PERVASIVE SURVEILLANCE AND THE FUTURE OF THE FOURTH AMENDMENT

Russell D. Covey

Fourth Amendment law is at a crossroads. It traditionally has sought to balance two critical objectives: the protection of individual privacy, and the need to permit the state the necessary means to solve crimes, keep order, and safeguard the national security. Increasingly, however, it seems to do neither. In recent decades courts have construed privacy under the Fourth Amendment so narrowly and formalistically that real privacy protection seems deeply threatened. At the same time, courts have struggled to adapt traditional doctrines in light of new terrorism threats. Technological change, moreover, which already is poorly accommodated in the case law, threatens to accentuate these trends in two respects. First, rapid advances in technology continue to increase the technological power available to individuals while decreasing its costs. For example, Moore’s law has, at least to date, accurately predicted that the number of transistors that can be crammed onto a computer chip will double approximately every eighteen to twenty-four months.¹ The so-called “Carlson Curve” forecasts that the cost of synthesizing DNA falls at a similar geometric rate, a prediction that to date has also proved accurate.² Similar phenomena have been observed in other areas of technology, while the growth of the internet has sparked a diffusion of information

² See, e.g., Robert Carlson, The Changing Economics of DNA Synthesis, 27 NATURE BIOTECHNOLOGY 1091 (2009) (observing that over the past 20 years “the number of bases a single individual can synthesize in a day using commercial instruments has increased by five orders of magnitude, whereas the per base cost of synthetic genes has dropped by nearly three orders of magnitude”).
and technology across the globe. These developments tend to amplify each other, as increasing computer power fuels technological advances across the board, while the internet and other communications technologies efficiently distribute the new knowledge to individuals seeking it anywhere in the world.

The steep rise of the technology curve has radically increased the ability of ill-meaning persons to obtain highly destructive weapons. The complete genetic sequence for the small-pox virus, for example, is available on the internet, and the biotechnology necessary to synthesize it can be mastered by persons with a high-school education and the equipment purchased on eBay for approximately $10,000 or less. Detailed plans for building an atomic bomb are similarly available. Cyber-attacks on commercial and government computer systems are prevalent and growing, and permit individual hackers as well as foreign states and terrorist groups new ways to sow disruption. These technological changes place enormous pressure on governments to take increasingly intrusive measures in the name of safeguarding public security from terrorist threats. Advancing technology plainly enhances the destructive capabilities of individuals and small groups who are bent on engaging in terrorism, while the increasing complexity and interdependence of critical system infrastructure magnifies the scale of potential destruction that might result from such acts.

---


5 See Deborah N. Pearlstein, *Form and Function in the National Security Constitution*, 41 Conn. L. Rev. 1549, 1593 (2009) (noting that “[t]he nuclear physics required to understand how to build a crude nuclear bomb has been in the public sphere for decades”).

Governments possess only a handful of strategies, generally falling into three “buckets,” to prevent the misuse of potentially destructive technologies. In the first bucket are strategies aimed at preventing malicious persons from acquiring destructive technologies through various methods of interdiction. In the second are strategies aimed at minimizing the damage that can be accomplished through the use of destructive technologies by hardening potential targets. In the third are strategies focused on monitoring the uses to which technology is put through a variety of surveillance programs. Although all three strategies—interdiction, target-hardening, and surveillance—undoubtedly need to be and no doubt will be pursued, interdiction’s historic inefficacy in policing the drug and arms trades suggests that by itself it will likely prove an ineffective deterrent to future catastrophic threats. Not only is interdiction of technology itself dauntingly difficult, it risks driving marginal activities underground, where monitoring is even more difficult, and thereby inducing creation of specialized black markets for the targeted technologies.\(^7\)

Target-hardening strategies include “making borders, buildings, airplanes, and critical infrastructures more difficult to breach, disrupt, or destroy” and vaccinating people to make them more resistant to deadly diseases.\(^8\) Although target-hardening is imperative where possible, certain threats, including those posed by nuclear terrorism and bio-terrorism, cannot be sufficiently mitigated through target-hardening strategies. Nothing we can do will prevent a massive loss of life and material wealth in the event that terrorists succeed in detonating

---

\(^7\) As Carlson argues with respect to proposed government controls on technologies used to synthesize DNA:

[O]ne potential outcome of restricting access to synthesis might mirror the problem encountered by the US Drug Enforcement Agency when it cracked down on domestic methamphetamine production: information on activities the agency wished to monitor and suppress became much harder to obtain, whereas methamphetamine use continued to rise.

Carlson, \textit{supra} note 2, at 1093.

\(^8\) \textsc{Comm. on Sci. \\& Tech. for Countering Terrorism, Nat’l Research Council, Making the Nation Safer: The Role of Science and Technology in Countering Terrorism} 28 (2002).
a nuclear weapon in a major urban area or in releasing certain deadly biological agents on a large scale. Because of the inherent shortcomings of interdiction and target-hardening, surveillance will necessarily play a major, and increasing, role in safeguarding national security.

The government’s growing need to heighten its surveillance activities is complemented by the second major consequence of technological change—the rapidly expanding power of the government to acquire and process information about persons, both home and abroad. New and increasingly powerful technologies permit the government to obtain types and quantities of information about citizens to an extent previously unimaginable. Ubiquitous closed-circuit television monitors, cell-phone tracking methods, GPS devices, and electronic tolling systems permit remote, around-the-clock monitoring of an individual’s location and movements. “Deep-packet” electronic surveillance methods permit digital eavesdropping of telephone and electronic communications. Cyber-surveillance techniques permit access to a huge, and ever-growing, amount of information about the activities and interests of individuals, including phone and email contacts, internet searches, websites visited, purchase records, travel plans, health records, and more. New technologies make through-the-wall surveillance devices readily imaginable, and through-the-clothing surveillance devices are already a fixture in many airports. Forensic biometric techniques, including DNA identification, already have revolutionized the government’s ability to locate and identify human traces and promise to become ever more powerful in

---

9 Vaccination programs could minimize the harms from release of some viruses or bacteria, such as smallpox, but would likely be ineffective against a wide variety of genetically-altered “supergerms.”

10 See Kim Zetter, Deep-Packet Inspection in U.S. Scrutinized Following Iran Surveillance, WIRED, June 29, 2009 (reporting concerns that Iran is using deep-packet inspection technology to “snoop on the content of e-mail, VoIP calls and other online communication” and that same technology is being installed in the United States).

11 See Kyllo v. United States, 533 U.S. 27, 36 n.3 (2001) (discussing various “through the wall” surveillance devices under development by the Department of Justice).
the future. This is but a partial list of the new technologies that are already reshaping the way that government obtains information about individuals.

