



THE FUTURE OF THE CONSTITUTION

December 08, 2010



Reuters/Brendan McDermid

Is the Fourth Amendment Relevant in a Technological Age?

Christopher Slobogin

It's the year 2015. Officer Jones, a New York City police officer, stops a car because it has a broken taillight. The driver of the car turns out to be a man named Ahmad Abdullah. Abdullah's license and registration check out, but he seems nervous, at least to Jones. Jones goes back to his squad car and activates his Raytheon electromagnetic pulse scanner, which can scan the car for weapons and bombs. Nothing shows up on the screen. Nonetheless, he attaches a Global Positioning Device known as a Q-ball underneath the rear bumper as he pretends to be looking at Abdullah's license plate.

Over the next several weeks, New York police use the GPS device to track Abdullah's travels throughout the New York City area. They also watch him take walks from his apartment, relying on public video cameras mounted on buildings and light poles. When cameras cannot capture his meanderings or he takes public transportation or travels in a friend's car, the police use drone cameras, powerful enough to pick up the numbers on a license plate, to monitor him. Police interest is piqued when they discover that he visits not only his local mosque but several other mosques around the New York area. They requisition his phone and Internet Service Provider records to ascertain the phone numbers and email addresses of the people with whom he communicates. Through digital sources, they also obtain his bank and credit card records. For good measure, the police pay the data collection company Choicepoint for a report on all the information about Abdullah that can be gleaned from public records and Internet sources. Finally, since Abdullah tends to leave his windows uncurtained, police set up a Star-Tron—binoculars with nightvision capacity—in a building across the way from Abdullah's apartment so they can watch him through his window.

These various investigative maneuvers might lead to discovery that Abdullah is consorting with known terrorists. Or they might merely provide police with proof that Abdullah is an illegal immigrant. Then there's always the possibility that Abdullah hasn't committed any crime.

The important point for present purposes is that the Constitution has nothing to say about any of the police actions that take place in Abdullah's case once his car is stopped. The constitutional provision that is most likely to be implicated by the government's attempts to investigate Abdullah is the Fourth Amendment, which prohibits unreasonable searches of houses, persons, papers and effects, and further provides that, if a warrant is sought authorizing a search, it must be based on probable cause and describe with particularity the place to be searched and the person or thing to be seized. This language is the primary constitutional mechanism for regulating police investigations. The courts have held that, when police engage in a search, they must usually have probable cause—about a 50 percent certainty—that the search will produce evidence of crime, and must also have a warrant, issued by an independent magistrate, if there is time to get one. As construed by the United States Supreme Court, however, these requirements are irrelevant to many modern police practices, including most or all of those involved



Christopher Slobogin is Milton Underwood Professor of Law, Vanderbilt University Law School.

in Abdullah’s case.

The Fourth Amendment’s increasing irrelevance stems from the fact that the Supreme Court is mired in precedent decided in another era. Over the past 200 years, the Fourth Amendment’s guarantees have been construed largely in the context of what might be called “physical searches” — entry into a house or car; a stop and frisk of a person on the street; or rifling through a person’s private papers. But today, with the introduction of devices that can see through walls and clothes, monitor public thoroughfares twenty-four hours a day, and access millions of records in seconds, police are relying much more heavily on what might be called “virtual searches,” investigative techniques that do not require physical access to premises, people, papers or effects and that can often be carried out covertly from far away. As Abdullah’s case illustrates, this technological revolution is well on its way to drastically altering the way police go about looking for evidence of crime. To date, the Supreme Court’s interpretation of the Fourth Amendment has both failed to anticipate this revolution and continued to ignore it.

The Supreme Court’s Fourth Amendment

The Fourth Amendment’s protections—warrants sworn under oath, particular descriptions of sought-after evidence, and cause requirements—are not triggered unless the government is carrying out a “search.” The Supreme Court has never defined this word the way a layperson would, as an act of looking for or into something. Rather it has looked to either property law or privacy values in fleshing out the concept.

Initially the Court defined Fourth Amendment searches in terms of property interests. A search only occurred when government engaged in some type of trespass.¹ Thus, for instance, wiretapping a phone was not a search because the surveillance involved accessing only outside lines. By contrast, the use of a spike mike that touched the baseboard of a house did implicate the Fourth Amendment.²

Then, in 1967, came the Court’s famous decision in *Katz v. United States*, which held that covert interception of communications counts as a Fourth Amendment search.³ Acting without a warrant, FBI agents bugged the phone booth Charlie Katz was using to place illegal bets. The government sought to justify the absence of a warrant by arguing that a phone booth is not a “constitutionally protected area” (because it is not a house, person, paper or effect) and that planting and listening to the bugging device on a public booth worked no trespass. Justice Black also argued, in dissent, that conversations like those intercepted in *Katz* were intangibles that “can neither be searched nor seized” and in any event did not fit

¹ See, e.g., *Silverman v. United States*, 365 U.S. 505, 510 (1961).

² Compare *Olmstead v. United States*, 277 U.S. 438 (1928) to *Silverman v. United States*, 365 U.S. 505 (1961).

³ 389 U.S. 347 (1967).

into the Fourth Amendment's foursome of houses, persons, papers and effects.⁴ All of these arguments were consistent with the traditional, property-based approach to the Fourth Amendment. But the majority stated that the Fourth Amendment "protects people, not places," and concluded that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."⁵ Justice Harlan's concurring opinion elaborated on the latter idea by recognizing that while the Fourth Amendment's protection of people still usually "requires reference to a place," places should receive that protection if they are associated with "an expectation . . . that society is prepared to recognize as 'reasonable.'"⁶ It was this latter language that has become the focal point for the Supreme Court's treatment of the Fourth Amendment's threshold.

Although it still defined the word "search" more narrowly than a layperson would, *Katz* was hailed as a long-overdue expansion of Fourth Amendment protection that was needed in an increasingly technological age. That celebration was premature. Supreme Court caselaw since *Katz* has pretty much limited that decision to its facts. While non-consensual interception of the contents of one's communications over the phone or via computer remains a Fourth Amendment search, all other government efforts to obtain evidence of wrongdoing are immune from constitutional regulation unless they involve some type of physical intrusion. The Court has arrived at this intriguing result relying on four variations of the search-as-physical-intrusion theme: the knowing exposure doctrine, the general public use doctrine, the contraband-specific doctrine, and the assumption of risk doctrine. All four doctrines have the effect of enabling the government to conduct most technologically-aided, virtual searches without having to worry about the Fourth Amendment.

Katz itself said that while conversations over a public phone can be private for Fourth Amendment purposes, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."⁷ This notion was first applied to government monitoring of activities in public spaces. In *United States v. Knotts*, the police lost visual sighting of the defendant's car as it travelled the streets but were able to use a tracking device affixed to the car to locate its eventual whereabouts.⁸ Although the police would have been unable to find the defendant without the beeper, the Court held that its use was not a Fourth Amendment search because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."⁹ Thus, after *Knotts*, police can use technology to spy on public activities without worrying about the Fourth Amendment.

⁴ Id. at 365 (Black, J., dissenting).

⁵ Id. at 351.

⁶ Id. at 361 (Harlan, J., concurring).

⁷ 389 U.S. at 351.

⁸ 460 U.S. 376 (1983).

⁹ Id. at 281.

