THE NEW REALITY OF SEARCH ANALYSIS: FOUR TRENDS CREATED BY NEW SURVEILLANCE TECHNOLOGIES

Ric Simmons[*]

INTRODUCTION

The Fourth Amendment was drafted and ratified in a radically different world than that in which we live today. The political, social, and economic realities of the late eighteenth century created different concerns than those we face in the early twenty-first century. But, the most important changes we have seen over the past two hundred years—and the most important changes which will affect search analysis in the near future—are scientific in nature: new technologies which have revolutionized both how individuals commit crime and how law enforcement investigates it.

The primary way new technologies have altered the landscape of search analysis is by enabling law enforcement

* Professor of Law, Moritz College of Law, The Ohio State University. Funding for this work was underwritten by the National Center for Justice and the Rule of Law at the University of Mississippi School of Law, which is supported by a Grant awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position of the United States Department of Justice.

officials to conduct surveillance in new, often more intrusive, ways. As law enforcement officials employ these new technologies, courts must apply the Fourth Amendment to determine whether the new kind of surveillance constitutes a "search" at all and, if so, what showing the government must make in order to legally conduct the search. In cases involving electronic eavesdropping,[1] thermal imagers,[2] and hidden video cameras,[3] the courts have had to decide how the Fourth Amendment limits law enforcement's power in new ways that the Framers never imagined.

But, there is also another, more subtle way in which new technologies have influenced Fourth Amendment jurisprudence—they have enabled criminals to commit new types of crimes or commit traditional crimes in new ways that are much more difficult to detect and prevent. A child pornographer who wanted to distribute his goods was previously limited by very tangible, practical constraints regarding the number of pictures he could distribute and the number of people to whom he could distribute them; today, computers and e-mail make such limits obsolete. A teenage vandal in past eras might break store windows or spray-paint graffiti on walls; today, the same teenager might write a computer virus and cause millions of dollars worth of damage. An anarchist in the nineteenth century might seek to assassinate a president or plant dynamite in an opera house; his twenty-first century counterpart is able to destroy cities with nuclear weapons or poison an entire society with chemical or biological agents. Criminals now utilize encryption and cell phones to further their ends and hide deadly explosives in small backpacks or suitcases. Law enforcement, understandably, has engaged in aggressive counter-measures to prevent these crimes and apprehend the criminals who commit them. They have invaded suspects' computers to record their keystrokes,[4] they have read e-mails stored on remote servers,[5] and they have indiscriminately searched passengers on planes[6] and subway trains.[7]

---

[1] *See* Katz v. United States, 389 U.S. 347 (1967).
[2] *See* Kyllo v. United States, 533 U.S. 27 (2001).
[3] *See* United States v. Torres, 751 F.2d 875 (7th Cir. 1984).
[4] *See* United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).
[5] *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
[6] *See* United States v. Edwards, 498 F.2d 496 (2d Cir. 1974).
[7] *See* MacWade v. Kelly, 460 F.3d 260 (2d Cir. 2006).

These twin effects of technology have dramatically impacted search analysis. This Article will examine four interconnected ways new technologies have affected how courts analyze government searches: the tendency of Congress to supplement the Fourth Amendment with legislation, the shift from a "binary" approach to a "spectrum" approach in categorizing surveillance methods, a heightened deference to the legislature and to the executive with regard to new surveillance technologies, and a troubling tendency of courts to misunderstand new surveillance technology and thereby create overly formalist tests. This last phenomenon occasionally leads Congress to step into the area to correct the mistake, thus beginning the cycle anew.

The first trend stems directly from the rapid pace of technological advancement and the mistakes courts make when they try to regulate these new technologies. These mistakes have encouraged Congress to step in and create its own rules regulating law enforcement's use of technology or curtailing the use of technology by criminals. Thus, most judges conducting a modern day search analysis must go beyond the text and jurisprudence of the Fourth Amendment and its associated jurisprudence; they must also interpret one (or more) of a dozen or so federal provisions limiting the use of technology by law enforcement, from the Federal Communications Act of 1934[8] through the USA PATRIOT Act of 2001.[9] And although these statutory provisions are theoretically secondary to the protections of the Fourth Amendment, they have also had a feedback effect on how courts interpret the Fourth Amendment.

The second trend has been a shift away from a "binary" approach, in which the court's only job was to decide whether a certain type of surveillance is or is not a search, to a "spectrum" approach, in which a court must determine the level of invasiveness of the search in order to choose the appropriate restrictions to impose on the search. This trend famously began in 1968 with *Terry v. Ohio*, when the Supreme Court held that a pat-down is not a "search" but nevertheless implicates the Fourth Amendment.[10] This created a new category of surveillance ("*Terry*

---

[8] *See* 47 U.S.C. § 605 (2006).

[9] *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[10] 392 U.S. 1, 30-31 (1968).

stops") and a new standard for evaluating surveillance in this category (reasonable suspicion). Congressional interference in surveillance regulation has accelerated this trend substantially, adding more layers to the spectrum.

Congressional interference has also accelerated the third trend. Because so many statutes now regulate surveillance methods, courts are far more likely than they were in the past to defer to Congress in analyzing surveillance techniques. In fact, as we will see, courts have even adopted statutory standards and imported them into their Fourth Amendment jurisprudence, effectively allowing Congress to interpret the contours of the Fourth Amendment. But, courts are not only showing greater deference to the legislative branch; they have also become more deferential to law enforcement as well. Since new technology enables criminals to hide their activities more effectively—and cause more damage when they succeed in those activities—courts are more likely to defer to law enforcement officers when they employ more aggressive tactics to detect these criminals.

