



2013

Preserving Privacy in a Digital Age: Lessons of Comparative Constitutionalism


David Cole

Georgetown University Law Center, cole@law.georgetown.edu

This paper can be downloaded free of charge from:
<https://scholarship.law.georgetown.edu/facpub/1310>
<http://ssrn.com/abstract=2383935>

David D. Cole, *Preserving Privacy in a Digital Age: Lessons of Comparative Constitutionalism*, in *SURVEILLANCE, COUNTER-TERRORISM AND COMPARATIVE CONSTITUTIONALISM* (Fergal Davis, Nicola McGarrrity & George Williams, eds., New York: Routledge 2013)

This open-access article is brought to you by the Georgetown Law Library. Posted with permission of the author.
Follow this and additional works at: <https://scholarship.law.georgetown.edu/facpub>

 Part of the [Constitutional Law Commons](#), [Fourth Amendment Commons](#), [National Security Law Commons](#), and the [Privacy Law Commons](#)

7 Preserving privacy in a digital age

Lessons of comparative constitutionalism

David Cole

7.1 Introduction

Like so much else, privacy these days is not what it used to be. In November 2012, Central Intelligence Agency (CIA) Director, David Petraeus, a much-decorated four-star general, resigned when a Federal Bureau of Investigation (FBI) inquiry into anonymous email threats to a woman in Tampa, Florida, disclosed, in the “Drafts” folder of a joint Gmail account, that Petraeus was having an affair with his biographer. The latter had sent the threatening emails to the Tampa woman in a jealous pique. The FBI investigation included examination of some 30,000 pages of emails, and also revealed potentially inappropriate emails between the recipient of the threats and General John Allen, the United States’ (US) top commander in Afghanistan. The military launched a public investigation of Allen’s allegedly “flirtatious” emails, which ultimately cleared him of any wrongdoing – but not before he and his correspondent’s names were dragged through the media mud. In the “old days”, such affairs and flirtations would have left no such electronic trail, in all likelihood would never have been discovered, and would have been deniable if they were. No longer.

In October 2012, the *New York Times* reported that the campaigns of President Barack Obama and his challenger, Mitt Romney, were using sophisticated data-mining tools to access detailed information about potential voters, in order to target their appeals. It reported that:

[C]onsultants to both campaigns said they had bought demographic data from companies that study details like voters’ shopping histories, gambling tendencies, interest in get-rich-quick schemes, dating preferences and financial problems. The campaigns themselves, according to campaign employees, have examined voters’ online exchanges and social networks to see what they care about and whom they know. They have also authorized tests to see if, say, a phone call from a distant cousin or a new friend would be more likely to prompt the urge to cast a ballot.

The campaigns have planted software known as cookies on voters’ computers to see if they frequent evangelical or erotic websites for clues to their moral perspectives. Voters who visit religious websites might be

greeted with religion-friendly messages when they return to mittromney.com or barackobama.com. The campaigns' consultants have run experiments to determine if embarrassing someone for not voting by sending letters to their neighbors or posting their voting histories online is effective.¹

In the modern age, we increasingly live our lives through, and accompanied by, digital media. Virtually every transaction or communication that uses such media, as well as every move of mobile phone owners, is recorded. Computers are able to store, transmit, and analyze the data as never before, drawing on multiple sources to construct an intimate picture of our interests, contacts, travels and desires. Private data-mining services, most often used for commercial advertising purposes, can determine: what we read, listen to, and look at; where we travel to, shop, and dine; and with whom we speak or associate. Meanwhile, social networking sites such as Facebook encourage individuals to broadcast their personal lives to ever-increasing networks of "friends". Privacy, many pundits declare, is dead.

The legal consequences of these developments largely remain to be worked out, as technology has advanced much more rapidly than the law. Courts have begun to confront the implications of new technology, as police and prosecutors increasingly rely on such tools to guide their investigations and make their cases.² American mobile phone service providers reported that, in 2011 alone, they responded to over 1.3 million requests from law enforcement for mobile phone data, including text messages, location data, and subscriber information.³ From 2005 to 2010 British public authorities made 2.7 million requests for communications data to private service providers.⁴ How should the law adapt to the new reality of this digital age?

In 2012, the US Supreme Court (USSCt) issued what could be one of its most important privacy decisions in decades, as it took up one version of this issue – namely, whether police use of a global positioning system (GPS) device to monitor the public movements of a car for a month amounted to a search subject to constitutional constraints. The case of *United States v Jones (Jones)* generated a surprising unanimous decision concluding that the prohibition on unreasonable searches in the Fourth Amendment to the US Constitution was implicated, but the justices were sharply divided in their reasoning.⁵ Some justices looked back to notions of property to find that the police action was a search; others looked forward, warning that technology enables the police to invade privacy in ways unheard of when the Fourth Amendment was adopted. That division of reasoning and outlook is emblematic of the uncertainty that new technology has created for the constitutional law of privacy.

As Chapter 9 by Federico Fabbrini and Mathias Vermeulen in this volume ably discusses at length, the European Court of Human Rights (ECtHR) addressed virtually the same issue two years earlier in *Uzun v Germany (Uzun)*.⁶ The ECtHR, like the USSCt, affirmed that the use of such technology invaded the right to respect for private life, guaranteed by art 8 of the

European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).⁷ It ruled, however, that in the instant case, the interference was justified for a number of reasons: the crimes under investigation were serious; the authorities had tried other, less intrusive means of surveillance, but the targets had frustrated those efforts (by, for example, disabling a radio transmitter found in a friend's car before the GPS was installed); and the law contained a number of safeguards and checks, including the possible remedy of exclusion of the evidence from a criminal trial if it was found to have been obtained illegally.

That the USSCt and the ECtHR reached similar conclusions with respect to the critical threshold issue of whether GPS monitoring implicates privacy concerns suggests that reports of privacy's death are, like those of Mark Twain's, greatly exaggerated. We remain free to adapt domestic and international protections to safeguard privacy. But adaptation will clearly be necessary. The challenge hardly stops at the GPS device. Widely available technological innovations – including smart phones, unmanned aerial drones, and computer data-mining programs – make it possible to watch citizens more intimately and comprehensively than was remotely conceivable when the US Constitution, or even the ECHR, was adopted. These devices give the state the ability to follow virtually our every movement in public as well as many in private, our every keystroke at the computer and our every electronic transaction or communication.