Even more revolutionary technologies, such as nanotechnology and bio-engineering, promise to further radically expand the capabilities of government surveillance and information acquisition. Experts forecast that nanotechnology will soon permit the development of detection and sensing devices that can “precisely identify, and perhaps isolate single molecules, viruses, or other complex, nanoscale structures.” One writer predicts “a world covered by imaging radar, multispectrum nanotech sensors, chemical sampling and a host of other data sources.” In that world, “tiny sensors will be designed to detect the minutest traces of chemical or biological agents or...

12 The remarkable investigative capabilities provided by these new technologies were displayed in the investigation of the recent attempted S.U.V. bombing of Times Square. Within hours of the incident, law-enforcement agents gathered hundreds of still and video images of the vehicle and suspicious activity of individuals in the vicinity at the time of the attempted bombing. Electronic toll records and images of vehicle license plates were searched in order to identify the manner by which the vehicle entered the city. Experts speculated that DNA traces would be recovered from a search of the car’s interior. As a result of the investigation, a suspect was arrested while attempting to board a flight to Dubai and taken into custody within forty-eight hours of the failed attempt. See Michael M. Grynbaum, William K. Rashbaum, & Al Baker, Police Seek Man Taped Near Times Sq. Bomb Scene, N.Y. TIMES, May 2, 2010, at A1, available at http://www.nytimes.com/2010/05/03/nyregion/03timessquare.html?scp=1&sq=times%20square%20bombing&st=cse (reporting that “license plate readers and cameras at the area’s tollbooths were being checked to determine where the car had entered Manhattan”).

13 These new technologies also promise to increase, perhaps dramatically, the destructive capabilities of ill-meaning individuals and groups. As Bill Joy, the founder of Sun Microsystems, wrote in a much-discussed article regarding twenty first century technologies such as genetics, nanotechnology, and robotics: “I think it is no exaggeration to say we are on the cusp of the further perfection of extreme evil, an evil whose possibility spreads well beyond that which weapons of mass destruction bequeathed to the nation-states, on to a surprising and terrible empowerment of extreme individuals.” Bill Joy, Why the Future Doesn’t Need Us, WIRED, Aug. 2004, http://www.wired.com/wired/archive/8.04/joy_pr.html.


explodet to eavesdrop and transmit conversations.”

These technological developments will inevitably change the landscape of Fourth Amendment law. This Article suggests how that change might occur. Part I describes the Fourth Amendment’s current inability to prevent government agents from using technology to obtain information that most people would consider deeply private. It then shows how even Supreme Court decisions celebrated as enhancing privacy protection against high-tech surveillance actually provide little substantive protection, but more worrisome, also seem to erect substantial limits on the types of surveillance the government will almost certainly need to engage in to battle growing terrorism threats fueled by new technology. Part II argues that what is needed is a fundamental rethinking of the purposes animating Fourth Amendment law, and a shift in focus from privacy protection understood as permitting citizens to keep some stock of information secret from governmental inquiry to privacy protection as regulation of the use of information about citizens in ways that permit citizens to lead lives secure in the knowledge that the information will not be misused or disclosed to persons who are not entitled to it. It then suggests two ways to update Fourth Amendment jurisprudence. First, it advocates abandonment of the so-called third-party doctrine and expansion of the definition of what constitutes a search for Fourth Amendment purposes. Second, it argues for recognition of an antiterrorism exception that would exempt anti-terrorism surveillance from the probable cause and warrant requirements, coupled with far more stringent regulation of the use of information obtained in the course of an antiterrorism, or of any special needs, search.

I. THE FOURTH AMENDMENT’S FAILURE TO PROTECT SUBSTANTIVE PRIVACY

Fourth Amendment law, as it has developed over the course of the twentieth-century, has proved singularly inept at

16 Id.
dealing with the technological revolution. Perhaps since the Supreme Court’s first landmark Fourth Amendment decision *Boyd v. United States*,\(^{17}\) and certainly since *Katz v. United States*,\(^{18}\) the Fourth Amendment has purported to regulate and control the non-consensual governmental acquisition of information from individuals in the name of privacy protection. Arguably, in attempting to regulate governmental acquisition of information, Fourth Amendment law has focused on the wrong problem\(^{19}\) and has failed to solve that problem to boot. Notwithstanding this supposed aim, as numerous commentators have explained, Fourth Amendment law does a terrible job of protecting privacy in ways that make a difference in the modern world.\(^{20}\) Weak privacy protection can largely be traced to the so-called “third party doctrine,” which permits the government to obtain an enormous amount of information about individuals under the rationale that information voluntarily disclosed to a third-party is no longer reasonably held “private.”\(^{21}\) As a result, the government can deploy an undercover agent wearing a wire and tape recorder into an individual’s home,\(^{22}\) obtain cancelled checks, deposit slips, and other financial data from his bank,\(^{23}\) subpoena telephone records,\(^{24}\) surreptitiously track his movements throughout the day using an electronic

---

\(^{17}\) 116 U.S. 616 (1886).

\(^{18}\) 389 U.S. 347 (1967).

\(^{19}\) For one commentator making this argument, see Scott Sundby, “Everyman”’s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?, 94 COLUM. L. REV. 1751, 1758 (1994) (“Formulating Fourth Amendment interests in privacy terms has undermined the Amendment’s protections.”).

\(^{20}\) The classic article criticizing the third-party doctrine for its disregard of privacy between persons is Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593 (1987); see also Thomas P. Crocker, From Privacy to Liberty: The Fourth Amendment After Lawrence, 57 UCLA L. REV. 1, 3 (2009) (arguing that third-party doctrine undermines privacy and liberty).

\(^{21}\) See Stephen E. Henderson, Beyond The (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too, 34 PEPP. L. REV. 975, 976 (2007) (defining third-party doctrine as “meaning that so far as a disclosing party is concerned, information in the hands of a third party receives no Fourth Amendment protection”).