In three later decisions, sometimes called the “flyover cases,” the Court held that the knowing exposure doctrine also sanctions suspicionless police viewing of activities on *private* property—even those that take place on the curtilage (the area immediately surrounding the premises)—so long as the police do not physically enter that area but rather view it from the air.¹⁰ To the argument that the curtilage should be protected by the Fourth Amendment, at least when it is surrounded by a fence, the Court fancifully responded that “[a]ny member of the public” flying in navigable airspace could have seen what the police saw.¹¹ In one of these three cases, Chief Justice Burger, apparently recently returned from a trip to London, opined that even someone on a double-decker bus could have seen over the defendant’s fence, thus rendering unreasonable any privacy expectation harbored by the defendant.¹²

The implications of this take on the knowing exposure doctrine for technological surveillance should be fairly clear. As long as the police are located on a lawful vantage point, they can use technology to spy on anything occurring in public spaces or on private property outside the home without worrying about the Fourth Amendment. Governments have been quick to recognize how significantly this rule enhances investigations in an era of technological innovation. Putting a cop on every street corner 24/7 is expensive and not cost-effective. But video cameras of the type used to track Abdullah are increasingly seen as a good investment, especially since 9/11 has triggered federal funding for such projects. For instance, Chicago trains more than 2,200 cameras, many equipped with zoom and nightviewing capacity, on its urban populace day and night, every day of the week, some operating openly, others covertly; all of them are patched into the city’s \$43 million operations center.¹³ Where cameras don’t exist, satellite photography or drone cameras (like the ones just recently positioned over Houston¹⁴) might be available. *Knotts* ensures that the Fourth Amendment will not get in the way of these surveillance systems, at least if they are trained on venues outside the home.

Similar developments are occurring with tracking technology. Today it is both technologically and economically feasible to outfit every car with a Radio Frequency Identification Device that communicates current and past routes to an Intelligent Transportation System (ITS) computer.¹⁵ Cell phones can be used to track anyone who has one within feet of their location; in the past several years, police have made over 8 million requests to phone companies for help in carrying

¹⁰ *Ciraolo v. California*, 476 U.S. 207 (1986); *Riley v. Florida*, 488 U.S. 445 (1989); *Dow Chemical v. United States*, 476 U.S. 227 (1986).

¹¹ *Riley*, 488 U.S. at 446.

¹² *Ciraolo*, 476 U.S. at 211.

¹³ Fran Spielman, *Feds Give City \$48 Million in Anti-terrorism Funds*, *Chicago Sun-Times*, Dec. 4, 2004, at 10.

¹⁴ Katie Baker, *Houston Police Use Drone Planes*, available at <http://www.truthnews.us/?p=973>.

¹⁵ See Federal Trade Comm’n, *Radio Frequency Identification: Applications and Implications for Consumers 3-5* (2005); Smithsonian National Air and Space Museum, *How Does GPS Work?*, at <http://www.nasm.si.edu/exhibitions/gps/work.html>.

out cellphone GPS tracking.¹⁶ Again, in light of *Knotts*, most courts hold that the Fourth Amendment has nothing to say about such programs even when they catalogue weeks of travel.¹⁷ And the flyover cases also make clear that tracking onto private property, short of entry into the home, does not implicate the Fourth Amendment as long as, during that process, no government agent physically intrudes on curtilage.

One of the flyover cases also introduced the second Court doctrine limiting the definition of “search” — the general public use concept. In *Dow Chemical v. EPA*, the government relied on a \$22,000 mapmaking camera to spy on Dow Chemical’s fenced-in business property from an airplane. The Court had no problem with this use of technology because, it astonishingly asserted, such cameras are “generally available to the public.”¹⁸ According to the majority, because ordinary citizens can obtain such cameras and use them to view open fields and curtilage from airplanes, the government’s actions in *Dow Chemical* did not infringe the Fourth Amendment.

Fifteen years later, the Court appeared to rethink this idea, at least when technology is used to spy on a home. In *Kyllo v. United States*, it held that a thermal imaging device is not in general public use, despite the fact that it costs a mere \$10,000, and went on to hold that relying on such a device to detect heat differentials inside a house is a search.¹⁹ In the end, however, *Kyllo* places few limitations on the use of technology to spy on the populace, for three reasons.

First, *Kyllo*’s ban on sophisticated technology applies only to viewing of the home. Thus, as already noted, government is able to use, without infringing Fourth Amendment interests, any type of technology, generally available or not, if the target is located in a public space or on curtilage that is viewed from an area outside the curtilage.

Second, *Kyllo* expanded on *Dow Chemical*’s holding by stipulating that even the home is not protected from spying with devices that are in “general public use.” While thermal imagers may not cross that threshold, a wide array of technology is easily accessible by the public and thus can be used to peer inside the home. For instance, the lower courts have been willing to hold that police reliance on flashlights, binoculars, and zoom cameras to see inside premises does not implicate the Fourth Amendment.²⁰ Since telescopes can be bought at Walmart for under

¹⁶ Justin Elliott, How Easy Is It for the Police to Get GPS Data from Your Phone? TPM Muckraker, Dec. 9, 2009, at http://tpmmuckraker.talkingpointsmemo.com/2009/12/cell_phone_surveillance_unpacking_the_legal_issues.php

¹⁷ Kevin Keener, Personal Privacy in the Face of Government Use of GPS, 3 Info. Soc’y J. L. & Policy 473 (2007) (describing cases permitting warrantless use of GPS for real-time tracking and to learn about previous travels, and noting that only three jurisdictions require a warrant for either purpose). See also *In re Application of USA for Order Directing Provider of Electronic Communication Service to Disclose Records to Government*, 2010 WL 3465170. But see *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).

¹⁸ 476 U.S. at 238.

¹⁹ 533 U.S. 37, 40 (2001).

²⁰ *State v. Vogel*, 428 N.W.2d 272, 275 (S.D. 1988) (zoom cameras); *State v. Rose*, 909 P.2d 280, 286 (Wash. 1996) (flashlights); *Colorado v. Oynes*, 902 P.2d 880, 883 (Colo. Ct. App. 1996) (binoculars); *Oregon v. Carter*, 790 P.2d 1152, 1155 (1990) (binoculars).

\$100, presumably they too fit in this category. Two courts have even held that night-vision scopes of the type used in Abdullah's are in general public use (which is not surprising, since they can be bought on eBay for under \$2000).²¹

A third reason *Kyllo* is a thin reed for privacy advocates is that, in a bow to the knowing-exposure doctrine, the majority in that case stated that even very sophisticated technology may be used to view activities that take place in the home if it merely duplicates what a law enforcement officer could have seen with the naked eye from a lawful vantage point.²² That idea, taken literally, could mean that government can rely on images from public camera systems or even satellites to see through uncurtained windows without infringing Fourth Amendment interests, as long as those windows are situated near a public street or sidewalk.

Even those parts of the home that are curtained and walled-off may not be protected from sophisticated technological surveillance if the technology is contraband-specific, meaning that it detects only items that are evidence of criminal activity. The Supreme Court broached this third limiting doctrine in a case involving a drug-sniffing dog, where it concluded, as a majority of the justices later put it, that "government conduct that can reveal whether [an item is contraband] and no other arguably 'private' fact[] compromises no legitimate privacy interest."²³ As anyone who has visited an airport knows, scientists have developed "mechanical dogs" that can sniff out weapons or contraband. Most of these instruments, particularly if based on x-ray technology, are not weapon- or contraband-specific; they expose other items as well. But as contraband-specific devices are developed, such as the Raytheon device the state police officer aimed at Abdullah's car, they will allow police to cruise the streets scanning vehicles, people and homes for illicit items without in any way infringing on Fourth Amendment interests, because that type of virtual search would reveal only contraband.²⁴

The three doctrines discussed to this point provide law enforcement officials with a wide array of options that allow technology to play an important, if not dominant role, in their investigative pursuits, with no interference from the Fourth Amendment. The Supreme Court doctrine that most powerfully facilitates that role, however, is found in a series of cases holding that people assume the risk that information disclosed to third parties will be handed over to the government and thus cannot reasonably expect it to be private.