In 1956, at the height of McCarthyism in the US, sociologist Edward Shils wrote that liberal democracy demands confidentiality for its citizens and transparency for its government.⁸ Today, it is the citizenry that is increasingly transparent, while government operations are shrouded in secrecy. That development poses a serious challenge not merely to privacy but to liberty and democracy. Sir Thomas Erskine May's words from 1863 apply with equal if not greater immediacy 150 years later:

Next in importance to personal freedom is immunity from suspicions and jealous observation. Men may be without restraints upon their liberty; they may pass to and fro at pleasure; but if their steps are tracked by spies and informers, their words noted down for crimination, their associates watched as conspirators – who shall say that they are free? Nothing is more revolting to Englishmen than the espionage which forms part of the administrative system of continental despotisms. It haunts men like an evil genius, chills their gaiety, restrains their wit, casts a shadow over their friendships, and blights their domestic hearth. The freedom of this country may be measured by its immunity from this baleful agency.⁹

The question posed in both *Jones* and *Uzun*, at its most general level, confronts every nation in the 21st century: how should law respond to ensure that technology does not erode privacy altogether, when computers, satellites,

of conspiracy to distribute cocaine and crack cocaine, and sentenced to life imprisonment.

The US Court of Appeals for the District of Columbia Circuit ruled that the GPS monitoring of Jones' car violated the Fourth Amendment ban on unreasonable searches and seizures. It reasoned that such extensive monitoring, by compiling a wealth of detail about an individual's movements, constitutes a search and must be justified under the Fourth Amendment. The Obama Administration sought review in the USSCt, contending that the monitoring obtained only public information and invaded no privacy. Therefore, the government maintained, use of the GPS required no warrant, no probable cause, not even any individualized suspicion of wrongdoing.

Government lawyers were confident that they would prevail in the USSCt, and not without reason. The USSCt had ruled in 1983 that a police officer's use of a radio transmitter, or beeper, to assist in trailing a car on public roads as it traveled through the night from an airport to a house in the country some 100 miles away was not a search, and therefore not subject to the legal restrictions of the Fourth Amendment.¹⁴ It reasoned that the beeper merely assisted the police in capturing information that was already public – the route of an automobile on public roads. Since this information was not private to begin with, the USSCt concluded, the driver had no “reasonable expectation of privacy” triggering Fourth Amendment protection.

In *Jones*, the government argued that if using technology to monitor a car as it travels from A to B does not invade privacy, then it also invades no privacy to monitor a car as it travels from A to B to C to Z, and back, even around the clock for a month. As Scalia J expressed the government's point during oral argument in the USSCt, “[a] hundred times zero equals zero. If – if there is no invasion of privacy for one day, there's no invasion of privacy for a hundred days.”¹⁵

To the surprise of many observers, the USSCt unanimously rejected the government's argument, concluding that the use of the GPS device did constitute a search regulated by the Fourth Amendment. The unanimous result, however, masked substantial disagreement among the nine justices. The case generated three different opinions. Two, the majority opinion of Scalia J and a concurrence of Alito J, advanced starkly different approaches to the issue. The third opinion, by Sotomayor J, appeared to register sympathy with *both* of the competing approaches, while going further to suggest the need to rethink Fourth Amendment doctrine more systematically in the face of new technological realities.

Justice Scalia resurrected a long-dormant Fourth Amendment doctrine that linked privacy to property, and concluded that the attachment of the GPS device to Jones' car was a “search” because it was a trespass for the purposes of gathering information. The USSCt had for many years relied on property notions in interpreting the scope of the Fourth Amendment but, since 1967, it had focused instead on whether the police action invaded a “reasonable expectation of privacy”. Justice Scalia, long skeptical of that

concept for its open-ended nature and its lack of support in the “original understanding” of the Fourth Amendment, reasoned that in this case, no inquiry into “reasonable expectations of privacy” was required because there could be no dispute that installing a GPS device on someone else’s property is a “trespass” conducted for the purpose of gathering information. Five justices joined Scalia J’s opinion, making it the controlling opinion of the USSCt.

However, Alito J, writing for four justices, rejected Scalia J’s resort to notions of property and trespass as outmoded and superseded by the USSCt’s adoption of the “reasonable expectation of privacy” test in 1967. He argued that the focus on trespass was overly formalistic, might vary from state to state based on local property laws and was a poor proxy for the true purpose of the Fourth Amendment – the protection of privacy. He reasoned that Jones had a reasonable expectation that the government would not monitor his every movement in public around the clock for a month. It is unreasonable to expect that a single trip on a public road will remain private, but reasonable to expect that the full pattern of one’s public movements over a month will remain private. Thus, Alito J sought to retain the doctrinal focus on “expectations of privacy”, but concluded that here, unlike in the case involving a single trip, legitimate expectations of privacy had been infringed by the scope of the information gathered.

The two justices reached the same conclusion in *Jones*, but their approaches would lead to different results in other cases. If the police affixed a GPS device to a car and monitored it only for a single ride on a public street, Scalia J would presumably treat that as a search because it would be a trespass for the purposes of gathering information. Justice Alito would not, because he did not question the existing precedent holding that one has no reasonable expectation that a single public trip will remain confidential. By contrast, if the police obtained a month’s worth of location data from a private company that had installed a GPS device in the car at manufacture (such as OnStar, a GPS device in many new cars that enables emergency responders to identify a car’s precise location when an accident happens), Alito J would presumably treat that as a search, because it constitutes the same invasion of privacy as in *Jones*. Justice Scalia would not, because there would be no trespass.

