

> The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect . . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone.[83]

Ultimately we need Fourth Amendment doctrines that are built around phrases such as "the privacy and dignity befitting a free people," "the space to explore and create one's identity," and the "universal need for a refuge from the glare of the community." We need jurisprudence that reads "papers and effects" broadly to include the modern-day equivalent – electronic files in all their forms – and provides protection for them. A richer privacy jurisprudence might incorporate the European notion of "proportionality,"[84] the importance of individuals' actual desires for privacy, and the principle that where people have no choice but to give up information, privacy should receive heightened protection. And most of all, we need jurisprudence that preserves the substance of privacy, not just its form, through rapid changes in technology.

D. Privacy in the States

Another possible source for alternatives to current Fourth Amendment jurisprudence comes from the states. Indeed, Justice Brennan argued in an influential 1977 law review article that, in light of the direction the Supreme Court was taking on privacy, Americans should look to the states as a beacon of protection in a "new federalism." He also criticized state jurists who interpret their state constitutions in "lockstep" with the federal judiciary.[85]

An ACLU review of state constitutions and jurisprudence on the third party doctrine makes clear that a significant number have departed from the Supreme Court in areas where the federal jurisprudence is problematic. Some have done so because their courts have found that their state constitutions do not permit it, but others with language very close to the federal

---

[81] *Id*. at 473 (Brandeis, J., dissenting).
[82] *Id.*
[83] *Id.* at 478.
[84] Christopher Slobogin argues for the centrality of a principle of "proportionality" in privacy jurisprudence in PRIVACY AT RISK, *supra* note 25.
[85] William J. Brennan, Jr., *State Constitutions and the Protection of Individual Rights*, 90 HARV. L. REV. 489, 491 (1977). *See also* Stephen E. Henderson, *Learning From All Fifty States: How To Apply the Fourth Amendment And its State Analogs To Protect Third Party Information From Unreasonable Search*, 55 CATH. U.L. REV. 373 (2006); Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1129-53 (2002).

constitution have also taken a different interpretive path, whether on the third party doctrine, the reasonable expectation standard, or on various technologically enhanced searches.

California is an example of a state that has much stronger privacy laws than the federal government. While the state constitution contains language almost identical to the Fourth Amendment, the state has decisively rejected the third party doctrine. In a case similar to – but preceding – the *Miller* ruling on protection for bank records, California's high court rejected the government's arguments for warrantless access based on the lack of voluntariness in customers' furnishing of financial details to the bank, as well as the revealing nature of the information.[86]

Brennan later cited this case extensively in his own dissent in *Miller*, saying that the decision "strikingly illustrates the emerging trend among high state courts of relying upon state constitutional protections of Individual liberties – protections pervading counterpart provisions of the United States Constitution, but increasingly being ignored by decisions of this Court."[87]

Other states also offer a variety of alternative approaches. Examples include:

- Washington state, where the law centers around a substantive inquiry into whether a search is an intrusion into one's "private affairs," defined as "those privacy interests which citizens of this state have held, and should be entitled to hold."[88]
- New Jersey, which relies on a modified version of the "reasonable expectation" test that requires only that there *can be* a reasonable expectation under the circumstances. It has also stated that "disclosure to a third-party provider, as an essential step to obtaining service altogether, does not upend the privacy interest at stake."[89]
- Pennsylvania, which has rejected the third party doctrine, finding that "so long as a person seeks to preserve his effects as private, even if they are accessible to . . . others, they are constitutionally protected."[90]
- Hawaii, where courts have adopted the "reasonable expectation" standard but have interpreted it to require "that governmental intrusions into the personal privacy of citizens of this State be no greater in intensity than absolutely necessary."[91]
- Indiana, where courts look at whether a particular search is reasonable "under the totality of the circumstances," without examining the subjective expectations of the person targeted by the search.[92]

Overall, the ACLU review of state laws found that 11 states have, to a greater or lesser extent, explicitly rejected federal third party doctrine,[93] while nine more have indicated in some

[86] *See generally* Burrows v. Superior Court of San Bernardino County, 529 P.2d 590 (Cal. 1974).
[87] United States v. Miller, 425 U.S. 435, 454 (1976) (Brennan, J., dissenting).
[88] State v. Myrick, 688 P.2d 151, 154 (Wash. 1984).
[89] State v. Reid, 945 A.2d 26, 33 (N.J. Super. Ct. App. Div. 2008); *see also* State v. Hemplele, 576 A.2d 793 (N.J. 1990).
[90] Commonwealth v. DeJohn, 403 A.2d 1283, 1289 (Pa. 1979), *cert. denied*, 444 U.S. 1032 (1980) (quoting Commonwealth v. Platou, 312 A.2d 29, 34 (Pa. 1973), *cert. denied*, 417 U.S. 976 (1974)).
[91] State v. Kaluna, 520 P.2d 51, 58-59 (Haw. 1974).
[92] Moran v. State, 644 N.E.2d 536, 539 (Ind. 1994).

fashion that they could reject it in the future.[94] An additional 12 states diverge from federal third party doctrine in other, minor ways,[95] while 18 states follow federal doctrine "in lockstep."