The two most important decisions in this regard are *Miller v. United States* and *Smith v. Maryland*. In *Miller* the Court held that an individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that

²¹ Baldi v. Amadon, No. Civ. 02-3130-M, 2004 WL 725618, at *3 (D.N.H. Apr. 5, 2004); *People v. Katz*, No. 224477, 2001 WL 1012114, at *2 (Mich. App Sept. 4, 2001).

²² 533 U.S. at 40 (concluding that if the police could have seen the details inside the home "without physical intrusion" than viewing them technologically is not a search).

²³ *Place v. United States*, 466 U.S. 109, 122-23 (1984); *Jacobsen v. United States*, 462 U.S. 696, 707 (1983).

²⁴ See Paul Joseph Watson, Fourth Amendment-Violating Mobile X-Ray Scanners Hit the Streets, Prison Planet.com, August 25, 2010, available at www.prisonplanet.com/4th-amendment-violating-mobile-x-ray ("backscatter x-ray vision devices mounted on trucks are already being deployed inside the United States to scan passing individuals and vehicles . . .").

person to the government . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”²⁵ That reasoning might make sense when the other person is an acquaintance, who can decide for his or her own reasons to reveal a friend’s secrets to others.²⁶ But in *Miller* the third party was a bank. The Court held that even here one assumes the risk of a breach of confidence, and therefore that depositors cannot reasonably expect that information conveyed to their banks will be protected by the Fourth Amendment. In *Smith*, the Court similarly held that a person who uses the phone “voluntarily” conveys the phone number to the phone company and “assume[s] the risk that the company would reveal to police the numbers he dialed.”²⁷ As a result of *Miller* and *Smith*, the Fourth Amendment is irrelevant when government agents obtain personal information from third party record-holders, at least when the subject of that information knows or should know the third party maintains it.

These decisions, which came at the dawn of the Information Age in the mid-1970s, have enormous implications for law enforcement investigation today. Traditionally, gathering documentary evidence required physically travelling to the relevant repository and asking for the appropriate records, or in more modern times at least arranging for a fax transmission. That has all changed in the past couple of decades. The quantity of the worlds’ recorded data has doubled every year since the mid-1990s. Computing power necessary to store, access, and analyze data has also increased geometrically since that time, and at increasingly cheaper cost.²⁸ Because of *Miller* and *Smith*, government can access free and clear of Fourth Amendment constraints all of this information, as well as the other types of data the police gathered in Abdullah’s case, either directly or through the many private companies that today exist for the sole purpose of collecting and organizing personal transactions.

As Abdullah’s case illustrates, not only is personal information now easier to obtain, but it is much easier to aggregate. In the old days accumulation of data from disparate sources involved considerable work. Today it can often occur at the touch of a button, with the result that private companies as well as governments now excel at creating “digital dossiers” from public and quasi-private records.²⁹

The scope of the government’s technologically-driven data-gathering efforts is staggering. A program tellingly called REVEAL combines information from

²⁵ 425 U.S. 435, 443 (1976).

²⁶ See, e.g., *Hoffa v. United States*, 385 U.S. 293 (1966).

²⁷ 442 U.S. 735, 744 (1979).

²⁸ Jeffrey W. Seifert, *Data Mining and Homeland Security: An Overview 2* (Congressional Research Service, Jan. 18, 2007), available at www.fas.org/sgp/crs/intel/RL31798.pdf.

²⁹ See Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age* ch. 2 (2004); Martha Neil, *Beyond Big Brother: Som Web Hosts Are Watching Your Every Keystroke*, *Privacy Law*, August 2, 2010, available at www.abajournal.com/news/article/some_web_hosts_are_watching_your_every_keystroke (“Web hosts are watching what you read, what you say, what you buy and where you go online, via cookies and other tracking tools that enable them to assemble—and sell-detailed profiles to other companies.”).

sixteen government and private databases, including those maintained by the IRS and the Social Security Administration.³⁰ MATRIX, a federally-funded data accumulation system that at one time catered to a number of state law enforcement agencies, claimed to allow clients to “search tens of billions of data records on individuals and business in mere seconds.”³¹ The best known effort in this regard originally carried the discomfiting name “Total Information Awareness” (TIA), later changed to “Terrorism Information Awareness.” The brainchild of Admiral Poindexter and the Department of Defense’s Defense Advanced Research Projects Agency (DARPA), TIA was designed to access scores of information sources, including financial, travel, educational, medical and even veterinary records, at which point terrorist profiles would help determine which individuals should receive special attention.³² Although TIA was de-funded in 2003,³³ it continues to exist under other names and in other forms, including something called “fusion centers,” which feature computer systems that “fuse” information from many different sources in an effort to assist law enforcement efforts.³⁴

TIA’s original icon, a picture of an all-seeing eye surveying the globe accompanied by the maxim “Knowledge is Power,” would seem to trigger the privacy protection meant to be provided by the Fourth Amendment. But the Supreme Court’s assumption of risk doctrine has apparently exempted TIA-like programs from constitutional scrutiny. As a result, government may constitutionally construct personality mosaics on each of us, for no reason or for illicit ones, as long as all of the information comes from third parties.

Even if, because of its scope, the Total Information Awareness program were thought to be governed by the Fourth Amendment, other Supreme Court doctrines might well permit it to continue in relatively unrestricted fashion. The most important of these doctrines is implicated, in the words of a widely cited 1985 Supreme Court opinion, “in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.”³⁵ Lower courts have made clear that this special needs exception readily applies to anti-terrorism efforts like TIA. For instance, courts have held that checkpoints established to detect terrorists are not focused on “normal” crime. As then-Judge Sotomayor stated in upholding a federal program that authorized routine suspicionless searches of passengers and cars on a New York ferry system in the wake of 9/11, “[p]reventing or deterring large-scale terrorist attacks presents problems that are distinct from standard law

³⁰ Dalia Naamani-Goldman, *Anti-Terrorism Program Mines IRS’ Records*, Los Angeles Times, Jan. 15, 2007, at C1.

³¹ See Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. Crim. L. & Criminol. 1059, 1151 (2006).

³² Defense Advanced Research Projects Agency, U.S. Dept’ of Defense, *Report to Congress Regarding the Terrorism Information Awareness Program 3-9* (May 20, 2003).

³³ TIA was de-funded by a voice vote. See 149 Cong. Rec. Sen. 1370-02 (Jan. 23, 2003).

³⁴ For a description of post-TIA programs, see Ellen Nakashima & Alec Klein, *Profiling Program Raises Privacy Concerns*, Washington Post (Feb. 28, 2007) at B1; Shane Harris, *TIA Lives On*, National J. 66 (Feb. 25, 2006); and Lillie Coney, *Statement to the Department of Homeland Security Data Privacy and Integrity Advisory Committee 1, 4* (Sept. 19, 2007) (available at www.spic.org/privacy/fusion/fusion-dhs.pdf).