Justice Sotomayor concurred separately. She formally joined Scalia J’s approach but also seemed to endorse Alito J’s approach. In this sense, there may, for all practical purposes, be two majority opinions in *Jones*. Justice Sotomayor called for a rethinking of Fourth Amendment jurisprudence in the digital age. Perhaps most significantly, she pointed to the need to reconsider the USSCt’s “third-party disclosure” doctrine. That doctrine provides that individuals assume the risk that any information they share with others may be transmitted to the government by those with whom it is shared, and therefore have no Fourth Amendment objection to the government obtaining that information from the “third party”. On this rationale, the USSCt has permitted the police to rummage through garbage, obtain bank records, and

place recording wires on informants engaged in private conversations without any constitutional constraints. In the digital world, this principle has vast repercussions because, unless one lives as a hermit, virtually everything one does requires sharing information with a third party – whether it be a credit card company, internet service provider, phone company, bank, or grocery store. Computers make it feasible for these entities to keep accurate records of these transactions and for the government to collect and analyze the data. Justice Sotomayor suggested that these facts may justify revisiting that doctrine, which has taken on implications in the digital age that were unthinkable when the doctrine was first announced.

The USSCt's efforts to confront the impact of technology on privacy, and not simply to stand by as technology erases the private realm, are laudable. The *Jones* decision may have important implications for other technologically enhanced forms of surveillance. Justice Alito's recognition that extended GPS monitoring invades reasonable expectations of privacy might suggest that computer data-mining, in which the government similarly collects and aggregates lots of otherwise unprotected information to compile a comprehensive picture of an individual's private activities, also triggers Fourth Amendment protection. While Fourth Amendment doctrine provides that border searches generally enjoy little or no constitutional protection, Alito J's approach might imply that searches of laptops at the border necessitate greater protection. Similarly, while Fourth Amendment doctrine now holds that obtaining information from a phone company about the numbers its users call, and how long they are connected, does not implicate the Fourth Amendment, Alito J's approach might imply that the collection of mobile phone location tracking data deserves Fourth Amendment protection, especially when used over an extended time to construct a pattern of private activity. As with the GPS, we do not reasonably expect the government, short of these technological advances, to be able to learn everything about us that a laptop can reveal simply because we are crossing the border, or to be able to learn our every move in public simply because we carry a smart phone. Justice Sotomayor also appears to be sympathetic to such arguments.

The majority approach articulated by Scalia J has less potential to address the threats posed by the digital age. It protects against intelligence gathering techniques when they require the state to trespass on an individual's privacy. But technology makes trespass less and less necessary in order to obtain private information. Indeed, that fact was the reason the USSCt adopted the "reasonable expectation of privacy" standard in confronting electronic wire-tapping in 1967. Still, Scalia J's opinion is agnostic with respect to non-trespassory investigative tactics. And since four justices signed Alito J's opinion, and Sotomayor J's appears to be at least as sensitive to the need to protect privacy from new threats, this opinion might ultimately prove more influential over time.

The *Jones* case, however, only scratches the surface. What sorts of adaptation are necessary to ensure that privacy remains a protected value in liberal

democracies? The following section will explore a number of proposals from constitutional scholars.

7.3 Alternatives to privacy in the modern age?

Many constitutional scholars have taken up the challenge of rethinking privacy protection in the digital age. This section will review four such proposals. Each offers important insights. In the end, however, their proposals are insufficient to meet the challenge.

In *One Nation under Surveillance*, Chesterman argues convincingly that the spectre of catastrophic terrorist attacks creates extraordinary pressure for intrusive measures in the name of prevention; technological advances have made the collection and analysis of vast amounts of previously private information feasible and relatively inexpensive; and, finally, in a culture transformed by social media, in which citizens are increasingly willing to broadcast their most private thoughts and acts, privacy may already be as outmoded as chivalry. His concerns are well founded. In 2010 the *Washington Post* reported that:

[T]he top-secret world the government created [in response to the terrorist attacks of September 11, 2001], has become so large, so unwieldy and so secretive that no one knows how much money it costs, how many people it employs, how many programs exist within it or exactly how many agencies do the same work.¹⁶

The *Washington Post* found that 1,271 government organizations and 1,931 private contractors do national security-related work and more than 845,000 people have “top-secret” security clearances. Most or all of what these individuals and entities do is hidden from public view.

The statutory and administrative regulations limiting surveillance have been substantially eased since 9/11. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act) allowed prosecutors to bypass established limits on criminal wiretaps and searches whenever they could say that the investigation also involved foreign intelligence gathering.¹⁷ It expanded the FBI’s use of “national security letters”, which enable its agents to obtain credit reports, financial records, and personal internet subscriber records without judicial supervision.¹⁸ Attorneys-General John Ashcroft and Michael Mukasey each watered down executive branch guidelines governing FBI investigations after 9/11.¹⁹

In Chesterman’s view, it is futile to put up much of a fight against the state’s collection and analysis of massive amounts of information about our personal lives. The fears of terrorism are too deep, the technology is too advanced and the populace has already been seduced into forfeiting its privacy by Facebook and other modern conveniences. He proposes that we

instead forge a new “social contract” setting forth the terms on which we allow the government to *use* such information. But the terms he proposes are frustratingly skeletal. Chesterman contends that intelligence should be guided by three principles: first, that it be carried out by public authorities rather than private contractors; second, that it be based on law; and, finally, that it be ‘consequence sensitive’. There is nothing objectionable about any of these suggestions. Intelligence operations often involve a great deal of discretion and judgment, and we might well prefer that they be carried out by politically accountable government actors rather than profit-seeking private contractors. Actions guided by law are definitely better than lawlessness. And who could be against sensitivity to consequences? But it is less clear that such a “contract” would really solve the problems of privacy in the age of surveillance. The devil is in the details, and Chesterman does not offer many.

Take his objection to the use of private contractors for intelligence operations. He reports that 70 percent of the US intelligence budget goes to private contractors, who on average charge twice what it would cost a government official to do the same task. In 2005 that amounted to US\$42 billion on private contractors. But certainly private contractors are appropriate for some intelligence work, just as they are for some defence work. And the abuses by contractors that Chesterman identifies – rendition, coercive interrogation, and warrantless wiretapping – were also committed by public officials and would have been just as objectionable had they been implemented exclusively by public authorities. At the root of each of these abuses was not unregulated private outsourcing, but the decisions of public officials who expressly authorized such acts.²⁰ And while Chesterman may be right to focus on the use rather than the collection of data, are use restrictions enough? If we give up on restricting collection, what is left of privacy? The invasion of privacy occurs when the government gains access to information we think it should not have; how it then uses the information is less an issue of *privacy* than of other concerns, such as discrimination, retaliation, due process, and the like. The last concerns are indisputably important, but they are not substitutes for privacy itself.