\(^{24}\) E.g., Smith v. Maryland, 442 U.S. 735 (1979).
tracking device,\textsuperscript{25} rifle through his trash,\textsuperscript{26} and fly a helicopter over his property\textsuperscript{27} without any need to comply with the Fourth Amendment’s traditional probable cause and warrant requirements. It is hardly an overstatement to say that, by removing from privacy protection any information revealed to others, the Fourth Amendment’s function as guarantor of individual privacy has been crippled. In an increasingly networked and technology-dependent world, the amount of information that has not been deposited with, or at least casually exposed to, some other commercial, governmental, or corporate entity is miniscule and shrinking.\textsuperscript{28}

This is not to say that Fourth Amendment law sets up no barriers to police investigation. The cases do establish a small zone of privacy in a limited number of physical spaces—chiefly, the home, but also to a lesser extent, physical containers such as coat-pockets, bags, luggage, and footlockers, and to a still lesser extent, automobiles. Of these, protection of the physical integrity of the home has received special Fourth Amendment deference. That deference has been extended in two important cases to technological surveillance. In \textit{United States v. Karo}, the Supreme Court held that while monitoring of an electronic beeper in public was permissible, monitoring an electronic beeper inside a home (or other constitutionally-protected place) was not.\textsuperscript{29} In \textit{Kyllo v. United States},\textsuperscript{30} the Court held that government use of a thermal-imaging device to measure heat radiation emitted from private residences was the functional equivalent of physical entry and therefore unlawful without a warrant.\textsuperscript{31}

\begin{itemize}
  \item \textsuperscript{25} \textit{E.g.}, United States v. Knotts, 460 U.S. 276 (1983) (obtaining information from an electronic beeper).
  \item \textsuperscript{26} \textit{E.g.}, California v. Greenwood, 486 U.S. 35 (1988).
  \item \textsuperscript{27} \textit{E.g.}, Florida v. Riley, 488 U.S. 445 (1989) (permitting warrant based on surveillance obtained by aerial overflight).
  \item \textsuperscript{28} See Susan W. Brenner, \textit{The Fourth Amendment in an Era of Ubiquitous Technology}, 75 Miss. L.J. 1, 68 (2005).
  \item \textsuperscript{29} 468 U.S. 705 (1984).
  \item \textsuperscript{30} 533 U.S. 27 (2001).
  \item \textsuperscript{31} Id. at 40. Similar limits on government’s ability to search or seize have been recognized outside the home as well. In \textit{Florida v. J.L.}, the Supreme Court significantly limited the ability of police officers to investigate uncorroborated anonymous tips, even
\end{itemize}
Although these cases do impose some restraints on police surveillance, at least on the actual facts of the cases, the limitations on police information-gathering tactics do not appear well-designed to protect privacy in any but the most formal and abstract sense. After all, police monitoring of a beeper inside a can of ether that has been carried into a person’s house reveals to the police only the fact that the beeper, and hence the can of ether, is inside the house. It tells the police nothing about the house itself, nor reveals any private information that the homeowner might seek to conceal (other than the fact that the item containing the beeper is inside the house). Of course, the valence of that narrow fact turns to an extent on the nature of the item. Possession of some items—drug paraphernalia or child pornography, for instance—might itself be compromising. Be this as it may, it was the view of the majority in Karo that monitoring the beeper after it had emerged from a constitutionally-protected location was permissible, even if absent the beeper police would have had no way to know that the surveilled item had been moved.\textsuperscript{32} Any deterrent impact of the rule precluding the monitoring of a beeper inside a house is thus attenuated by the lawfulness of monitoring the movement of that item up to the threshold of the house, and then again after it leaves the house and begins its journey to the next destination. Under such a rule structure, police have been given a green light to use tracking technology, knowing that the most of the information obtained thereby will ultimately be admissible. As a result, Karo offers individuals little meaningful privacy protection.

Similarly, despite all the talk of revealing the secrets of the lady of the house and her daily sauna and bath in Kyllo,\textsuperscript{33} when investigation of the tip posed relatively minor intrusion on the suspect, where there were few practical alternatives available to the police, and where the threat reported—a teenager unlawfully in possession of a gun—was not insignificant. 529 U.S. 266, 274 (2000).

\textsuperscript{32} Karo, 468 U.S. at 721 (holding that unlawful monitoring of beeper while it was located in private residence did not taint subsequent monitoring of beeper when item was moved out of residence, even though the movement of the item was otherwise undetected).

\textsuperscript{33} Kyllo, 533 U.S. at 38; id. at 44, 50 (Stevens, J., dissenting).
the tactic employed by the police in pointing a thermal-imaging device at Kyllo’s residence implicated privacy to, in the words of Justice Stevens, at most a “trivial” degree.\textsuperscript{34} What privacy interest could an individual have in the relative distribution of heat being emitted from her home? Compare that with the trash searches at issue in Greenwood, which were held not to implicate Fourth Amendment concerns. Unlike a thermal imager scan, a trash search can reveal an enormous amount of truly private information, including love letters, political correspondence, financial records, medicines, and evidence of sexual practices. Contrasting Karo and Kyllo with third-party doctrine cases like Greenwood, it is clear that the Court has privileged a formalistic understanding of privacy as “information about the home” over a substantive understanding of privacy as information that an individual reasonably would prefer not to disclose to strangers. Of course, in both Karo and Kyllo, the Court was quite clearly less concerned with redressing any actual privacy intrusion that occurred in the cases before them than it was with anticipating the use or development of new technologies that might reveal more intimate facts. While a beeper reveals no more than its present location, an electronic listening device or small camera might well reveal all sorts of information about the home and its occupant’s activities which the homeowner reasonably expects to keep private. The Kyllo Court was quite explicit about this, expressly crafting a rule not merely for the case before it but in anticipation of potentially more intrusive technologies.\textsuperscript{35} But given the types of technology actually used, it is hard to see how either Karo or Kyllo provides much real privacy protection.\textsuperscript{36}

\textsuperscript{34} Id. at 45 (Stevens, J., dissenting).

\textsuperscript{35} See id. at 35-36 (majority opinion) (explaining that an alternative rule “would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home” and that “the rule we adopt must take account of more sophisticated systems that are already in use or in development”).

\textsuperscript{36} The same might be said of another recent pro-privacy protection Fourth Amendment decision, Bond, which held unlawful government agents’ warrantless and suspicionless prodding of luggage in the overhead storage bin of a bus. Like Kyllo and Karo, the information disclosed by the unlawful search in Bond seems rather innocuous (whatever can be felt by prodding and squeezing a closed piece of luggage) and the
These decisions, however, are almost as perverse in their potential effects on limiting legitimate government surveillance tactics as the third-party doctrine has been in eradicating personal privacy. Not only do the Fourth Amendment barriers erected in these cases provide relatively little substantive privacy protection to individuals, but they seem impractical, if not positively dangerous, in light of potential terrorist threats in a future promising ever-cheaper and more powerful technologies deployable for destructive purposes. Consider two potentially valuable anti-terrorism tactics that these cases seem to foreclose: the use of electronic tags and microscopic sensors that might be embedded into physical objects, and the use of imaging and scanning devices that might be used remotely or directly by government agents to detect various phenomena.