³⁵ *T.L.O. v. New Jersey*, 469 U.S. 325, 353 (1985) (Blackmun, J., concurring).

enforcement needs and indeed go well beyond them.”³⁶

Courts have also relied on special needs analysis to uphold programs that are not investigative in nature. For instance, in holding that a government plan to force prisoners to provide DNA samples is exempt from traditional Fourth Amendment rules, the Fourth Circuit noted that the sampling was “not trying to determine that a particular individual has engaged in some specific wrongdoing.”³⁷ Courts could easily decide that TIA and similar programs are designed primarily to collect intelligence about terrorism or other criminal activity and thus are special needs programs that, even if denominated “searches,” do not have to meet the usual Fourth Amendment requirements.

Who Cares?

Most virtual searches are not Fourth Amendment searches or, if they are, they can usually be carried out on little or no suspicion if they do not involve interception of communication content. Given the huge amount of information that virtual searches provide about everyone’s activities and transactions, traditional physical searches—with their cumbersome warrant and probable cause requirements—are much less necessary than they used to be. American citizens may eventually live, and indeed may already be living, in a world where the Fourth Amendment as currently construed is irrelevant to most law enforcement investigations. Technological developments have exposed the fact that the courts’ view of the Fourth Amendment threatens the entire edifice of search and seizure law.

Some might react to all of this with a shrug of the shoulders. Think about Abdullah again. If he is a terrorist, technology has been a boon to our security. Even if he’s merely an illegal immigrant, technology has enabled us to catch a miscreant who otherwise might not have been caught. And because the virtual searches in his case were carried out covertly, if he’s innocent of wrongdoing he’ll probably never even find out he’s been investigated. Indeed, given economic and other practical constraints on the government, most people who have done nothing wrong will never become a target at all. So, why impose constitutional limitations on virtual searches?

One reason is that many people *are* bothered by technological surveillance. Studies that have asked people to rate the “intrusiveness” of various types of police investigative techniques show that the typical person views the techniques the government used in Abdullah’s case to be more than a minor transgression.³⁸ On average, this research indicates, government accessing of bank, credit card and

³⁶ Cassidy v. Chertoff, 471 U.S. 67, 82 (2d Cir. 2006).

³⁷ Nicholas v. Goord, 430 F.3d 652, 668 (2005). See also, United States v. Pool, 2010 WL 3554049 (upholding provision of federal Bail Reform Act requiring defendant to provide DNA sample as a condition of pre-trial release).

³⁸ See Christopher Slobogin, Privacy at Risk: The New Government Surveillance and the Fourth Amendment 112 & 184 (2007) (tables reporting data).

phone records is thought to be more intrusive than search of a car, which requires probable cause under the Fourth Amendment.³⁹ Technological tracking of a vehicle is viewed, on average, to be nearly as intrusive as a frisk, which requires reasonable suspicion, a lesser level of certainty than probable cause but still something more than a hunch.⁴⁰ And public camera surveillance is considered, on average, to be much more intrusive than a roadblock, which is also regulated by the Fourth Amendment and in some situations requires individualized suspicion.⁴¹

Even programs designed to protect national security have sparked resistance. In 2006 reports surfaced that the National Security Agency had monitored hundreds of millions of overseas and domestic phone calls to determine whether any communication patterns fit terrorist profiles. A subsequent poll indicated that, while 63% felt that the program was an “acceptable way to fight terrorism,” 37% disagreed.⁴² The latter percentage would undoubtedly climb if this kind of surveillance were to spread from the NSA to ordinary police departments, and from national security investigations to investigations of ordinary crime.

Antipathy toward virtual searches could exist for a number of reasons. First, there is the prototypically American aversion to overweening government power. As one opponent of the NSA program inveighed,

Whether the next president is a Republican or a Democrat, there is nothing to prevent him from using this Executive Branch database for his own political purposes. That is a real threat to America. This database needs to be immediately and completely destroyed.⁴³

From J. Edgar Hoover’s misuse of FBI files to Attorney General John Mitchell’s illegal authorization of wiretaps on thousands of 1970s’ dissidents, from recent reports of the FBI’s illicit use of National Security Letters to the Bush Administration’s attempts to access information about anti-war journalists and protesters, history confirms that, as TIA’s icon proclaims, Knowledge is Power.⁴⁴ And power can be abused.

Even when government officials act in good faith in an effort to stomp out real crime, they can overstep their initial authority. The phenomenon of mission creep is well-known in virtual search circles. For instance, fusion centers, initially designed as a replacement for TIA, now routinely come into play in ordinary investigations and collect all sorts of information about all sorts of individuals.

³⁹ *Carroll v. United States*, 267 U.S. 132 (1925).

⁴⁰ *Terry v. Ohio*, 392 U.S. 1 (1968).

⁴¹ *Indianapolis v. Edmond*, 531 U.S. 32 (2000).

⁴² Karen Tumulty, *Inside Bush’s Secret Spy Net*, *Time*, May 22, 2006, at 35.

⁴³ Michael Stabeno, *Letter to the Editor*, *Portland Oregonian*, May 16, 2006, at B09, available at 2006 WLNR 8457654.

⁴⁴ For a description of Hoover’s abuses, see Solove, *The Digital Person*, 175-187; for Mitchell’s, see Frederick S. Lane, *American Privacy* xvii (2009); for recent abuses, see Christopher Slobogin, *Distinguished Lecture: Surveillance and the Constitution*, 55 *Wayne St. L. Rev.* 1107, 1128-29 (2009), and William Fisher, *DoD Release Records of Illegal Surveillance*, *William Fisher*, March 3, 2010, available at www.truthout.org/dod-release-records-illegal-surveillance57329 (detailing DoD collection of intelligence on Planned Parenthood, antiwar groups, and nonviolent Muslim conferences).

One fusion center trainer put the point quite succinctly: “If people knew what we were looking at, they’d throw a fit.”⁴⁵ Similarly, municipal cameras originally set up to deter violent crime and property theft are today more commonly used as a means of identifying “flawed consumers” — the homeless and vagrants — and removing them from community centers.⁴⁶ As Peter Swire has observed, “history . . . shows the temptation of surveillance systems to justify an ever-increasing scope of activity.”⁴⁷

Exacerbating the mission creep phenomenon is the inevitable fact that, just as with physical searches, virtual searches can lead to mistakes, sometimes serious ones. Based on record reviews conducted after 9/11, thousands of persons of Middle-Eastern descent were subject to interviews and scores of them were detained as “material witnesses” for months on end on little or no suspicion, as evidenced by the fact that virtually none were prosecuted for terrorism-related crime and the vast majority were not prosecuted for any crime.⁴⁸ No-fly lists contain a notorious number of false positives, including the late Senator Ted Kennedy and former Assistant U.S. Attorney General Jim Robinson.⁴⁹ Gun-detection devices might sound the alarm for those who are legally, as well as illegally, carrying concealed weapons.⁵⁰ Methamphetamine profiles can lead to arrests of anyone who buys an abnormal amount of cold medicine.⁵¹

It does not take much imagination to compare the capacious intrusions technology facilitates to the general warrants that led to the inclusion of the Fourth Amendment in the Constitution. General warrants were abhorred by the colonists because they permitted ordinary officers to search any home and conveyance at their discretion.⁵² As James Otis declared in the speech that John Adams later declared gave birth to the American Revolution, writs of assistance were obnoxious because they permitted entries of anyone’s home or conveyance on “bare suspicion.”⁵³ Under the Supreme Court’s approach to virtual searches, even bare suspicion is not required when police monitor our transactions and public activities.