Solove advocates a reconceptualization of the Fourth Amendment. He suggests that courts should not ask whether government access to an individual’s web browsing history, for example, invades a “reasonable expectation of privacy”, but instead whether it “causes problems of reasonable significance” by, for example, creating the potential for government abuse.²¹ Any government action that poses such “problems”, he argues, should be subject to Fourth Amendment regulation by courts, regardless of its impact on privacy. The USSCt is unlikely to look with favor on this suggestion. The Fourth Amendment by its terms demands only that “searches and seizures” be reasonable, not that all government action be reasonable. Solove is correct that the USSCt has defined what constitutes a search too restrictively, but inviting it to oversee all “problems of reasonable significance” is not a sufficiently tailored alternative.

Kerr advances what he calls an “equilibrium-adjustment” theory of the Fourth Amendment.²² He argues that the USSCt’s Fourth Amendment doctrine, often criticized as incoherent and internally contradictory, is best understood as an effort to maintain a fair balance between the police and potential criminals. Where technological developments make it easier for criminals to commit crime – as in the development of the automobile, which facilitated robberies, smuggling, and other crimes – the USSCt adjusts Fourth Amendment doctrine to make it easier for the police to investigate and interdict criminals using that technology. Thus, the USSCt created an “automobile exception” to its general Fourth Amendment rule that searches must be authorized in advance by a judicial warrant.²³ And, as alluded to above, when wiretapping technology made it possible for the police to eavesdrop on private phone conversations without trespassing on property, the USSCt abandoned its focus on trespass and proclaimed that the Fourth Amendment protects “reasonable expectations of privacy”, even when there has been no intrusion on a property interest.²⁴

Kerr maintains that this theory is not only an accurate description of what the USSCt has done, but also reflects what it should do as a normative matter. The Fourth Amendment should be interpreted so as to maintain the balance between police and criminals that existed at what Kerr calls “year zero”. This is a purposefully vague concept that has no specific time reference, but appears to identify the balance between the state and the citizen before it was altered by technology. On Kerr’s view, courts confronting new technological developments should assess whether a particular development has tipped the balance of power between the police and potential criminals in the direction of the state or the private citizen, and “adjust” Fourth Amendment doctrine so as to maintain the status quo.

Kerr’s view contains an important insight. Privacy protections, whether found in a constitution or an international treaty, are premised on a particular state of affairs. One way of conceptualizing a court’s role going forward is indeed to interpret the law to preserve that status quo in the face of real world developments. In some sense, that is what Alito J sought to do in his *Jones* concurrence. He asked what expectations of privacy citizens would have in the absence of GPS technology, and then concluded that because the technology allowed the state to invade that expectation in ways that the police could not realistically have done without it, its use should be treated as an invasion of privacy triggering Fourth Amendment protections.

It is not clear how Kerr’s approach differs from conventional understandings of Fourth Amendment doctrine. Under what some have called constitutional common law, courts begin with an understanding of the purposes of the Fourth Amendment and then apply these to new factual scenarios over time, generating a jurisprudence that builds organically on itself.²⁵ Kerr seeks to distinguish his approach from common law methodology by maintaining that the common law looks forward while equilibrium adjustment looks backward. But common law necessarily also looks backward, because

of the need to follow precedent. Because of its foundation in a constitution, constitutional common law always looks back ultimately to the constitution from which its authority arises.

An equally conventional approach to the Fourth Amendment describes it as balancing the rights to privacy and liberty against law enforcement prerogatives. The more robust the safeguards for privacy, the more difficult it is for the police to investigate crime. A traditional balancing approach to the Fourth Amendment would predict, like Kerr, that where police investigative tools become more invasive of privacy, the USSCt should strike a balance that favors privacy; when law enforcement interests are challenged by developments that make criminal activity more difficult to uncover, the USSCt might relax constitutional constraints to preserve law enforcement interests. Thus, it is not clear what Kerr's approach adds to the traditional conception of Fourth Amendment balancing.

Kerr's characterization of the Fourth Amendment as preserving a certain balance between law enforcement and criminals seems oddly out of step with the amendment's underlying purposes. In Kerr's formulation, the Fourth Amendment appears to be a kind of umpire in a game between cops and robbers. But the Fourth Amendment is generally understood to protect the privacy of the citizenry at large against all unreasonable government intrusions. One by-product of doing so is that its rules sometimes frustrate law enforcement, but its purpose is to protect the privacy of all, not to ensure some concept of a "fair fight" between the police and criminals.

While both balancing and common law methodology are accurate descriptions of what the USSCt generally does in constitutional adjudication, at least at a sufficiently high level of generality, they do not provide much guidance as to how the balance should be struck, or the common law adjusted, in particular circumstances. Similarly, equilibrium adjustment may be more useful as a general descriptive account than as a normative guide. Moreover, Kerr's concept of "year zero" is curious. If the USSCt's proper role is to retain a certain equilibrium, should it not be the equilibrium in place at the time the Fourth Amendment was adopted? But if that is all equilibrium adjustment does, it is simply another term for originalism. If "year zero" is not the time of adoption of the Fourth Amendment, but rather some "state of nature" that preceded the development of technology, what basis is there for believing that this strikes the "right" balance between law enforcement and privacy? There is no obvious normative reason to prefer the state of nature. If so, then there is no reason to adjust by reference to year zero.

Finally, how does one assess whether a new development favors the police or the criminal? Most technologies can be used for good or ill. Thus, bank robbers can use cars to speed their getaway, much faster than they could escape by horseback. But police can similarly use cars to increase their ability to respond to a robbery and catch the criminals. The phone enables criminals to coordinate their criminal activities more efficiently, but also enables the police to do the same, as well as to obtain personal information about

who an individual is talking to, how frequently, for how long, and on what subjects. The equilibrium-adjustment theory tells us very little about how to assess how far any particular development has taken us from the equilibrium, much less how to adjust doctrine to offset the shift in the balance of power if we could quantify it.

