Denver Law Review

Volume 79
Issue 4 *Symposium - Privacy*

Article 3

December 2020

Little Brothers Are Watching You - The Importance of Actors in the Making of Fourth Amendment Law

Sam Kamin

Little Brothers Are Watching You:

The Importance of Private Actors in the Making of Fourth Amendment Law[1]

It is something of a truism in criminal procedure (as elsewhere in constitutional law) that unless the conduct of a government agent is involved, the Constitution is not implicated.[3]

Thus, if a Federal Express employee acting on her own initiative opens a shipped package that turns out to contain drugs and then gives these drugs to law enforcement, no search has occurred.[4] Similarly, if a hotel manager searches the room of a guest and then turns over any contraband he finds to the government, no search has occurred.[5] So long as the private citizen is acting as such and not at the direction or encouragement of law enforcement,[6] the government is free to use the discovered material without concern for its exclusion at trial.[7] To the extent that actions by private actors ever find their way into our consideration of criminal procedure, it is generally to prove this point: only the government and its agents can be found to have violated the Fourth Amendment.

In this essay, I argue that this focus on state action has distracted both scholars and practitioners from an important point: the interrelationship between privacy vis-à-vis private actors and privacy vis-à-vis the government. While it is true that the absence of a state actor means that a Fourth Amendment search has not been conducted, it does not follow from this fact that Fourth Amendment doctrine is unaffected by such invasions of privacy. Quite the contrary: I argue that the more privacy an individual surrenders to private actors, the less privacy he will have from the government. The more we become inured to our neighbors, employers, creditors, and advertisers having greater and greater access to areas we think of as private, the more we run the risk that the government will have unfettered access to them as well.

The principal basis for this argument is the Supreme Court's decision in *Katz v. United States*[8] and the line of precedent that it has spawned. In *Katz*, the Supreme Court stated that a search occurs and the Fourth Amendment is implicated whenever the government invades an area in which an individual has a reasonable expectation of privacy.[9] The Court held that whether an

"INSTEAD of asking whether the place searched...is a place entitled to Fourth Amendment protection...the question became whether the defendant behaved in a way that demonstrated his subjective belief that the place searched was entitled to protection..."

individual is entitled to Fourth Amendment protection depends not on where the search of the object takes place, but rather on how the individual and society treat that area.[10] Thus, as the court put it:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . [b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[11]

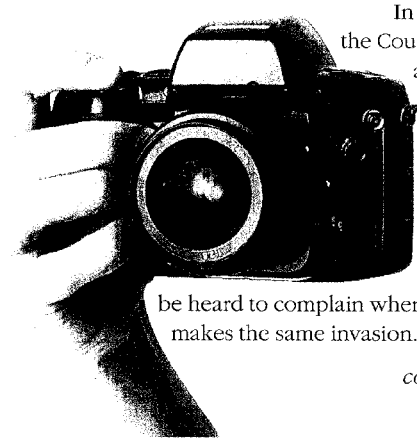
Instead of asking whether the place searched — in *Katz* a public phone booth — is a place entitled to Fourth Amendment protection in the abstract, the question became whether the defendant behaved in a way that demonstrated his subjective belief that the place searched was entitled to protection, and whether society is willing to validate that belief as reasonable.[12]

On a case-by-case basis over the last thirty-five years, the contours of the Fourth Amendment under *Katz* have come into focus. I argue that one thing that has become very clear is that even things in which one generally has a very high privacy interest — one's home, one's business records, etc. — can be searched by the government without implicating the Fourth Amendment if one has permitted others to have access to these things. If an individual has given up a reasonable expectation of privacy in his property or information by exposing them to the view of others, he cannot attempt to deny the government similar access to these areas.

Of course, in these cases one rarely waives an interest in property or information explicitly. Instead, in a number of contexts, courts have inferred from a defendant's actions that he could not have had a privacy interest in his activities, or that such an interest could not be reasonable. For example, in *California v. Greenwood*[13], the Supreme Court held that no search occurred when police removed trash that Greenwood had placed by the side of the road for collection.[14] Without explaining whether Greenwood had demonstrated that he did not expect his discarded trash to be kept secret, or whether that expectation of privacy, even if actually entertained by the defendant, was not reasonably held, the Court simply reasoned that there could not be a reasonable expectation of privacy in something consciously abandoned.[15]

The Court's reasoning was clearly influenced by the fact that by putting the trash in front of the house, Greenwood had made it available not just for sanitation workers but for anyone else who happened by. The Court stated, "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."[16] Furthermore, the Court reasoned, the sanitation workers themselves, once in possession of the trash, might have conveyed it to anyone else.[17] Thus, because the police officers merely did what any other member of the public could have done — looked through the trash that had been left out — they did not invade Greenwood's reasonable expectation of privacy.