There are a huge variety of new electronic tagging systems and devices coming online. As noted above, some of these devices are being engineered at the nanoscale, and promise to permit very selective search, identification, and tracking tactics. In addition, Radio Frequency Identification (“RFID”) technology is already widely used to monitor the movement of goods in a variety of ways, and has even been used to implant identification information in the human body. It is easily conceivable that efforts to control the diffusion of powerful bioengineering technologies that have widespread legitimate commercial and scientific uses as well as the potential to manufacture biological weapons of mass destruction might incorporate RFID or other tracking technologies that monitor the location and use of biotech equipment. Karo’s rule that monitoring the location of such equipment is unlawful when it intrudes into constitutionally-protected spaces, including homes or private businesses, seems to call such precautionary surveillance into question.

holding driven less by an actual concern with protecting privacy and more with a general distaste for a particular police information-gathering tactic.

Kyllo’s holding, well-meaning as it is, seems even more obviously problematic in the age of terrorism. Devices designed to sense the presence of nuclear, chemical, or biological materials, including both nanotech sensors and scanning devices that might be used to detect the signature traces of chemical, biological, or nuclear materials would be tremendously helpful in preventing the deployment of Weapons of Mass Destruction (“WMD”) in major urban areas. 38 Kyllo’s rule, however, on its face seems to preclude their use, at least as long as those technologies are not “in general use.” 39

The gravity of the threat posed by WMD, made or hidden in private residences, suggests that a Fourth Amendment jurisprudence that constructs a relatively impermeable wall around the home or any other “constitutionally-protected area” is imprudent and potentially disastrous. Although a long line of Supreme Court cases have reiterated the principle that the home must remain impervious to unregulated governmental intrusion, 40 the proliferation of destructive technologies and the increasing ease of manufacturing them will continually increase the hazards of placing off-limits any physical locations to preventative surveillance efforts by the state. 41

In short, Fourth Amendment law has utterly failed to develop sensible rules in response to changing technology. By fo-

38 This point was made by Justice Stevens in his dissent in Kyllo. See 533 U.S. at 48 (Stevens, J., dissenting) (arguing that the Court’s holding renders unconstitutional “the use of other new devices that might detect the odor of deadly bacteria or chemicals for making a new type of high explosive”).

39 Kyllo, 533 U.S. at 34 (majority opinion) (holding that “obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical ‘intrusion into a constitutionally-protected area’ constitutes a search”) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

40 See, e.g., id. at 31 (asserting that “[a]t the very core of the Fourth Amendment ‘stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion’”) (quoting Silverman, 365 U.S. at 511).

41 Imagine a nuclear device capable of obliterating a major city that could fit in a shoebox and be constructed, based on plans downloaded from the internet, using materials available at the neighborhood hardware store. How might the government respond to such a threat? How might those responses fit within our rules of constitutional criminal procedure intended to secure individuals from unreasonable government searches?
cusing on the protection of “privacy” defined as keeping information about activities occurring within a small set of specially-protected areas secret from government observation, the Fourth Amendment has wandered down the wrong path. Because most intimate activities involve limited disclosures of information to others, Fourth Amendment law already fails to protect privacy in a sense meaningful to most persons, even while it continues to bar the state from engaging in some activities that might measurably advance anti-terrorism efforts. Meanwhile, future technological developments will increase the threat of major acts of terrorism, the number of persons or groups who will have the means to engage in such terrorism will multiply, and the government’s capability to engage in surveillance and its interest in deploying highly intrusive surveillance systems will grow ever stronger.

II. SHIFTING CONSTITUTIONAL SCRUTINY FROM INFORMATION ACQUISITION TO INFORMATION UTILIZATION

Contrary to the dire warnings of some privacy activists, the increasing reliance upon surveillance technologies is neither surprising nor especially alarming. Rather, as Jack Balkin observes, “[g]overnment’s increasing use of surveillance and data mining is a predictable result of accelerating developments in information technology.”42 Thus, unlike many scholars who critique the law’s failure to restrain the proliferation of surveillance,43 I accept the surveillance state as an apparently inevitable concomitant of a technologically-advanced society. We cannot, and increasingly will not, live in an un-surveilled world because the risks of averting our gaze are, or likely will become, too great.

Because of the ever-increasing threat to public safety posed by evolving technology, both law and society must learn to accommodate a regime of pervasive surveillance. That is,

government must be permitted to obtain the information it needs to keep its citizens and infrastructure secure. Individual privacy cannot continue to be conceptualized as the right or expectation to maintain one or more physical locations that are immune from all forms of surveillance because any absolute location-based prohibitions on the government’s ability to surveill will inevitably be exploited by those seeking to inflict harm. Transitioning to a constitutional surveillance state, however, will require careful rethinking about the basic purposes of Fourth Amendment law.

If I am right that pervasive surveillance will become the norm, then the problem for constitutional criminal procedure must necessarily shift from the regulation of the state’s acquisition of information to the regulation of the state’s use and dissemination of that information. Such an argument might seem radical because the Fourth Amendment bars unreasonable searches and seizures—which are methods of bringing information, property, and people into governmental custody or control—but says nothing on its face about the governmental use of information, however obtained, that is already in its possession. But the argument is less radical, I would argue, than it might at first glance seem. The exclusionary rule, long an accepted, if contested, element of Fourth Amendment doctrine, designedly addresses the legitimate and illegitimate uses of evidence and information in the state’s possession.44 Similarly, the Court has considered the use of evidence as one factor in evaluating the reasonableness of a search. For example, the exemption from full Fourth Amendment scrutiny of searches and seizures that are not primarily directed at enforcing the criminal law is logically grounded in the view that use of information matters.45 That proposition is undercut to some extent by the plain view doctrine that permits information that

44 Of course, what makes the exclusionary remedy so controversial is that while it regulates the government use of some information, it prohibits seemingly legitimate uses of that information—to prosecute criminals—at a significant cost to the public interest.

45 See, e.g., Indianapolis v. Edmond, 531 U.S. 32, 42 (2000) (finding that checkpoint program designed to interdict drugs was unlawful because its “primary purpose” was “to uncover evidence of ordinary criminal wrongdoing”).
otherwise wouldn’t have been available to the government to be used for criminal prosecution as long as it was otherwise lawfully obtained. Still, the fact that the state’s purpose in acquiring information often determines the lawfulness of the acquisition suggests that use, as well as acquisition method, is a subject of constitutional import.

In short, any easing of constitutional restrictions on government’s ability to acquire the information necessary to combat terrorism will necessitate new safeguards to ensure that government neither misuses that information in ways that cause real privacy harms to individuals nor abuses its enormous surveillance powers for pretextual ends. The concern with preventing governmental misuse of information will require strict regulation of the uses to which anti-terrorist surveillance data can be put.