Ohm finds Kerr's theory attractive, but acknowledges that it is underspecified with respect to assessing the impact of technological developments.²⁶ As he puts it, most technology is "dual-assistance", for it can assist both the police and the outlaw. Ohm proposes that the courts look to empirical facts to assess who has got the better of the deal, by examining such factors as "the length of investigations and number of indictments".²⁷ But this effort to specify and quantify what Kerr left vague only reveals how indeterminate the inquiry is. The length of investigations and the number of indictments will be affected by a wide range of factors and will never be reducible to the effects of a particular technology. Ohm's effort to render Kerr's vague equilibrium more specific only highlights the difficulty of the task.

All four scholars recognize that one of the principal challenges facing the USSCt and the polity in the near term is how constitutional and/or statutory law will adapt to fast-paced developments in surveillance technology. Technological developments threaten to leave privacy, like the eight-track player, behind. Each scholar discussed here has accurately identified the problem, but none offers a fully satisfactory solution. The following section turns to comparative constitutional law to identify three developments, inspired by other legal systems, which might point the way toward reforming Fourth Amendment law in order to preserve privacy.

7.4 Resurrecting privacy in the digital era: lessons from abroad

The conundrum of how to protect privacy in a digital age is, of course, not limited to the US. Many constitutions and human rights treaties protect privacy, or a "respect for private life", and the technological developments described in section 7.1 of this chapter are global in effect. Doctrinal approaches adopted by other legal systems to protect privacy may therefore offer suggestions for how to preserve privacy that might be appropriate for consideration in the US. There are, of course, many difficulties with transplanting legal concepts, rules and doctrines from one system to another. At a minimum, however, other systems' approaches suggest ideas and experiences that may inform the development of privacy protections in the US.

A review of other legal systems suggests at least three steps that might be considered in the US. First, instead of treating privacy as an on/off concept that is forfeited once any amount of sharing of information takes place, or once an individual is in the public sphere, some systems define privacy more expansively as encompassing the details of one's personal life that are not commonly available to the public. This approach allows for protections even

where private information is shared with a third party. Second, some systems require the state to justify particularly intrusive investigative techniques by demonstrating that less intrusive investigatory tactics were insufficient – a sort of “least restrictive means” test. This approach might preserve privacy where less intrusive measures serve the state’s interests. Third, some legal regimes incorporate an independent oversight body tasked to protect privacy. Where, as is often the case in the national security arena, surveillance operates largely behind closed doors, often without even belated notice to the target of a search, such alternative safeguards may be the best that can be afforded. Each of these approaches has the potential to keep privacy protected in the face of the technological onslaught, and each is consistent with basic Fourth Amendment principles.

7.4.1 Refining privacy

At least until *Jones*, the USSCt tended to treat privacy as close to an all-or-nothing concept. It has jealously protected the privacy of the home and, to a somewhat lesser extent, has protected other realms in which people reasonably expect privacy, including workplaces, luggage, clothing, and cars. However, the USSCt has generally treated privacy as forfeited when individuals engage in conduct in public, or share information with others, even where they have little choice but to do so. This leaves the government free in such situations to act without any objective basis for suspicion, without any judicial or other authorization, and free of any constitutional constraint. Even when they were first announced, these doctrines were criticized for being insufficiently attentive to privacy concerns. But whatever one thought then, the effects of these doctrines on privacy are much more severe today, when technology has made it far easier for the government to follow and record our every public move, and to gather, collate, and “mine” data reflecting our every transaction with others. It is one thing to say that one loses one’s expectation of privacy with respect to one’s garbage; it is another entirely to say that one has forfeited it with respect to every transaction recorded by a computer in the modern age.

Justice Alito’s opinion in *Jones* suggests a more nuanced approach, one that retains the USSCt’s focus on “reasonable expectations of privacy”, but treats as private personal information that, absent technological innovations, the government could not realistically obtain without extraordinary effort (such as our precise physical location over an extended period of time). As noted earlier, similar reasoning could undermine the “third-party disclosure” rule; the fact that, in surfing the internet or sending email, we share information with Google should not mean that we thereby share it with the government too. The state, unlike Google, can deprive us of our liberty and is more likely to punish dissent. Thus, sharing information with Google and the government should be seen as qualitatively distinct acts. The way to Fourth Amendment reform is not to abandon the concept of privacy altogether, but

to update it, much as the USSCt did with respect to wiretapping in 1967 and *Alito J* did with respect to GPS surveillance in *Jones*.

Article 8 of the ECHR, which guarantees “respect for private life”, suggests a way forward. The ECtHR has construed this right to be implicated by the government’s storage and use of any information specific to an individual.²⁸ The personal information need not be entirely private, in the sense of not shared with anyone else. In *Malone v United Kingdom*, the ECtHR held that art 8 extended to “pen register” phone data, even though it was legitimately recorded by the Post Office.²⁹ Neither need it involve only information about conduct behind closed doors. The ECtHR instead attempts to protect a realm of “private” or “personal” information. According to the ECtHR, “private life” is “a broad term not susceptible to exhaustive definition”.³⁰ It includes “gender identification, name and sexual orientation and sexual life”, and “a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world”.³¹ Far from being defeated by sharing with others, the right to private life encompasses a “zone of interaction” with others “even in a public context”.³² It is implicated by the recording of “private” or “personal” data, even when those data are gathered in public. Thus, the ECtHR ruled that Closed Circuit Television (CCTV) monitoring and recording of an individual’s attempted suicide on a public street late at night implicated art 8.³³ In short, unlike privacy under the Fourth Amendment, respect for private life is not forfeited simply because information is shared with a bank, credit card company, or internet service provider, or that it concerns conduct carried out in public.