The ill effects of virtual searches do not stop with official misuse of information resulting from general searches. Less tangible, but arguably just as important, is the discomfort people feel when they are being watched or monitored even if, or perhaps especially when, they aren’t sure they are being targeted. In other words, for many individuals privacy vis-à-vis the government has value in and of itself,

⁴⁵ Torin Monahan & Neal A. Palmer, *The Emerging Politics of DHS Fusion Centers*, 40 *Security Dialogue* 617, 625-30 (2009).

⁴⁶ Slobogin, *Privacy at Risk*, 96 & 257-58 n. 134.

⁴⁷ Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 *Geo. Wash. L. Rev.* 1306, 1371 (2004).

⁴⁸ See William Fisher, *Ashcroft’s Post-9/11 Roundups Spark Lawsuit*, Sept. 27, 2010, available at [www.Truth-out.org/ashcrofts-post-911-roundups-spark-lawsuit63626](http://www.truth-out.org/ashcrofts-post-911-roundups-spark-lawsuit63626).

⁴⁹ Slobogin, *Surveillance and the Constitution*, at 1128.

⁵⁰ In more than half the states, carrying a concealed weapon is legal. See Nat’l Rifle Ass’n, *Inst. for Legislative Action, Right-to-Carry* (2007), available at <http://www.nraila.org/Issues/FactSheets/Read.aspx?ID=18>.

⁵¹ Brian Sullivan, *Silly Surveillance*, *ABA Journal* 71 (Dec. 2009).

⁵² JACOB B. LANDYNSKI, *SEARCH AND SEIZURE AND THE SUPREME COURT* 30-31 (1966).

⁵³ 2 *LEGAL PAPERS OF JOHN ADAMS* 142-44 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965).

regardless of whether there is evidence of government abuse, over-stepping or mistake. Thus, when Daniel Solove asked people on his privacy blog how they would respond to the person who claims to be unconcerned about government surveillance because “I’ve-got-nothing-to-hide,” he received numerous vigorous retorts: “If you’ve got nothing to hide, why do you have curtains?”; “If you’ve got nothing to hide, can I see your credit card bills for the last year?;” and “If you’ve got nothing to hide, then you don’t have a life.”⁵⁴

These sentiments may be associated with real-world impacts even when government makes no use of the surveillance product. Studies of the workplace indicate that panoptic monitoring makes employees, even completely “innocent” ones, more nervous, less productive, and more conformist.⁵⁵ And surveillance of public activities—whether via cameras, satellites, or visual means—clearly diminishes the anonymity people expect not only in the home but as they go about their daily activities in public spaces. As one court—unfortunately, an outlier that is not representative of the typical court on these issues—stated in describing the impact of a Q-ball GPS device of the type used in Abdullah’s case:

Disclosed in the data retrieved from the transmitting unit, nearly instantaneously with the press of a button on the highly portable receiving unit, will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on. What the technology yields and records with breathtaking quality and quantity, is a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our professional and avocational pursuits.⁵⁶

Most broadly, freedom from random governmental monitoring—of both public spaces and recorded transactions—might be an essential predicate for self-definition and development of the viewpoints that make democracy vibrant. This reason to be concerned about virtual searches, while somewhat amorphous, is important enough to have been remarked upon by two Supreme Court justices. The first Justice wrote:

Walking and strolling and wandering . . . have been in part responsible for giving our people the feeling of independence and self-confidence, the feeling of creativity. These amenities have

⁵⁴ Daniel Solove, “I’ve Got Nothing to Hide” and Other Misunderstandings of Privacy, 44 *San Diego L. Rev.* 745, 750 (2007).

⁵⁵ Carl Botan, *Communication Work and Electronic Surveillance: A Model for Predicting Panoptic Effects*, 63 *Communications Monographs* 293, 308-09 (1996). See Slobogin, *Privacy at Risk*, 257 n. 129.

⁵⁶ *People v. Weaver*, 12 N.Y.3d 433, 882 N.Y.S.2d 357, 909 N.E.2d 1195 (May 12, 2009). For a more recent case espousing the same views, see *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).

dignified the right to dissent and have honored the right to be nonconformists and the right to defy submissiveness. They have encouraged lives of high spirits rather than hushed, suffocating silence.⁵⁷

The second justice wrote:

Suppose that the local police in a particular jurisdiction were to decide to station a police car at the entrance to the parking lots of a well-patronized bar from 5:30 p.m. to 7:30 p.m. every day . . . I would guess that the great majority of people . . . would say that this is not a proper police function. . . . There would be an uneasiness, and I think a justified uneasiness, if those who patronized the bar felt that their names were being taken down and filed for future reference. . . . This ought not be a governmental function when the facts are as extreme as I put them.⁵⁸

The first passage comes, not surprisingly, from Justice William Douglas, a lion of civil rights. More surprising is the author of the second passage. It was William Rehnquist, writing soon after he joined the Court and began a long career of reducing Fourth Amendment protections.

None of this means that surveillance by the government should be prohibited. But it does suggest that it should be regulated under the Constitution, just as physical searches are. Furthermore, it suggests that back-end regulation of virtual searches, through provisions limiting information disclosure and use, will not be sufficient, because it will not prevent the subterranean abuse of information already collected, nor will it eradicate the feeling of being watched and the chilling effects occasioned by surveillance. Thus, proposals advocating a trade-off between disclosure rules and collection rules (allowing the latter rules to be relaxed or eliminated if the former rules are strengthened) will probably greatly exacerbate these harms.⁵⁹ Restrictions on the extent to which covertly obtained information is revealed to the public are necessary, but they are not a panacea. Just as search of a house requires probable cause even when the occupant is not at home, the government should have to justify privacy-invading virtual searches even though no physical confrontation is involved.

A Technologically-Sensitive Fourth Amendment

If reform of the Fourth Amendment were thought to be important as a means of responding to technological developments, the most obvious first step would be to conform the definition of search to its lay meaning of looking into, over or through

⁵⁷ *Papachristou v. Jacksonville*, 405 U.S. 156, 164 (1972).

⁵⁸ William H. Rehnquist, *Is An Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement: Or: Privacy, You've Come a Long Way, Baby*, 23 *Kansas L. Rev.* 1, 9 (1974).

⁵⁹ See William J. Stuntz, *Local Policing after the Terror*, 111 *Yale Law Journal* 2137, 2181 (2002).

something in order to find somebody or something.⁶⁰ This move would immediately encompass virtual searches within the ambit of the Fourth Amendment's protections. Camera surveillance, tracking, targeting places or people with devices (whether or not they are in general public use or contraband-specific), and accessing records via computer all involve searches under this definition.

Reform could not stop there, however. Current Fourth Amendment law also usually requires probable cause for a search. If police attempts to watch a person walk down the street, follow a car on the public highway, or peruse court records or utility bills all required probable cause, law enforcement would come to a screeching halt. Indeed, it may have been to avoid such a disaster that most members of the Court, including many of its liberal members, have been willing simply to declare that these investigative techniques are immune from constitutional review.⁶¹

But there is a compromise position, suggested by the Fourth Amendment itself. After all, the Fourth Amendment only requires that searches and seizures be "reasonable." It does not require probable cause or any other particular quantum of suspicion.

I have argued elsewhere that the Fourth Amendment's reasonableness inquiry should adhere to a proportionality principle.⁶² The idea of calibrating the justification for an action by reference to its impact on the affected party permeates most other areas of the legal system.⁶³ For instance, at the adjudication stage the law assigns increasingly heavier burdens of proof depending upon the consequences: a mere preponderance of the evidence in civil litigation, the more demanding clear and convincing evidence standard for administrative law suits and civil commitment, and the most onerous requirement of proof beyond a reasonable doubt when the state deprives an individual of liberty through criminal punishment. Similarly, levels of scrutiny in constitutional litigation vary depending on whether the individual right infringed by the government is "fundamental."