A. Regulating Use of Surveillance Data

One of the fundamental flaws of the Court’s focus on information acquisition is that it exaggerates the importance of the search/non-search dichotomy. An investigatory tactic deemed not to constitute a search is subject to no constitutional regulation at all, while a tactic that is deemed a search is subject to close constitutional scrutiny. Undoubtedly, the third-party doctrine was fashioned in part to permit the state to engage in certain types of investigatory activities, such as using undercover informants, that if burdened by the traditional probable cause and warrant requirements, might be foreclosed altogether. But a shift from regulation of information acquisition to regulation of its use would permit a de-emphasis of the search/non-search dichotomy. In a regime focusing on regulation of use, government practices that currently receive no Fourth Amendment scrutiny as a result of the third-party doc-

46 See Arizona v. Hicks, 480 U.S. 321, 326 (1987) (evidence seized during warrantless search of apartment admissible as long as it is obtained by officer during lawful intrusion and there is probable cause to seize it).

47 See, e.g., Hoffa v. United States, 385 U.S. 293, 303 (1966) (holding that government need not obtain warrant prior to using undercover informant to obtain information from suspect unaware of the informant’s identity).
trine, such as the deployment of electronic tracking devices to trace an individual's public movements, garbage searches, and obtaining individual internet usage data records, might be recognized as searches for Fourth Amendment purposes. In other words, the scope of the warrant requirement should expand to include far more borderline search conduct than it currently does. Such an expansion can be effectively accomplished simply by acknowledging the mundane truth that people routinely, and reasonably, make limited disclosures of private information to others who are entrusted with the information for specific purposes and expected not to use their access to the information to make inferences about the individual disclosing it. People place their trash on the sidewalk expecting that the garbageman, but not newspaper reporters or police officers, will have access to it during the short interval before their trash commingles with others'. People release financial information to banks, medical information to hospitals and insurance companies, and information about personal and sexual matters to therapists, reasonably expecting that such information will not be turned over to third parties. Simple recognition of the concept of limited disclosure should make it possible to distinguish between a truly private item that has been disclosed to one or more others, and information that has been "knowingly exposed to the public"—as for example, a blog post on a popular website might be. Where government conduct intrudes upon such expectations, that conduct should be subject to judicial oversight through the traditional warrant requirement.

48 The District of Columbia Circuit Court of Appeals recently reached precisely this conclusion in an important case involving the warrantless use of a GPS monitoring device to surveil the movements of a suspect for a month. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010). According to the Court: "A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain "disconnected and anonymous."" Id. at 563, 568 (holding that extended monitoring with GPS device requires warrant) (quoting Nader v. Gen. Motors Corp., 25 N.Y.2d 560, 572 (1970) (Breital, J., concurring)).
But whether the warrant should issue, and for what uses the information obtained thereby should be permitted, should not simply be a matter of probable cause. Indeed, individualized probable cause itself need not always be the focus of the warrant inquiry. In a regime prioritizing the regulation of the use of information, the reasonableness of any search depends not only on the presence or absence of probable cause that the search will turn up evidence of a crime, but also on the degree to which the information sought by the state is of an intimate nature, as well as on the state’s intended use of the information. Before issuing a warrant, magistrates might be asked to balance factors such as the degree of privacy intrusion implicated by the search, the gravity of the crime suspected, and whether the state has a justifiable basis to suspect the individual targeted by the search. Highly intrusive searches should require stronger justifications than minimally intrusive searches. At the same time, where grave crimes are suspected, a lower threshold—perhaps reasonable suspicion—should suffice to justify the search. Where less serious crimes are suspected, a correspondingly stronger showing—probable cause or in some cases, perhaps something even higher—might be demanded before a warrant should issue. Just as importantly, judicial oversight should not be restricted to the acquisition of information. As will be discussed in the next section, the government’s use of information obtained in a search should be limited by the needs that justified the intrusion at the start. Such regulation of the use of private data is essential to safeguarding individual privacy.

Balancing these factors may be difficult, but the process would be smoothed once a search-specific methodology was developed, and distinctions made—and regularized—among the variety of search methods, such as garbage searches and the use of tracking devices, that currently receive no judicial oversight. The net result might be a Fourth Amendment that provides greater privacy protection to individuals against govern-

49 Cf. Arizona v. Gant, 129 S. Ct. 1710, 1723 (2009) (permitting vehicular searches incident to arrest where driver is outside vehicle at time of search when it is “reasonable to believe the vehicle contains evidence of the offense of arrest”).
ment search techniques that currently are completely unregulated, without preventing the state from investigating serious allegations of criminal activity.

B. Regulation of Suspicionless Searches

If an expanded warrant requirement is necessary to ensure judicial oversight over governmental use of data-gathering technologies that the state focuses upon individual suspects, the threat posed by the diffusion of technology increases the urgency of instituting new forms of anti-terrorism surveillance in the absence of particularized suspicion. Such searches might include the widespread use of scanning devices and sensors, the use of artificial intelligence technology to monitor telephonic and electronic communications, and data-mining tactics intended to identify patterns of suspicious activity that would otherwise be unobservable. At the same time that Fourth Amendment standards must be bolstered to protect targeted individuals against the misuse or abuse of intrusive search tactics, Fourth Amendment standards should be relaxed in the context of suspicionless surveillance of the general population to ensure that the government can obtain the information it needs to protect the nation against terrorism. As explained below, that relaxation must be accompanied by a narrow use requirement that bars the state from using suspicionless searches for any purpose other than that which justified the search.

Suspicionless searches are hardly a new phenomenon. As the Supreme Court held in Camara v. Municipal Court50 and See v. City of Seattle,51 where the government’s purpose is primarily “administrative,” the individualized suspicion normally demanded by the Fourth Amendment is not necessary. In a series of subsequent cases, the Court expanded the administrative search doctrine to a variety of other areas. Under a doctrine that came to be known as “special needs,” the Court

51 387 U.S. 541, 545-46 (1967).
has permitted suspicionless searches at borders\textsuperscript{52} and highway checkpoints,\textsuperscript{53} drug-testing of student-athletes\textsuperscript{54} and railroad employees,\textsuperscript{55} and searches by government employers and school officials on less than probable cause.\textsuperscript{56} Suspicionless searches justified by the administrative and special needs doctrines also were instituted at airports and public buildings in the late 1960s in response to a dramatic upsurge in airplane hijackings and courthouse bombings.\textsuperscript{57} Special needs searches have been permitted so long as the government’s primary purpose in conducting the searches was something other than simple law-enforcement or the “general interest in crime control,” and was effectively advanced by them.