The situation in the states is significant for several reasons. First, state law today serves as a source of alternative legal thinking on privacy. Prior to the 20th century expansion in First Amendment rights, the states played just that kind of role. While the Supreme Court was extremely hostile to free speech claims before World War I, historians point out that the legal and cultural groundwork for the subsequent revival of the First Amendment could be found in the states, where a significant number of court decisions rejected the Supreme Court's approach and kept the possibility of genuine free speech rights alive within the American legal "conceptual universe."[96]

Over time, the spread of alternative interpretations of privacy rights within the states could gain influence at the national level, as has happened before on other issues including the exclusionary rule and the death penalty, where state law has influenced interpretations of "evolving standards of decency" under the Eighth Amendment.[97]

Second, divergent state interpretations on privacy are also a symptom of unease with the current state of the law, and to some extent they highlight the arbitrariness and indeterminateness of privacy law as it now stands. They are also, not incidentally, a source of privacy protection for a large number of people. As the majority noted in *Katz*, "the protection of a person's *general* right to privacy – his right to be let alone by other people – is, like the protection of his property and of his very life, left largely to the law of the individual States."[98]

The problem, of course, is that unlike state protections against theft and murder, state and federal privacy laws collectively do not yet provide individuals anything resembling reliable certainty that they will be protected, especially with today's rapidly evolving technology.

## IV. Conclusion: Toward a New Fourth Amendment

Our legal system moves slowly via common law evolution. A problem with evolutionary change, however, is that it can get stuck in what evolutionary theorists term a "local peak" in the fitness landscape – a suboptimal state that requires a large, discontinuous shove in order to come

---

[93] The states that have rejected federal third party doctrine are, in rough descending order of the strength of their protection, California, Washington, New Jersey, Montana, Colorado, Illinois, Pennsylvania, Hawaii, Florida, Idaho, and Utah.

[94] The states that have indicated an openness to doing so are Alaska, Massachusetts, Minnesota, New Hampshire, Oregon, Indiana, Vermont, Arkansas, and South Dakota.

[95] Those states are Arizona, Connecticut, Delaware, Louisiana, Michigan, Nevada, New Mexico, New York, Ohio, Texas, Tennessee, and Wyoming.

[96] RABBAN, *supra* note 47, at 131-132.

[97] Stephen E. Henderson, *Learning From All Fifty States: How To Apply the Fourth Amendment And its State Analogs To Protect Third Party Information From Unreasonable Search*, 55 CATH. U.L. REV. 373 (2006); Mapp v. Ohio, 367 U.S. 643 (1961)); Atkins v. Virginia, 536 U.S. 304, 314-317 (2002).

[98] Katz v. United States, 389 U.S. 347, 350 (1967) (quotations omitted).

into better alignment with current conditions.[99] The Fourth Amendment, as it is now interpreted, is highly inadequate to protect the substantive privacy rights that Americans have always enjoyed. Unlike so many other rights, privacy in America today is actually in many respects far weaker than in the past.

It could be argued that our society has simply evolved toward requiring less privacy than individuals expected in the 18th century. It could be that all the liberationist social trends and movements in the years between have rendered a broad range of human activity simply less scandalous than it was in more straight-laced times.

Even so, privacy will never stop being a vital human right. If, as it often seems, our culture is evolving in a more open and freewheeling direction, where people feel more at liberty to disclose more things about themselves, that is all to the good. But it is important that such disclosures be voluntary, and under the individual's control, and that the framework of our fundamental rights remains sound. There is still a broad range of personal preference in our society when it comes to privacy intuitions and desires, and individuals still need the right to have those preferences respected as much as possible. Privacy does not mean keeping secrets. Rather, it means having the power to keep them if you wish, and especially not to be forcibly stripped of them by the government or others. While it is a sign of progress that people have less to fear from what might once have been ruinous disclosures, human beings will always need space to think and to converse privately, to experiment, to create and define themselves, and to exercise control over their reputations and "presentation of self" to various audiences.

With today's accelerating technological revolution, however, the inadequacies of our Fourth Amendment law are facing a crisis point. The history of the First Amendment suggests that reform is possible when it comes to privacy, and there are several places to which we can look as sources for change: a vigorous line of Supreme Court dissents to key Fourth Amendment cases and state constitutional jurisprudence, which suggest alternatives shapes for the law. And the originalist approach that Justice Scalia and others have taken to privacy suggests the basis for the kinds of Supreme Court coalitions necessary to change the direction of federal jurisprudence. We must work to make this happen, lest America become a meaner, less forgiving, less just, and less free place.

[99] *See, e.g.*, STUART KAUFFMAN, AT HOME IN THE UNIVERSE: THE SEARCH FOR THE LAWS OF SELF-ORGANIZATION AND COMPLEXITY 149-90 (1995).