Indeed, the proportionality principle even has found its way into the Supreme Court's Fourth Amendment caselaw. It provides the best explanation, for example, of why arrests require probable cause, while stops only require reasonable suspicion. As the Court stated in *Terry v. Ohio*, the case that established this particular hierarchy, "there can be 'no ready test for determining reasonableness other than by balancing the need to search against the invasion

⁶⁰ Of more than passing interest is the fact that, in *Kyllo*, Justice Scalia felt prompted to note that this was also the definition of search at the time the Fourth Amendment was drafted. 533 U.S. at 32, n.1.

⁶¹ See Christopher Slobogin, *The Liberal Assault on the Fourth Amendment*, 4 Ohio St. J. Crim. L. 603, 605-11 (2007) (making this argument).

⁶² Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (2007).

⁶³ See generally Alice Ristroph, *Proportionality as a Principle of Limited Government*, 55 Duke L. J. 263 (2005) ("Principles of proportionality put the limits into any theory of limited government.").

which the search entails.”⁶⁴ Unfortunately, the Court has applied this principle only haphazardly and, when it does apply it, inconsistently.

A more formal adoption of the proportionality principle would state that, for every government action that implicates the Fourth Amendment, government must demonstrate “cause” — defined as the level of certainty that evidence of wrongdoing will be found — roughly proportionate to the intrusiveness of the search.⁶⁵ Given the history of the Fourth Amendment, the baseline rule for application of the proportionality principle would be that searches of houses and similarly intrusive actions require probable cause. But less intrusive searches and seizures could be authorized on something less. For instance, the Court is clearly correct in its intuition that police viewing of public activities are generally less invasive than police entries into houses. Short-term camera surveillance and tracking of public movements, use of binoculars to look through a picture window, or perusal of a record of an individual’s food purchases would not require probable cause under proportionality reasoning.

In contrast to the Supreme Court’s jurisprudence, however, only the most minimal intrusions would be exempt from Fourth Amendment regulation in a proportionality-driven regime. Thus, while randomly surveying the public streets with a camera might be untouched by the Fourth Amendment, using cameras to target an individual would trigger its guarantees (albeit perhaps only in the sense that an articulable reason for the targeting would be required).⁶⁶ In further contrast to the Supreme Court’s approach, proportionality reasoning dictates that law enforcement demonstrate a high degree of cause for virtual searches determined to be as invasive or nearly as invasive as entry into the home. For instance, if the aforementioned empirical research on lay views is replicated — thus contradicting the Court’s dismissive assertions about the expectation of privacy “society” associates with bank and phone records — *Miller* and *Smith* would be overturned, and police would have to demonstrate reasonable suspicion or perhaps even probable cause before gaining access to such information.

At least one exception to the proportionality principle should be recognized, however. When the purpose of a search is to prevent significant, specific, and imminent danger, society’s interest in protecting itself is sufficiently strong that the justification normally required by proportionality reasoning should be relaxed. This danger exception is consistent with the clear and present danger exception in First Amendment jurisprudence, as well as with *Terry v. Ohio*, which sanctioned preventive frisks when police have reasonable suspicion, rather than probable

⁶⁴ 392 U.S. at 21 (quoting *Camara v. Municipal Ct.*, 387 U.S. 523, 536-37 (1967)).

⁶⁵ References to “intrusiveness” or “invasiveness” are found throughout the Court’s Fourth Amendment caselaw with little or no attempt at definition. I have argued that the concept should be an amalgam of empirically-determined views and positive law reflecting views about privacy, autonomy, freedom of speech and association and, most generally (following the Fourth Amendment’s language), “security.” Slobogin, *Privacy at Risk*, at 23-37, 98-108. See also, Christopher Slobogin, *Proportionality, Privacy and Public Opinion: A Reply to Kerr and Swire*, 94 *Minn. L. Rev.* 1588, 1594-1608 (2010) (describing the concept of intrusiveness in detail).

⁶⁶ For a more detailed description of this regime, see Slobogin, *Privacy at Risk*, ch. 5.

cause, that a person they have stopped is armed.⁶⁷

Other exceptions might be necessary, especially if, as discussed below, the search is of a large group. The important point for now is that proportionality reasoning should be the presumptive framework for Fourth Amendment analysis. The Court's Fourth Amendment jurisprudence—which, aside from the holding in *Katz* itself, is identical to the property-based regime that *Katz* supposedly discarded—opens the door wide to the extremely invasive investigative techniques that technological advances are providing the government at an increasing rate. By recognizing that Fourth Amendment searches may take place on something less than probable cause, proportionality reasoning facilitates extension of the Fourth Amendment's protection beyond physical invasions and thus allows it to adapt to modern law enforcement.

Searches of Groups

A number of the technologically-aided investigative techniques described in earlier pages—camera surveillance and Total Information Awareness, to name two—involve searches that affect large numbers of people. In effect they are search and seizure *programs*, not searches and seizures targeting a specific individual. The usual Fourth Amendment paradigm—sometimes said to focus on “individualized suspicion”—does not work well in these situations. At least four possible alternatives can be imagined, varying most prominently in terms of the degree to which courts have control over whether the program is constitutionally viable.⁶⁸

The Supreme Court has usually dealt with group searches and seizures by invoking its special needs doctrine. Extremely deferential to legislative and executive decision-making, special needs jurisprudence usually upholds government programs that allow suspicionless searches and seizures of groups, based on two bald assertions. First, the Court proclaims that the government is confronted with a significant law enforcement problem involving something other than “ordinary criminal wrongdoing” of the type handled by the regular police force—such as illegal immigration, student drug use, or terrorism—and notes that the problem will be difficult to handle if individualized suspicion is required.⁶⁹ Second, the Court declares that the intrusions occasioned by the program will be relatively minimal (a brief stop at a roadblock) or will occur in an environment where expectations of privacy are already reduced (schools, the workplace).⁷⁰

In carrying out this analysis, the Court rarely specifies the significance of the

⁶⁷ See *id.* at 28. The exception would not, however, allow relaxation of justification requirements associated with investigating *past* crime; the intrusiveness associated with search of a house does not vary by the nature of the crime, just as the prosecution's burden of proof is not lessened simply because homicide is the charge. See Slobogin, *Proportionality, Privacy and Public Opinion*, at 1611-14, for elaboration of this argument.

⁶⁸ Much of this discussion is taken from Christopher Slobogin, *Government Dragnets*, 73 *J. of Law & Contemp. Probs.* (forthcoming, 2010).

⁶⁹ See discussion in *Edmond v. City of Indianapolis*, 531 U.S. 32, 37-40 (2000).

⁷⁰ See *Vernonia School District 47J v. Acton*, 515 U.S. 646, 654-57 (1995).

crime problem. And although, as discussed further below, the degree of intrusion may be somewhat mitigated by the group nature of the search or seizure, the Court's conclusion that this fact, by itself, justifies giving carte blanche to law enforcement is too facile. Programmatic investigations do raise special concerns, but they should not be exempt from the usual Fourth Amendment strictures simply because they are focused on "extraordinary" rather than ordinary crime or on groups rather than individuals.