In reaching this conclusion, the Court analogized to other, earlier examples of this line of reasoning. For example, in *Smith v. Maryland*[18] the Supreme Court held that the installation and use of pen registers — devices that allow law enforcement to access and record all of the numbers dialed from a particular phone — was not a search subject to the requirements of the Fourth Amendment. The Court held that the installation and use of these devices (by the phone company at the direction of law enforcement) was not a search because in the course of using his phone, the defendant voluntary conveyed information to the phone company about the numbers he was dialing.[19] Thus, Smith knew (or at the very least should have known) that he was transmitting this information to a third party, and "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[20] Similarly, in *United States v. Miller*,[21] the Supreme Court ruled that records held by banks may be subpoenaed without invoking the Fourth Amendment. The reasoning was the same: "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[22] Like Greenwood putting out her trash, Smith and Miller had essentially abandoned their privacy interests by allowing others access to their information.[23]



In still other contexts, the Court has held that when an individual has simply failed to protect herself from an invasion of privacy that a member of the public could have made, she will not be heard to complain when the government makes the same invasion. For example, in

continued on page 553

continued from page 545
The courts recognize a privacy interest in medical records and then balance that interest against various legitimate purposes associated with disclosing that information.

V. The HIPAA regulations adopt and seek to implement the privacy interests and balancing tests developed in the various cases.

In 1996, Congress enacted the Health Insurance Portability and Accountability Act ("HIPAA").[103] Among other things, HIPAA required Congress to enact new safeguards to protect the security and confidentiality of health care information. Congress failed to do so, requiring the Department of Health and Human Services ("HHS") to promulgate regulations for such protections.[104] In November of 1999, HHS published proposed regulations and, during the comment period, received 52,000 communications from the public.[105] In December 2000, HHS issued the final rule that took effect on April 14, 2001.[106] However, most covered entities have until April 14, 2003 to comply with the final rule's provisions.[107] The HIPAA regulations are intended to establish a set of basic national privacy standards to serve as a floor of ground rules for health care providers, health plans and health care clearinghouses to follow.[108]

In promulgating the regulations, HHS considered the need for privacy of medical records to be great.[109] The HHS recognized a "growing concern" stemming from several trends, "including the growing use of interconnected electronic media for business and personal activities, our increasing ability to know an individual's genetic make-up, and, in health care, the increasing complexity of the system."[110] Unless those public concerns were allayed, the HHS believed we would be "unable to obtain the full benefits of electronic technologies. The absence of national standards for the confidentiality of health information has made the health care industry and the population in general uncomfortable about this primarily financially-driven expansion in the use of electronic data."[111] The HHS focused on one of the same concerns that was recognized by various courts, the consequences of sharing information without the knowledge of the patient involved.[112]

In concluding that "privacy is a fundamental right," HHS looked to judicial authority and, in particular, to the *Whalen* decision.[113] In several aspects, the HIPAA regulations have followed the guidance from the federal courts.[114] In relying on this federal authority, HHS did not specifically address the fact that the judicial authority it cited related to the right to privacy from the perspective of government actors rather than the private sector, which is not subject to the constitutional restrictions.[115]

There are several principles from the federal decisions that are reflected and expanded in the HIPAA regulations. First, the cases generally accept that there is an expectation of privacy in medical records, although the extent to which it reaches a constitutionally protected right may be debated.[116] In promulgating the regulations, HHS characterized privacy as a "fundamental right" and concluded that the "United States Supreme Court has upheld the constitutional protection of personal health information" in *Whalen*.[117] Second, the HIPAA regulations focus on the first type of individual privacy protection identified in *Whalen*, the protection for medical records.[118] The HIPAA regulations do not seek to protect medical decision-making, an interest also largely ignored by the courts.[119] Third, the HIPAA regulations acknowledge that the right to privacy "is not absolute" and must be balanced against legitimate

continued on page 556

continued from page 518
California v. Ciraolo[24], the Court held that an overflight of the defendant's property by a police airplane did not amount to a search, on the unusual ground that the plane was in FAA approved air space. The Court's rationale for this rule was that no expectation of privacy could be reasonable, as "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed."[25] Here, the individual's fault is not conveying information to a third party, but failing to properly safeguard his property:

> That the area is within the curtilage does not itself bar all police observation. The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible.[26]

In its most recent Fourth Amendment case, *Kyllo v. United States*,[27] the Court held that the use of thermal imaging technology to measure the heat coming off of a dwelling was a search subject to the requirements of the Fourth Amendment. The Court held that because the device provided details about the interior of a home that could not otherwise be obtained without trespassing into the home and because the device had not yet entered into general use, its use constituted a search.[28] The flip-side of this argument appears to be that had the device used by the police

continued on page 574

continued from page 553
been in regular public use at the time that it was used to scan Kyllo's home, Kyllo's failure to take precautions against the device would be proof of his lack of a reasonable expectation of privacy in the heat coming off his house. Just as Ciraolo's case would have come out very differently 100 years ago (when airplanes were unknown) than today, so Kyllo's case might come out very differently 10 years from now when the use of thermal imaging technology becomes better known to the public.

This leads me back to my original thesis. What all of these cases demonstrate is that if an individual has allowed private actors to look into areas that would otherwise be private, he has invited the government in as well. Even if others were invited in for a narrow and specific purpose, the individual has run the risk that her trust will be abused. Similarly, even if one has behaved passively, not conveying or showing information to anyone, but simply failing to take precautions against intrusions by others, she has likely lost an expectation of privacy in the area she has carelessly exposed. Furthermore, precautions that might be sufficient to protect an expectation of privacy in one era — for example, protecting the four sides but not the roof of a shed from public view — will be deemed insufficient in another.

This is why I argue that privacy vis-à-vis private actors is crucial in defining the contours of Fourth Amendment law. In recent years, technological changes have made surveillance easier, cheaper, and much more pervasive. For example, a recent report indicated that more than one third of the United States work force is subject to workplace monitoring of their web use and e-mails.[29] Microsoft, which makes the vast majority of the operating systems in the world, placed code in its Windows XP operating system that records the titles of DVDs watched on an individual's computer and transmits this information back to the company "in a way that allows the company to match individuals with their music and movie choices."[30] Night vision goggles, long-distance microphones, and personal tracking devices can all be purchased by members of the public on the Internet for under $1,000.[31] While it was once possible to defeat nosy neighbors, prying employers, or avaricious marketers simply by shutting the door and keeping your voice down, such precautions are simply insufficient today.

As these examples illustrate and as many have written, much of this new surveillance technology has been adopted not by the government,[32] but by the so-called Little Brothers — advertisers, employers and other private snoops, who many argue pose a greater threat to privacy than is posed by government's Big Brother.[33] What has been less understood, however, is that the more power the Little Brothers gain, the more power Big Brother gains. Every time a Little Brother gains access to an area previously forbidden to him, it becomes easier for Big Brother to later claim that a defendant's reasonable expectation of privacy has been lost.

Thus, those of us interested in the amount of government intervention into our private lives should be deeply concerned with the extent to which others are allowed in. If we allow our employers to read our e-mails, we cannot very well complain when the government does so as well. If we allow our software companies to learn what movies we are watching, we cannot complain when the government does so as well. Yet we cannot do anything to eliminate the technologies that are making privacy more fleeting; technological fixes — encryption, wiretap blocking, etc. — will only lead to new and different technological responses by those who would invade our privacy. What is needed is a legal response, one that makes actionable the use of technology by private actors to obtain information that an individual has taken steps to keep private.

If it is a violation of statute for private actors to gain access to information in which an individual has a reasonable expectation of privacy, if those whose privacy has been invaded can bring a private cause of action akin to trespass against those who have invaded their privacy, then privacy can be preserved even in the face of technological change. Just as the possibility that private actors might break into your house and rifle through your things does not allow the government to freely break in and snoop around, so the tortious privacy invasion of a third party will not give the government carte blanche to snoop. So long as third party privacy invasions violate no laws, however, they will only embolden those in government who seek greater access to private information and will make it more difficult for any of us to claim that we should be protected from government attempts to get at this information

The current war against terrorism has energized civil liberties groups to respond to governmental attempts to extend surveillance of citizens and non-citizens alike. Of course, these attempts to control the worst excesses of government are laudable. But if civil libertarians wait until the government acts to invade privacy, they will have lost the battle before it has even begun.

Sam Kamin is an assistant professor of law at the University of Denver where he teaches Criminal Law, Criminal Procedure, and the Death Penalty. He is currently completing a book on the death penalty decisions of the California Supreme Court.