Antiterrorism searches fit well within the parameters of the special needs doctrine, and the next generation of surveillance tactics, including the deployment of sophisticated scanners to detect traces of chemical, biological, and nuclear weapons, as well as a wide variety of cyber-surveillance, biometric, and data-mining projects might well qualify as special needs searches. Given the gravity of the threat posed by the unchecked proliferation of technologies that can cause immense damage to government and society, permitting such surveillance absent traditional probable cause is sensible and, in any event, probably inevitable. Not all commentators, however,

\textsuperscript{52} United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) (noting that “travelers may be stopped at fixed checkpoints near the border without individualized suspicion even if the stop is based largely on ethnicity”) (citing United States v. Martinez-Fuerte, 428 U.S. 543, 562-63(1976)).


\textsuperscript{56} Because the primary purpose (or, after the 2005 amendments PATRIOT Act amendment, a “substantial purpose”) of Foreign Intelligence Surveillance Act (“FISA”) searches is to obtain information about foreign intelligence or to prevent acts of terrorism, both legitimate and weighty governmental interests, FISA searches also can be comfortably located within the realm of the special needs doctrine.

\textsuperscript{57} See generally Ric Simmons, Searching for Terrorists: Why Public Safety Is Not a Special Need, 59 DUKE L.J. 843 (2010) (recounting the history of suspicionless antiterrorism searches, beginning with the institution of suspicionless searches at airports and courthouses, and concluding that such searches are justified as special needs doctrine if, but only if, that doctrine were modified to prevent the state from using any evidence obtained in criminal prosecutions).
agree with this analysis. In a recent article, Ric Simmons has rejected the claim that antiterrorism searches might be justified under the current special needs doctrine on grounds that “the alleged special need of ‘public safety’ is ‘inextricably intertwined’ with the goal of crime control in the antiterrorism context.” 58 According to Simmons, claiming that antiterrorism searches have “a public safety purpose rather than a law-enforcement or crime-control purpose is simply disingenuous.” 59 Simmons is, of course, correct that the distinction between public safety and crime control purposes is unconvincing at best. But that is an argument against the special needs doctrine in general, because many of the special needs searches permitted by the Court, including establishing checkpoints to catch drunk drivers and illegal immigrants, have aims that are inextricably intertwined with law enforcement. Antiterrorism searches are no different, and involve a public safety issue of vastly greater danger that may well require use of a variety of suspicionless search tactics to detect. If one accepts that doctrine itself as legitimate—grounded perhaps more on the general reasonableness of suspicionless searches in some contexts rather than the existence of non-crime control primary purposes—the fact that antiterrorism searches necessarily implicate crime control goals is not an effective argument against inclusion of such searches within the doctrine. Thus, unlike Simmons, I believe the special needs doctrine is well-suited to deal with a variety of high-tech surveillance tactics that might soon be, or already are being, regularly utilized.

Nonetheless, the need for pervasive anti-terrorism surveillance must be reconciled with the need for privacy protection. The proper balance can be struck by modifying the special needs doctrine to enforce strict limits on the use the government may make of any non-terrorism-related information thereby obtained. 60 The real danger accompanying any expansion of suspicionless searches is that government will use them for

58 Id. at 890-91 (quoting Bourgeois v. Peters, 387 F.3d 1303, 1312-13 (11th Cir. 2004)).
59 Id. at 891.
60 Id. at 915.
purposes other than preventing terrorism and that anti-terrorism surveillance will become simply another tool to further the “general interest in crime control.” \(^6\) A strict ban on the use of the fruits gathered in such searches to prosecute crimes unrelated to terrorism would prevent that from happening. Here, the traditional arguments deployed on behalf of the exclusionary rule hold sway. If the state cannot use evidence of ordinary crimes obtained in the course of performing anti-terrorism searches, it will not have any incentive to use an anti-terrorism exception as a general vehicle to fight crime. In addition, it will not be able to use the anti-terrorism rationale as a pretext to search persons it suspects of criminal activity.

Ric Simmons has taken this position to the extreme. In Simmons’ view, if the government is authorized to perform suspicionless anti-terrorism searches, the government should not be able to use any evidence gathered in the course of such a search for any prosecutorial purpose whatsoever. Such a blanket rule, however, puts law enforcement to an impossible choice—either limit anti-terrorism searches to those in which the traditional Fourth Amendment prerequisites—probable cause and a warrant or exception to the warrant requirement—are present, or forego criminal punishment of the individual. The rule, even Simmons concedes, might be hard for many to swallow given that it might require the suppression of evidence necessary to convict “a criminal attempting to blow up an airplane or shoot a judge.” \(^7\) But such a Hobson’s choice is not necessary to effectuate the purposes of an exclusionary rule in this context. The problem with intrusive anti-terrorism searches, and indeed all searches justified by the administrative and special needs doctrines, has less to do with the potential prosecutorial use of sought-for evidence or contraband and more to do with the potential for the pretextual use of the suspicionless search authority to conduct broad “fishing expedition” searches. The governing assumption of these doctrines,

---

\(^7\) Simmons, supra note 57, at 921. Simmons locates this concern among “conservatives,” but I think such concerns would be readily shared by liberals, centrists, socialists, and tea partiers alike.
after all, is that the government’s “special needs” purpose for conducting the search outweighs the intrusions it imposes on citizens. If preventing a terrorist from blowing up a plane or bombing a courthouse permits a suspicionless search of persons entering airports and courthouses, the same preventive, specific and general deterrence arguments justify prosecuting any such terrorists caught by the program.

Although in general, special needs searches should authorize government agents to search for and seize only items related to the purpose of the search, and the exclusionary rule should bar the use of unrelated evidence uncovered by it, the doctrine of implied consent should impose reasonable limits on the use of the exclusionary rule in this context.

Recognition of an implied consent exception seems sensible. Consider an airport search in which the TSA official conducting the search discovers a kilo of cocaine in a suitcase. As a type of administrative or special needs search, the exclusionary principle advocated here, without some modification, would require the TSA agent to ignore the cocaine or perhaps more likely, simply dispose of it, but either way, the rule should bar the use of the cocaine in a criminal prosecution. Now consider a so-called “sneak and peak” search of the apartment of a person of interest in a foreign intelligence investigation. Imagine that government agents, lacking any individualized suspicion of criminal conduct, perform such a search and find a kilo of cocaine in the apartment. It seems to me quite reasonable to conclude that the cocaine should be admissible as evidence in the first case, but not the second because airplane travelers have the option of avoiding an encounter with airport security simply by choosing not to fly, whereas persons who are secretly targeted in foreign intelligence investigations have no ability to avoid the encounter. Where subjects of a search have a meaningful option of avoiding it, and can at least partially control the terms on which the search takes place, the doctrines of implied consent and assumption of the risk provide a strong justification for permitting the state to keep the fruits of any evidence obtained as a result of an administrative or special needs
search. Where searches are unanticipated and submission involuntary, however, search targets cannot be said to have assumed the risk or impliedly consented to the search, and the exclusionary rule should bar the state from using any evidence not related to the primary purpose of the search in a criminal prosecution.