A second, more judicially-oriented approach to the large-scale search and seizure scenario is to adapt the proportionality principle—the idea that the justification should be proportionate to the intrusion—to group settings. As the Court sometimes suggests, a group search may be less intrusive precisely because of its group nature. For instance, the studies cited earlier found that when the government is accessing thousands of records as it looks for the proverbial needle in the haystack, its investigative efforts are viewed as less intrusive than when the records are sought with a specific target in mind.⁷¹ Yet unless the intrusion is de minimis proportionality reasoning would still require some concrete justification for these blunderbuss intrusions, beyond the type of broad pronouncements about "law enforcement problems" on which the Court usually relies. More specifically, instead of looking for what the courts have called "individualized suspicion," proportionality analysis in the group context could require what might be called "generalized suspicion."⁷²

Generalized suspicion can be thought of as a measure of a program's success or "hit rate," which under proportionality analysis must match its intrusiveness. A requirement of generalized suspicion proportionate to the intrusion visited on individuals in the group would force the government to produce concrete justification for its search and seizure programs. For instance, in *Edmond v. Indianapolis*, a roadblock case, police searches produced evidence of drug crime in 5% of the cars stopped.⁷³ Whether that potential hit rate would be sufficient to justify the intrusion associated with a roadblock would depend on how that intrusion compares to other police actions, such as arrests, that require probable cause (which might require a hit rate of about 50%, given the similarity of probable cause to a more-likely-than-not standard), and field investigation stops, that require reasonable suspicion (which has been quantified at around 30%).⁷⁴ Assessment of hit rates might have to be speculative if a particular type of group search or seizure has never been attempted. But presumably a program instituted in good faith is motivated by the perception that a significant crime problem exists. In the absence of such facts (and assuming the danger exception does not apply) courts applying proportionality analysis would be leery of finding that a group

⁷¹ See Slobogin, *Privacy at Risk*, 191-92.

⁷² *Id.* at 40 (distinguishing generalized from individualized suspicion on the ground that the former is more explicitly based on profiles or statistical information).

⁷³ 531 U.S. at 450.

⁷⁴ See C.M.A. McCauliff, *Burdens of Proof: Degrees of Belief, Quanta of Evidence, or Constitutional Guarantees?* 35 *Vanderbilt L. Rev.* 1293, 1325 (1982) (summarizing a survey of judges)

investigation is justified.

The proportionality approach has at least two difficulties, however. As just mentioned, relevant hit rate information can be hard to come by. Second, proportionality analysis is unidimensional, in that it looks *only* at hit rates, not at the deterrent effects of the search and seizure program, alternative means of achieving the government's ends, and so on. In the individual investigative context, this unidimensionality is not problematic because programmatic concerns are irrelevant. But where group searches and seizures conducted pursuant to statutes or executive policies are involved, more depth of analysis is possible.

Thus, a third approach to regulation of group searches and seizures is to subject them to the type of judicial "strict scrutiny" analysis found in equal protection and First Amendment cases.⁷⁵ On the assumption that privacy from unwanted governmental intrusion is a fundamental right, the government could be required to show such programs not only advance a compelling state interest but also are the least drastic means of doing so. Under this approach, courts would be even more active than under proportionality analysis in determining whether group searches and seizures are the best means of fighting the crime problem.

Unfortunately, strict scrutiny analysis encounters the same difficulties as proportionality reasoning, only magnified. Fighting crime—whether it is terrorism, illegal immigration, or drug possession—is either always a compelling government need (the Court's assumption in its special needs analysis) or only compelling when a quantifiable problem in the relevant locale exists (the generalized suspicion inquiry). If courts adopt the latter approach to defining what is "compelling," as they probably should if they want to adhere to the spirit of strict scrutiny analysis, then the hit rate problem arises all over again. Regardless of how courts deal with this threshold issue, an even more confounding question, by a significant magnitude, is the remaining part of the strict scrutiny inquiry: whether a particular search and seizure program is necessary to achieve the government's interest. However competent courts may be at assessing, in First Amendment cases, whether time, place and manner restrictions on speech are necessary, they are sorely ill-equipped to analyze which law enforcement techniques work best.

Consider, for instance, how a court would apply strict scrutiny analysis to a public camera system. Assume that the area in which the government wants to set up cameras has a high crime rate and that research conducted in similar types of locations indicates that, through increased deterrence and apprehension, their presence can reduce property crime by as much as 25% and violent crime by as much as 5% (estimates based on the most optimistic studies).⁷⁶ In a proportionality regime, this information would be sufficient to allow the court to make its decision.

⁷⁵ See, e.g., Scott Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of Camara and Terry*, 72 *Minn. L. Rev.* 383 (1988).

⁷⁶ See Slobogin, *Privacy at Risk*, 84-88.

In a strict scrutiny regime, however, even if the court found the government's interest compelling it would still have to inquire into whether the camera system was narrowly tailored to meet the government's objective.

That inquiry raises a number of imponderables. Alternatives to a camera system could include placing more police on the scene (presumably limited to watching people only when they have individualized suspicion), installing more street lights and greater pedestrian access to the area, and passing broader loitering laws that would allow police greater preventive authority.⁷⁷ Comparing the effectiveness, not to mention the expense, of these competing approaches is far from the typical judicial job. And although assessing the relative intrusiveness of these various techniques *is* within the usual judicial purview, balancing that assessment with these other variables and figuring out which technique most efficaciously deals with the crime problem in the least restrictive manner raise micro-managing quandaries that most judges would find daunting and that, for both political and institutional reasons, are probably inappropriate for courts to address in any event.⁷⁸

That observation suggests a fourth approach to group searches and seizures, involving application of political process theory. As laid out by John Hart Ely, political process theory addresses the institutional tensions that arise when unelected judges review legislation enacted by popularly-elected bodies under vague constitutional provisions such as the Fourteenth Amendment's prohibition on deprivations of life, liberty and property "without due process of law."⁷⁹ In these situations, Ely argued, the appropriate division of labor should generally favor the legislature. Courts should strike down statutes passed by Congress or state representative bodies only if the legislative pronouncement is the result of a significant defect in the democratic process.

Ely did not focus on how this theory might apply to the amorphous reasonableness language of the Fourth Amendment. But Richard Worf has recently argued that it can apply in the latter context as well, at least where programmatic searches and seizures are involved. As Worf explains, "Where only groups are affected, very important, disputed questions can safely be left to the political process," because groups have access to that process.⁸⁰ Putting aside search and seizure programs that involve full-blown searches of house or arrests (situations which the colonists clearly believed required individualized probable

⁷⁷ Cf. Neal Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039, 1092-98 (2002) (exploring how city architecture might enhance crime control); *City of Chicago v. Morales*, 527 U.S. 41, 66 (1999) (O'Connor, J., concurring) (speaking of loitering statutes that might be "reasonable alternatives" to the loitering statute struck down by the majority).

⁷⁸ Cf. *Mich. Dep't State Police v. Sitz*, 496 U.S. 444, 453-54 (1990) ("for purposes of Fourth Amendment analysis, the choice among such reasonable alternatives remains with the governmental officials who have a unique understanding of, and a responsibility for, limited public resources, including a finite number of police officers.").

⁷⁹ John Hart Ely, *Democracy and Distrust: A Theory of Judicial Review* (1980).

⁸⁰ Richard C. Worf, *The Case for Rational Basis Review of General Suspicionless Searches and Seizures*, 23 *Touro L. Rev.* 93, 117 (2007). William Stuntz broached a similar idea back in 1992. William Stuntz, *Implicit Bargains, Government Power, and the Fourth Amendment*, 44 *Stan. L. Rev.* 553, 585-89 (1992).

cause⁸¹), this approach is worth considering. In theory at least, groups—such as those subjected to the TIA program or public camera surveillance—can protect themselves through the political process in ways that individuals cannot. If the authorizing legislation applies evenly to the entire group (including its legislative representatives), the full costs of the program are likely to be considered in enacting it. And, as already noted, evaluation of search and seizure programs requires analysis of deterrent effects, resource expenditures, and other complicated interdisciplinary matters that legislatures are much better than judges at addressing.