Private information also has Europe-wide statutory protection, guided by the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention on Personal Data Processing).³⁴ The Convention applies to both governmental and private actors, and has influenced the development of national legislation protecting data through much of Europe.³⁵ That legislation sets strict limits on the collection, storage, and use of personal data, whether or not it has been shared with another.

Both art 8 of the ECHR and the Convention on Personal Data Processing have spurred European nations to adopt domestic laws governing surveillance and personal data. For example, the United Kingdom’s (UK) Regulation of Investigatory Powers Act 2000 (RIPA) – enacted to respond to an ECtHR decision finding that the UK’s electronic surveillance system was insufficiently subject to legal limits and safeguards – regulates the covert acquisition of any “private information”, defined as “any information relating to a person’s private or family life”.³⁶ The UK Home Office’s Code of Practice specifies that privacy concerns are likely to arise:

if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (*whether or not available in the public domain*) are covertly (or in some cases

overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing ... In such cases, the totality of the information gleaned may constitute *private information* even if individual records do not (emphasis in original).³⁷

As these decisions and opinions illustrate, a legal system need not treat privacy as an on/off affair, but can – and in my view, should – recognize that private details of an individual’s life can be gleaned by the gathering, recording, collation, and analysis of hundreds of pieces of information about the individual’s purchases, travels, communications, contacts, and viewing and reading habits. As the UK Home Office has acknowledged, the creation of a mosaic – these days often constructed through data-mining – can turn what might be public information when viewed in isolation, into private information when it reveals patterns of an individual’s behavior that would not generally be available to public authorities. In *Jones*, the concurring justices similarly recognized that individual public acts, when collated over a sufficiently long period of time, can reveal private information. The same is true with respect to individual transactions with others, when collated over a sufficiently long time and range to reveal patterns of personal behavior. This is especially so when such patterns for all practical purposes can be generated only through the use of computer data analysis.

It must be acknowledged that an expansion in what counts as a “reasonable expectation of privacy” might lead to some relaxation of the rules governing intrusions into privacy. The USSCt in *Jones* simply held that the use of the GPS monitor triggered the Fourth Amendment, and then remanded the case without deciding what the Fourth Amendment actually required in this setting. The US government argued that, because a GPS monitor reveals only location data, its attachment and use should require only reasonable suspicion, not a warrant based on probable cause. Along similar lines, the USSCt in *Terry v Ohio* ruled that, because brief stops and pat-down searches are a less intrusive form of search than a full-scale search, they are justified on grounds of suspicion falling below probable cause and without a prior warrant.³⁸ The Fourth Amendment prohibits only “unreasonable” searches, and therefore has been interpreted to permit such flexibility. So, too, art 8(2) of the ECHR permits intrusions into the right to respect for private life for a wide range of “legitimate” aims. But until the USSCt recognizes that privacy is even implicated by such tactics as the retrieval and analysis of location and transaction data, the government’s actions need not even be “reasonable”.

7.4.2 Least restrictive means

Computer data-mining has become, by all accounts, a very powerful tool for developing a picture of individuals’ private lives. As noted earlier, both sides in the 2012 US presidential campaign mined such information, gleaned from private companies, to create sophisticated profiles of voters to determine

who they would likely favor in the race, and how they might best be approached and persuaded to vote.

Should police, prosecutors and other government officials be permitted to use such powerful and revealing tools where more limited intrusions might provide them with the information they need for a particular investigation? In some countries, courts consider, in assessing the legality of intrusive surveillance methods, whether the government has exhausted less intrusive alternatives. Such an inquiry might be appropriate under the Fourth Amendment and, indeed, has already been used in limited circumstances.

As noted already, the ECtHR upheld the GPS monitoring of Uzun, notwithstanding its infringement of Uzun's right to respect for private life, in part because the police had first pursued less intrusive measures. The availability of less intrusive alternatives might render a particular infringement on private life not "necessary in a democratic society" as required by art 8(2) of the ECHR.

In view of the particular dangers to privacy posed by wiretapping, Canadian law generally requires the police to show that there is "no other reasonable method of investigation" available before they can obtain a warrant for the interception of telephone communications.³⁹ The Canadian Supreme Court has referred to this "investigative necessity" requirement, albeit in dicta, as "one of the safeguards that made it possible for this Court to uphold [the electronic surveillance scheme] on constitutional grounds."⁴⁰ Investigative necessity does not literally require a showing that wiretapping is the "last resort", but does require more than a claim that it is the "most efficacious" technique available.⁴¹ The state might, for example, show that alternative methods of investigation would be dangerous or ineffective.⁴²

There is room in Fourth Amendment law for such an inquiry. The touchstone of the Fourth Amendment is "reasonableness", and where less intrusive means are readily available, a given search may not be reasonable. Thus, the USSCt has held that seizing an airline passenger's luggage at his arrival city for 90 minutes so that it could be brought to another airport and sniffed by drug-sniffing dogs was unreasonable. Given the advance notice provided to the police, the USSCt reasoned, they could have carried out the search in a less intrusive manner by having a drug-sniffing dog available at the arrival airport.⁴³ Similarly, the USSCt held that, even where the police have a warrant and probable cause justifying a search of a home, it is unreasonable to invite the media to "ride along" on the search, as the search can be conducted without the added intrusion of the media.⁴⁴

A strict "least restrictive means" test would involve too much judicial intrusion on legitimate police discretion. Such an inquiry would require courts – and police – to assess the relative intrusiveness of various methods of surveillance. In some instances, the answer will be self-evident. Detaining a passenger's luggage for 20 minutes is less intrusive than holding it for 90 minutes. Reading the content of emails is more intrusive than obtaining merely the emails' "envelope" address data. But, in other situations, the

assessments will be more subjective: is data-mining or GPS surveillance more intrusive than round-the-clock visual surveillance, for example? Is interception of email or web browsing history more or less intrusive than a search of a car or luggage?

Still, the Canadian and ECtHR approaches suggest that such assessments of the relative intrusiveness of different monitoring tactics may provide an important constraint on the use of new technologies. Incorporating the principle into Fourth Amendment law more generally would encourage police to internalize a “do less harm” approach to investigations. In Canada, the “investigative necessity” requirement was imposed initially by legislation, based on a parliamentary assessment of the particular danger that wiretapping poses to privacy values. Judgments about which types of investigation might trigger such an inquiry might be more amenable to legislative than judicial determination. But as technology makes intrusive investigative tools readily available to police, some such restraint may be necessary if we are to preserve a measure of privacy.