In short, well-designed anti-terrorism surveillance should be permitted under the special needs doctrine, and where evidence of terrorism activity is obtained through a special needs anti-terrorism search tactic, it should be admissible for prosecution of terrorism crimes. Any other evidence obtained as a byproduct of the search, however, unless doctrines of implied consent or assumption of risk apply, should be inadmissible. Although the authorization of even highly intrusive anti-terrorism surveillance is justifiable given the nature of the threat, any intrusive surveillance program must include narrow limits on the use of evidence or information obtained through such programs. Judicial oversight is crucial to this goal, and the administrative warrant model approved in Camara and See might provide the framework for an effective oversight model in the anti-terrorism context. Such oversight would properly shift to the judicial branch the heavy responsibility for ensuring that intrusive suspicionless surveillance is permitted only where the surveillance is reasonably calculated to safeguard important state anti-terrorism interests and less intrusive methods are unavailable or impractical.

Indeed, the doctrinal move I am advocating here for anti-terrorism surveillance should, I would argue, extend to the administrative and special needs doctrines in their entirety. When any type of state search or seizure activity that normally would be subjected to traditional Fourth Amendment stan-

---

63 That view was at work in many of the early airport search cases. See, e.g., United States v. Moreno, 475 F.2d 44 (5th Cir. 1973); United States v. Legato, 480 F.2d 408 (5th Cir. 1973).

64 To the extent that evaluating whether implied consent was present would raise difficult questions of voluntariness and risk assumption, such questions might be settled on a case-by-case basis. In drunk driving roadblock cases, for example, the bar on admission of collateral evidence might be found to apply unless the roadblock was set up so as to give drivers a meaningful way to avoid proceeding through the roadblock.
dards is exempted from those standards under the administrative or special needs doctrines, the state’s right to use information obtained thereby should be restricted to the purposes that justified the exemption in the first place. Roadblocks established to prevent drunk driving, or to gather evidence about hit-and-run incidents, should not be used as a pretext to search vehicles arbitrarily for weapons or contraband. School purse or locker searches that are justified by the school’s administrative need to maintain order and discipline and to enforce school rules should not be used as a pretext to permit school principals to act as constitutionally-unregulated deputies in searching for and seizing evidence of crime. Housing inspections of apartment buildings intended to ensure compliance with city housing codes should not be used by the state to gather evidence of crime against the residents of public housing.

This doctrinal solution was, in fact, pushed by some during the formative period of the administrative search and special needs doctrines, but it was ultimately rejected. However, subsequent experience with the impact of technology on the government’s ability to acquire information in myriad ways should lead to a reconsideration of that position. By shifting the focus of the Fourth Amendment away from regulating state acquisition of information and towards regulating the use of information in its possession, Fourth Amendment law would be poised to redress its twin failures: failing to provide any measure of real privacy protection in a technologically-advanced world, while failing to provide the state with a secure legal foundation to engage in the types of surveillance that will be necessary for national security in the twenty-first century.

C. The Contraband Exception and Smart Search Technology

As a practical matter, the tension between substantive privacy protection and the state interest in crime prevention

---

65 See United States v. Davis, 482 F.2d 893, 909 n.44 (9th Cir. 1973), abrogated by United States v. Aukai, 497 F.3d 955 (9th Cir. 2007); United States v. Skipwith, 482 F.2d 1272, 1278 (5th Cir. 1973) (rejecting defendant’s claim that suppression of contraband discovered during suspicionless airport search was necessary to negate incentive for officers to conduct pretextual searches).
can also be eased through expansion and development of “smart search” technology. In United States v. Place and Illinois v. Caballes, the Court established and reaffirmed the so-called “contraband exception,” holding that exposing closed luggage or automobiles to drug-sniffing dogs does not constitute a search and therefore requires no constitutional justification. According to the Court, “governmental conduct that only reveals the possession of contraband ‘compromises no legitimate privacy interest.’” This principle seems to permit deployment of sensory technologies of various sorts directed towards constitutionally protected spaces, including homes, as long as the technologies are designed, like dog sniffs, to reveal only the presence or absence of contraband. Such smart search technologies designed to detect radioactive, biological, and chemical weapons should fall safely within the Place-Caballes “contraband-only” exception.

To date, however, the Supreme Court has treated dog sniffs as sui generis, underscoring its reluctance to expand the contraband exception to other types of technology. This reluctance is in plain view in the Kyllo case. The Agema Thermovation 210 thermal imager employed by federal agents to scan Kyllo’s house was designed to detect infrared radiation which, the Court observed, “virtually all objects emit.” Since use of the thermal imager permitted the agents to obtain information about the “interior of the home that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area,’” it reasoned, the use of the thermal imager “is a search and is presumptively unreasonable without a warrant.” This holding seems to place severe limitations on the types of surveillance technologies that might fit within the Place-Caballes exception. After all, although scanning homes

---

68 Id. at 408 (emphasis in original) (quoting United States v. Jacobsen, 466 U.S. 109, 123 (1984)).
69 Id. at 409.
71 Id. at 34 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).
72 Id. at 40.
with a thermal imager provides some information of an innocent nature about the interior of the home to the person using the scanner, it is difficult to imagine many innocent homeowners caring whether the state obtains the information gleaned through use of the scanner. After all, the kind of information obtainable through use of a thermal imaging device is simply not particularly intrusive, revealing, or intimate. In revealing only information about which innocent people lack any substantial interest in preserving as private, the use of a thermal imaging device seems consistent in principle with the Place-Caballes exception. On its facts and given Place’s precedent, Kyllo probably should have been decided the other way.