While it does counsel deference to legislatures, political process approach is not simply special needs analysis dressed up in fancy theory. As conceptualized by Ely, judicial deference would be mandated only if the search and seizure program is established pursuant to legislation (as opposed to executive fiat), adequately constrains the executive branch (by, for instance, instructing police to search everyone, or everyone who meets pre-defined criteria), and avoids discriminating against a discrete and insular minority or any other group that is not adequately represented in the legislature. Irrational search and seizure programs—those that have no articulable rationale—would also be unconstitutional. Most of the group search and seizures addressed by the Court to date do not meet these requirements. Many were not even the product of legislative action.⁸² And in most of the remaining special needs situations the Court has encountered, the authorizing legislation delegated too much power to executive branch law enforcement officials.⁸³

In individual search and seizure situations proportionality analysis works well. But in the group search setting a combination of proportionality analysis and political process theory may be the best solution. The Supreme Court's special needs doctrine should be jettisoned because it is too vacuous. Strict scrutiny analysis in the criminal law enforcement context is too dependent on judicial (in)ability to evaluate complicated law enforcement strategies. Instead, if a search and seizure program is authorized by legislation that is untainted by political process defects and is not irrational, courts should defer to it. If a process defect exists, the courts should apply proportionality reasoning using the generalized suspicion concept.

Consider how the foregoing framework would apply to a data mining program such as TIA. First, it would have to be authorized by the legislature. This

⁸¹ See generally, Daniel Steinberg, *Restoring the Fourth Amendment: Revisiting the Original Understanding*, 33 *Hastings Cont. L. Q.* 47 (2005) (arguing that the Fourth Amendment was meant to govern only searches of homes and arrests).

⁸² See, e.g., *Michigan Dept. of State Police v. Sitz*, 496 U.S. 444 (1990) and *Edmond*, where roadblocks policies were promulgated by the local police department, and *Treasury Employees v. Von Raab*, 489 U.S. 656 (1989), where the policies were developed by federal officials.

⁸³ See, e.g., *New York v. Burger*, 482 U.S. 691 (1987) (statute allowed police to enter junkyards at will); *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602 (1989) (statute simply directed the executive agency to promulgate rules); *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976) (where, after the initial stop, immigration agents determined who was to be sent to the secondary checkpoint).

requirement would immediately disqualify TIA as a candidate for judicial deference, because it was the product of Admiral Poindexter's imagination and the executive branch, not Congress.⁸⁴ Assuming Congress were persuaded to establish such a program, careful attention would still have to be paid to whether it circumscribed executive discretion by, for instance, requiring that the records of everyone, including members of Congress, be collected or by requiring a random records-selection process (say, every fifth record). As Justice Jackson stated years ago, "There is no more effective practical guaranty against arbitrary and unreasonable government than to require that the principles of law which officials would impose upon a minority must be imposed generally."⁸⁵ A failure to follow this injunction, or a program that targeted an insular minority such as people of middle-eastern descent, would subject the program to further judicial review.

If a court determined that sufficient discretion-limiting features were not present in the legislation, it would have to ascertain, under proportionality reasoning, whether the potential hit rate of the data mining program justified the degree of intrusion involved. Assuming, as apparently was the case, that the TIA program contemplated obtaining and scrutinizing records describing financial information, credit card purchases, and phone and Internet contacts, a relatively high hit rate would be necessary. The required showing could only be reduced if human scrutiny were minimized through use of profiling technology⁸⁶ or, consistent with the danger exception described earlier, a significant, imminent threat existed.

Conclusion


Virtual searches are rapidly replacing physical searches of homes, cars and luggage. Outdoor activities and many indoor ones as well can be caught on camera, monitored using tracking devices or documented using computers. Yet none of this technological surveillance can be challenged under the Fourth Amendment if its target could conceivably be viewed, with the naked eye or with common technology, by a member of the public, or could be detected using a contraband-specific device, or has been voluntarily surrendered to a human or institutional third party. And even those technological investigations that are considered "searches" will usually survive Fourth Amendment challenge, if they can be characterized as preventive or intelligence-gathering exercises rather than efforts to solve ordinary crime.

It is time to revert back to first principles. A search involves looking for something. Justification for a search should be proportionate to its intrusiveness

⁸⁴ John Markoff, Pentagon Plans a Computer System that would Peek at Personal Data of Americans, N.Y. Times (Nov. 9, 2002) at A1, available at <http://www.nytimes.com/2002/11/09/politics/09COMP.html>.

⁸⁵ *Railway Express Agency, Inc. v. New York*, 336 U.S. 106, 112-113 (1949) (Jackson, J., concurring).

⁸⁶ A process known as "selective revelation," which allows humans to see records only after a computer applies a profile that generates the appropriate hit rate, might be useful here. See K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 Colum. Sci. & Tech. L. Rev. 2, 79-80 (2003).



except in the rare circumstances when the search is part of a large-scale program authorized by legislation that avoids political process defects or is aimed at preventing specific, imminent and significant danger. These principles will restore the Fourth Amendment to its place as the primary arbiter of how government investigates its citizens, even when those investigations rely on technology that can be used covertly and from a distance.

Christopher Slobogin has authored more than 100 articles, books and chapters on topics relating to criminal procedure, mental health law and evidence. Director of Vanderbilt Law School's Criminal Justice Program, he is one of the 10 most cited criminal law and procedure law professors in the nation, according to the Leiter Report. The book *Psychological Evaluations for the Courts*, which he co-authors with another lawyer and two psychologists, is considered the standard-bearer in forensic mental health; in recognition for his work in that field, he was named an Honorary Distinguished Member of the American Psychology-Law Society in 2008. Professor Slobogin has also served as reporter for the American Bar Association's Task Force on Law Enforcement and Technology and its Task Force on the Insanity Defense, and chair of the Florida Assessment Team for the ABA's Death Penalty Moratorium Implementation Project. In addition, he helped draft standards dealing with mental disability and the death penalty that have been adopted by the ABA, the American Psychiatric Association and the American Psychological Association. Professor Slobogin joined Vanderbilt's faculty in 2008, having previously held the Stephen C. O'Connell chair at the University of Florida's Levin College of Law. Over the course of his career, he has been a visiting professor at Stanford Law School, where he was the Edwin A. Heafey Visiting Scholar, as well as at the Universities of Virginia, Nebraska, Southern California and California – Hastings. He has also taught at the University of Frankfurt Law School in Germany and the University of Kiev, Ukraine, where he was a Fulbright Scholar. He has appeared on *Good Morning America*, *Nightline*, the *Today Show*, National Public Radio, and many other media outlets, and has been cited in over 1,800 law review articles and over 100 judicial opinions, including at the Supreme Court level. Professor Slobogin has a secondary appointment as Professor in the Vanderbilt University School of Medicine's Department of Psychiatry.

Governance Studies

The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

Editor

Jeffrey Rosen
Benjamin Wittes

Production & Layout

John S Seo

**E-mail your comments to
gscments@brookings.edu**

This paper is distributed in the expectation that it may elicit useful comments and is subject to subsequent revision. The views expressed in this piece are those of the author and should not be attributed to the staff, officers or trustees of the Brookings Institution.