7.4.3 Independent privacy agencies or commissions

A third approach to protecting privacy in the digital age is to create independent institutions whose mission it is to oversee particular investigative tools and practices with the goal of ensuring fidelity to privacy values. The gold standard for doing so is the Fourth Amendment requirement that judges authorize searches based on objective showings of “probable cause” that the investigation will reveal evidence of a crime. Under the Fourth Amendment, a warrant based on probable cause is presumptively required to render a search reasonable – subject to a long list of categorical exceptions. But individualized prior judicial authorization is not always possible, or necessary. Where it is not possible, some sort of *ex post* review may provide an important safeguard. Lawsuits for damages and individual complaints are one form of *ex post* review, but there are multiple obstacles to such avenues for relief. In the US, for example, immunity doctrines for government defendants frequently defeat after-the-fact challenges to unconstitutional searches and seizures. Moreover, many searches, particularly in the national security field, are conducted in secret and without notice to the affected individuals. In such situations, review by an independent commission may be the best that can be done.

Independent privacy agencies or commissioners can also perform a valuable function in the formulation of rules and regulations governing particular investigative techniques. The rules governing investigations are almost always constructed by agencies and officials charged primarily with criminal law enforcement and national security, and are therefore likely to reflect their biases. Where, as is increasingly the case, the technology is complicated, outstrips public awareness and is to some degree secret, public comment and oversight may be radically limited in practice. Creating agencies or commissioners

independent of the national security and law enforcement bureaucracy, with a focus on monitoring new technologies for privacy concerns, may encourage the informed input of privacy values into the initial architecture of such programs.

Such entities are common in Europe, particularly in the realm of data collection.⁴⁵ As Francesca Bignami notes, their authorities and responsibilities vary:

[B]ut most ... have the power to review proposed laws and regulations with a data protection impact, to conduct inspections of private and public data processors, and to commence administrative proceedings against violators which may result in injunctive orders or administrative fines.⁴⁶

Where they detect criminal law violations, they can often bring prosecutions or refer cases to prosecutors.⁴⁷

Canada has also adopted such an approach. Thus, in legislation creating the Communications Security Establishment Canada (CSEC) and empowering it to intercept overseas communications, the Canadian Parliament created the position of a CSEC Commissioner, who must be a former judge, to review the implementation of the legislation and to report annually to Parliament.⁴⁸ An independent commission or commissioner is no panacea, however. The UK, for example, has made ex post oversight by independent commissioners an integral part of its statutory authorization for interception of communications and data. But according to the watchdog group, JUSTICE, the commissioners have been granted insufficient resources and powers, and have been largely ineffective.⁴⁹

That said, the concept of an independent agency or commissioner charged with injecting privacy considerations into the framing of surveillance regulations, and with monitoring their implementation to safeguard against abuse, has promise. The problem with leaving surveillance to the authorities charged with keeping us safe is that they are institutionally likely to discount privacy concerns. Their job is to catch criminals or to keep the nation secure; privacy is likely to be viewed as an obstacle to this. The Fourth Amendment warrant requirement recognizes this problem and responds by requiring the police to convince an independent judge of the objective justifications for their actions before intruding on an individual's privacy or liberty with a search or seizure. The warrant process remains the gold standard for independent protection of privacy. But in those instances where prior judicial authorization is either not possible or too costly, and particularly where ex post lawsuits and complaints are unlikely to be effective, an independent agency tasked with protecting the public good of privacy may provide an important safeguard.

The US has inched in this direction with the appointment of privacy and civil rights officers within the Department of Homeland Security. But they

remain a part of the very agencies they are supposed to be monitoring and therefore lack the requisite independence. Inspectors general are also an example of monitoring, although they tend to focus on issues other than privacy. Where, as is often the case in the national security arena, surveillance is routinely carried out without notice to those subject to it, some sort of independent agency dedicated to the protection of privacy may be a useful mechanism for preserving privacy in the age of sophisticated, all-encompassing, and often secret technological surveillance.

7.5 Conclusion

Technological advances in surveillance have far outstripped the development of constitutional law in the US. The courts and the legislatures may be fated to playing catch up. But if privacy is to be preserved, the law must respond. Outmoded notions that whatever takes place in public cannot be private, or that sharing information with another necessarily forfeits any interest in preserving that information from prying government eyes, need to be rethought. Computers make it increasingly easy to gather massive amounts of “unprotected” information from public arenas and private companies, and to generate intimate portraits of citizens’ desires, contacts, actions, and associations. Privacy law, if it is to retain its relevance in the modern era, must confront this new reality.

Scholars have urged that, as privacy is increasingly squeezed out by technology, Fourth Amendment protection should look elsewhere – to a consideration of the balance of power between police and criminals or to the use rather than the collection of information. But comparative constitutional lessons from other jurisdictions suggest that we need not abandon the notion of privacy. Rather, what is needed is a more expansive definition of privacy. In particular, redefining the invasion of privacy to include the use of technology to compile comprehensive or intimate data about an individual’s private life, whatever the source of the information, would ensure that the Fourth Amendment remains relevant as government surveillance increasingly takes the form of accessing data gathered by private companies. So, too, once we recognize that privacy concerns are implicated by a wider range of activity than heretofore acknowledged, we might consider alternative mechanisms to protect it – such as “least intrusive means” assessments, or the creation of independent bodies charged with protecting privacy through effective oversight and participation in the framing of the rules and regulations governing surveillance.