As it stands, Kyllo places major obstacles in the path of efforts to deploy scanning and sensor technologies in residential areas. Although smart search technologies might be developed that exclusively detect criminal activity, it is also possible—indeed, quite likely—that technologies developed to detect the presence of nuclear, chemical, or biological weapons will also inevitably detect additional information about innocent activities.\(^{73}\) Such scanners would apparently be unlawful to use despite their significant benefits. Indeed, a second aspect of the Court’s ruling in Kyllo—its emphasis on the privileged Fourth Amendment status of the home—has led at least one court to conclude that even pure contraband searches conducted by drug-sniffing canines are unlawful when a private residence, rather than a suitcase or a car, is the target.\(^{74}\)

In light of the continuing diffusion of potentially destructive technologies, that outcome is problematic. Moreover, it seems unlikely that use of such scanners would be perceived by most citizens as a significant invasion of privacy. After all, scanners that allow security officials to view images of “naked” travelers have already been incorporated into airport security

\(^{73}\) For instance, a scanning device designed to sense the presence of radioactive substances might detect possession of isotopes used for medical purposes.

\(^{74}\) State v. Rabb, 920 So. 2d 1175 (Fla. App. 2006). The holding in Raab was anticipated by Justice Stevens in his Kyllo dissent. See 533 U.S. at 48 (Stevens, J., dissenting) (explaining that the Kyllo holding renders the use of dog-sniff-type devices unconstitutional when directed at homes).
systems, and air travelers continue to travel notwithstanding their use. Although some privacy advocates have protested the use of the scanners, most travelers appear willing to submit to such scans. The public’s grudging acceptance of through-the-clothing scanners in public airports suggests that a broader Place–Caballes doctrine might be tolerated. After all, a scanning device that renders individuals naked to the scanner obviously reveals information that most people consider to be quite private, yet scores of airport travelers already submit to such searches with little hesitation, and its routine use in the future is virtually certain. Acceptance of the technology, it seems likely, is less a result of the fact that people can opt out of such searches in favor of equally-intrusive pat-downs if they wish, than that 1) the searches occur at a remove, 2) the scans are performed by trained agents who see hundreds of such images each day and therefore are not likely to derive much personal gratification in viewing any particular image, 3) the scanners are used for the limited purpose of detecting weapons, and 4) the threat the scanners are intended to detect is significant and commonly acknowledged.

These same factors might also tend to minimize the perceived intrusion from the use of surveillance technologies that permit the government to search for the presence of WMD in constitutionally-protected places using technologies that may well also uncover information that is indisputably thought private. Public opposition to the use of such technology is likely to win reluctant acceptance, as the recent experience with airport full-body scanners suggests, as long as the surveillance occurs at a remove, information produced by the surveillance is not

disseminated beyond a small group of specially-trained agents, and the technology is used only for the limited purpose of detecting indications of significant terrorist activity.

CONCLUSION

Technology is a double-edged sword. The diffusion of destructive technology is a serious threat to national security that will require increasing vigilance to monitor and combat. Radical Islam may or may not be a passing threat, but the potential use of increasingly powerful technologies to cause major damage is a permanent feature of modern civilization that will persist as long as the technology remains available. At the same time, the government’s ability to use technology to surveil its citizens poses a dramatic threat to privacy, and that threat promises only to grow with the continued development of surveillance capacity.

In this paper, I have suggested that in order to make the Fourth Amendment relevant in light of these developments, it must adapt simultaneously in two ways. First, Fourth Amendment law must acknowledge the social and technological implications of privacy. In a high-tech, electronically networked society, virtually all important information will be stored in repositories accessible by others. Current law, which fails to recognize legitimate expectations of privacy in information that has been exposed to third parties, fails to protect privacy altogether. Understandings of what constitutes a reasonable privacy expectation must be modified to recognize that limited disclosure of private information is both necessary and essential, and that such limited disclosure does not strip such information of its private nature. Courts should broaden their definition of what constitutes a “search” by abandoning the third-party doctrine and expanding constitutional protection of information that has been disclosed to limited groups of others for anticipated purposes.

At the same time, the government’s pressing need to prevent major acts of terrorism from occurring will require it to take ever-more-intrusive surveillance measures. To the extent possible, anti-terrorism surveillance should rely on “smart surveillance technologies” that are triggered solely by the presence
of dangerous weapons or controlled materials that can be used to commit major acts of terrorism. Because such technology only reveals the presence of contraband, like the dog sniffs considered in *Place* and *Caballes*, the use of such technologies is not a “search” and thus need not be subject to any judicial scrutiny.

However, there is no guarantee that such technologies can be developed to locate and identify all major threats. In that case, other more invasive forms of surveillance may be necessary. To be effective, surveillance probably cannot be limited solely to public areas, but in all likelihood will need to intrude upon areas that currently receive constitutional protection under the Fourth Amendment. Fourth Amendment law must adapt to these eventualities while continuing to serve its vital function as a guarantor of individual liberty, autonomy, and privacy. The way to do this, I have argued, is to shift the Fourth Amendment’s focus from regulating acquisition of information to regulating its use. Such a shift can be commenced within the current doctrinal framework by recognizing that anti-terrorism surveillance constitutes a “special need” that makes application of the traditional requirements of individualized suspicion and warrants impractical and thus, in constitutional terms, unreasonable. To prevent this expansion of government search authority from undermining basic liberties, recognition of anti-terrorism searches as special needs searches must be accompanied by a restriction on the use of evidence obtained in the course of a special needs-authorized search. Any evidence of crime unrelated to terrorism should be flatly inadmissible in any criminal proceeding against the target of such a search. Evidence of terrorism crimes, however, would be admissible for purposes of criminal prosecution of such crimes, since admissibility furthers the goals for which the search was conducted. Use of the exclusionary rule here to preclude any use of non-terrorism evidence will serve its traditionally-recognized purposes of deterring improper or pretextual searches by depriving the state of the fruits of such searches.

These suggestions obviously represent only a partial solution to what is likely to become a perpetual problem—keeping the Fourth Amendment relevant in light of a rapidly changing
technological environment in which both the nature and gravity of public dangers and the capacity of government to acquire and process information about its citizens increases. Additional steps will undoubtedly be necessary, but the common denominator, I would suggest, is finding ways to shift the focus of Fourth Amendment law from regulation of the acquisition of information to regulation of its use. Additional appropriate measures might include exploring new forms of judicial oversight that demand both “prior disclosure and explanation and subsequent regular reporting and minimization,”76 perhaps along the lines already established for foreign intelligence investigations in FISA, accompanied by more carefully controlled regulation of access to and misuse of information stored in government databases, including new criminal penalties for unlawful disclosure or misuse. Not all, or perhaps not even the most important, solutions to the challenge of technology will be at the level of constitutional law. Legislative initiatives may be far more important. Nonetheless, keeping the Fourth Amendment alive and relevant in light of the coming onslaught of new technology is an essential task in the brave new world.

76 Balkin, supra note 42, at 22.