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
-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
information shared with any third party loses all Fourth Amendment protection; and (2) the

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*

---

*
hnology
Program. The author would like to thank former ACLU legal intern Jeremy Wolff for his excellent research on the Fourth Amendment jurisp8teC6(r)-3(is)4(p8teC6(r)-3(is)4(p8d16(r)-14(4(p8teC6(r)-3(is)4(p8d1ETBT1 0 0 1 72-4e)-111t)-2(o)-14(f)8t

fronts in attempting to defend our privacy. But ultimately, constitutional protection is needed.

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

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*

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 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

2.

it passes through the network of servers that make up the Internet, and when it arrives it is stored
s 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

system in which the Tr
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 [42] all cash transactions of $10,000 or more [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]

telephone and email communications. This was done first under the
(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

Constitution is there to protect us, it is to be expected that this kind of routine wholesale

le
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

tional.[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

articles by Harvard law professor Zechariah Chafee.[56]

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.

third party doctrine and in some ca

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. ▯

United States v. White, the 1971 case about

Katz he way toward a broader, more substantive, and non-circular standard for privacy.[63]

efore the

[64] He then evaluated the actual substantive effect of wearing a

> 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

[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.

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

A footnote in the majority opinion in *Smith* could also serve as fuel for future courts wishing to redirect Fourth Amendment la

[71] Such

Government were suddenly to announce on nationwide television that all homes henceforth
[72]

> recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was.
>
> 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

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 he *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 [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

[75]

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.*

[81] -

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 [82]

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
>
> 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

-day equivalent electronic files in all their forms and provides protection for them. A richer privacy jurisprudence might [84]

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

[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] acy 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*, 557C1(2 792.12 reW*)n /P <MCID 12>BD831] TJETE

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

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

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 sign

[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 ndment.[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* *general* right to privacy his right to be let alone by other people is, like the protection of his property and of his ve [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 certaint

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
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).