In the end, rights protections typically grow out of experiences of abuse. The international human rights revolution was sparked by the horrors of World War II; the right of equal protection in the US was defined in response to slavery, the Civil War, and Jim Crow segregation. Reform comes only when the public demands it, and the public demands it only when abuses are disclosed – as happened in the US in the 1970s after a congressional committee headed by Senator Frank Church revealed widespread government

spying on peace groups and civil rights activists. If the right of privacy is to survive the challenge of the all-seeing technological eye, it will be because citizens, enraged by stories of abusive and overly intrusive monitoring of their own activities, insist on it.⁵⁰

Notes

- 1 C Duhigg, "Campaigns mine personal lives to get out vote", *New York Times* (New York), 13 October 2012, A1.
- 2 S Sengupta, "Courts divided over searches of cellphones", *New York Times* (New York), 26 November 2012, A1.
- 3 E Lichtblau, "Wireless firms are flooded by requests to aid surveillance", *New York Times* (New York), 8 July 2012.
- 4 E Metcalfe, JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (London: JUSTICE, 2011) 74.
- 5 565 US __ (2012).
- 6 ECtHR, Fifth Chamber, Application No 35623/05, 2 September 2010.
- 7 Opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953).
- 8 E A Shils, *The Torment of Secrecy: The Background and Consequences of American Security Policies* (Glencoe: Free Press, 1956) 21–5.
- 9 T E May, *Constitutional History of England 1760–1860* (London: Longman, 1863) vol 2, 287–8.
- 10 S Chesterman, *One Nation under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty* (New York: Oxford University Press, 2011) 1–13.
- 11 D J Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven: Yale University Press, 2011) 1–18.
- 12 O Kerr, "An equilibrium adjustment theory of the Fourth Amendment" (2011) 125 *Harvard Law Review* 476, 479–90.
- 13 P Ohm, "The Fourth Amendment in a world without privacy" (2012) 81 *Mississippi Law Journal* 1309, 341–47.
- 14 *United States v Knotts*, 460 US 276 (1983).
- 15 Transcript of Proceedings, *United States v Jones* (USSCt, No 10-1259, 8 November 2011) 41 http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf (accessed May 2013).
- 16 D Priest and W M Arkin, "A hidden world, growing beyond control", *Washington Post* (Washington, DC), 19 July 2010.
- 17 Pub L No 107-56, 115 Stat 272 (2001), § 218, amending 50 USC §§ 1804(a)(7)(B) and 1823(a)(7)(B). See also Chapter 13 by Owen Fiss in this volume.
- 18 *Ibid*, PATRIOT Act § 505.
- 19 Letter from American Civil Liberties Union (ACLU) to US Attorney-General, Eric Holder, 20 October 2011 http://www.aclu.org/files/assets/aclu_letter_to_ag_re_rm_102011_0.pdf (accessed May 2013).
- 20 In Chapter 5 in this volume, Fiona de Londras similarly criticizes privatization and its interrelation with secrecy, but one is left wondering whether the real problem is not secrecy rather than privatization as such. We do not object to private contractors disposing of garbage or cleaning the streets if that is a more efficient and effective way to get the job done. There may well be legitimate concerns about privatization of some core government services, but too often the dangers are assumed without a careful explication of what they are.
- 21 Solove, above n 11, 118–19.
- 22 Kerr, above n 12, 482–90.

- 23 *Carroll v United States*, 267 US 132 (1925).
- 24 *Katz v United States*, 389 US 347 (1967).
- 25 D A Strauss, *The Living Constitution* (New York: Oxford University Press, 2010) 1–6, 33–50.
- 26 Ohm, above n 13, 1313–18.
- 27 Ohm, *ibid* 1313.
- 28 *Leander v Sweden* (Application No 9248/81) (1987) 9 EHRR 433, [48]; *Malone v United Kingdom* (Application No 8691/79) (1985) 7 EHRR 14, [84]; *European Parliament v Council of the European Union and Commission of the European Communities* (C-317/04, C-318/04) [2006] ECR I-4721, [207]–[233].
- 29 (Application No 8691/79) (1985) 7 EHRR 14, [83]–[88].
- 30 *Pretty v United Kingdom* (ECtHR, Application No 2346/02, 29 July 2002) [61].
- 31 *Ibid*.
- 32 *P G and J H v United Kingdom* (ECtHR, Third Section, Application No 44787/98, 25 September 2001) [56].
- 33 The ECtHR drew a distinction between mere monitoring and the recording of the monitored activity: “The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual’s private life ... On the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations”.: *Peck v United Kingdom* (Application No 44647/98) (2003) 36 EHRR 41, [59].
- 34 Signed 28 January 1981, CETS 108 (entered into force 1 October 1985) art 8; C J Bennett and C D Raab, *The Governance of Privacy and Policy Instruments in Global Perspective* (Cambridge, MA: MIT Press, 2nd ed, 2006) 84–7.
- 35 F Bignami, “European versus American liberty: a comparative privacy analysis of antiterrorism data mining” (2007) 48 *Boston College Law Review* 609, 643.
- 36 RIPA s 26(10).
- 37 Home Office (UK), *Covert Surveillance and Property Interference Revised Code of Practice* (2010) <http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-covert> (accessed May 2013) [2.6].
- 38 392 US 1 (1968).
- 39 S Penney, “National security surveillance in an age of terror: statutory powers and Charter limits” (2010) 48 *Osgoode Hall Law Journal* 247, 250, 255–6.
- 40 *R v Araujo* [2000] 2 SCR 992 [26] (*Araujo*); see also *R v S A B* [2003] 2 SCR 678 [53] referring to investigative necessity showing as a “constitutional requirement” for wiretap authorizations.
- 41 *Araujo*, *ibid* [29], [39].
- 42 *Araujo*, *ibid* [41]–[43].
- 43 *United States v Place*, 462 US 696 (1983).
- 44 *Wilson v Layne*, 526 US 603 (1999).
- 45 Bignami, above n 35, 647; Bennett and Raab, above n 34, 133–7.
- 46 Bignami, *ibid* 648.
- 47 Bignami, *ibid*.
- 48 Penney, above n 39, 282.
- 49 Metcalfe, above n 4, 59–64, 96–8, 109–11, describing UK oversight mechanisms and their shortcomings. See also Chapter 3 by Clive Walker for a critique of the role of the UK commissioners.
- 50 See Chapter 16 by Conor Gearty and Chapter 18 by Vanessa MacDonnell in this volume.