Finally, new surveillance technology has occasionally created confusion among judges, thus further complicating the jurisprudence of search analysis. In such cases, courts have resorted to overly formalist doctrines that fail to reflect the reality of how the technologies actually work. Frequently, these doctrines persist for decades before the courts correct them—as was the case in *Olmstead v. United States*,[11] which created a "property-based" concept of search analysis that persevered for forty years before it was overruled by *Katz v. United States*.[12] The most blatant existing example of this formalism—the third-party consent doctrine of *Smith v. Maryland*[13]—is only now being challenged by courts, over thirty years after its birth.

Luckily, the damage done by such formalist doctrines has been limited because the courts' most blatant mistakes have been corrected by Congress. In this sense, congressional interference may be seen as a positive development, or at the very least, as inevitable. The following Section examines the ways in which

---

[11] 277 U.S. 438, 466 (1928).

[12] 389 U.S. 347, 353 (1967).

[13] 442 U.S. 735 (1979); *see infra* notes 74-78 and accompanying text.

Congress has delved into the regulation of surveillance technology.

I. THE RISE OF CONGRESS

Historically, the Fourth Amendment, as interpreted by the courts, has acted as the primary restriction on the government's authority to search its citizens. A generation ago, scholars studying search and seizure could safely ignore statutes, and judges rarely went beyond Fourth Amendment jurisprudence in deciding search and seizure cases. Today, however, anyone who wants to understand search analysis in the context of new surveillance technologies must be familiar with the numerous statutes now dominating the field.

The first major foray by Congress into regulating government surveillance came in 1934. Predictably, the legislation came in response to a new technology the Supreme Court failed to understand and, thus, failed to regulate properly—the telephone. In the 1928 case of *Olmstead v. United States*, the Supreme Court held that the government did not conduct a "search" under the Fourth Amendment when it wiretapped a telephone.[14] The Court's reasoning betrayed its lack of understanding of how this new communications technology interacted with basic privacy rights. As a result of this misunderstanding, the Court resorted to a simplistic formalism to reach a disastrous conclusion: "The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment."[15]

This infamous "property-based" test for determining whether a search occurred remained in use until overturned by *Katz* forty years later.[16] In Part IV, we will see how new surveillance technologies frequently lead to this kind of formalism,[17] which may take decades to correct. With regard to the specific case of telephone wiretapping, Congress decided it could not wait for the

---

[14] 277 U.S. 438, 466 (1928).

[15] *Id.*

[16] *Katz*, 389 U.S. at 353.

[17] *See infra* note 71 and accompanying text.

courts to fix the mistake, and so the legislature stepped in to protect an individual's privacy interests by passing the Federal Communications Act of 1934, which prohibited intercepting and disclosing any information that passes over telephone lines.[18]

Since 1934, congressional intervention into surveillance regulation has grown exponentially, accelerating in recent decades. Among the more prominent examples are: Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III),[19] which regulates oral and wire communications; the 1986 Electronic Communications Privacy Act (ECPA),[20] which extends Title III to electronic communications; the Stored Communications Act (SCA),[21] which was part of ECPA and regulates government access to stored wire and electronic communications held by third-party internet service providers (ISPs); the Foreign Intelligence Surveillance Act of 1978 (FISA),[22] which sets out rules for electronic surveillance of agents of foreign powers; and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act),[23] which, among other effects, broadens the type of surveillance allowed under FISA and the ECPA.

In some ways, the relationship between the courts and the legislature in this context is typical: the legislature creates a statute, and the courts evaluate it in light of the Fourth Amendment and occasionally strike down the statute as unconstitutional. This was the process that occurred in the late 1960s—New York State passed a law regulating wiretapping,[24] and the Supreme Court, in *Berger v. New York*,[25] overturned the

---

[18] *See* 47 U.S.C. § 605 (2006).

[19] *See* 18 U.S.C. §§ 2516-2518 (2006).

[20] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[21] *See* Stored Wire and Electronic Communications and Transactional Records Access, ch. 121, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2701-2712 (2006)).

[22] *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978).

[23] USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[24] N.Y. CRIM. PROC. § 813-a (McKinney 1958), *overturned by* Berger v. New York, 388 U.S. 41 (1967).

[25] 388 U.S. 41 (1967).

law as inconsistent with the Fourth Amendment.[26] Congress responded in 1968 with Title III, which provides stronger protections than the New York statute had created. Similarly, the PATRIOT Act of 2001 amended FISA to allow "sneak and peek" warrants—search warrants, which could be exercised before notification was given to the suspect—if a "significant purpose" (rather than a "primary purpose") of the search was gathering foreign intelligence.[27] In 2007, a federal judge struck down this provision as inconsistent with the Fourth Amendment,[28] though her decision was later overturned on procedural grounds.[29]

But, this traditional relationship between courts and the legislature is not the whole story. In the context of regulating new surveillance technologies, the relationship between the courts and the legislature is a bit more complicated. Legislatures frequently create protections above and beyond what the Fourth Amendment requires—which leads to problems when citizens rely on these protections as though they are constitutionally protected, only to find them repealed by later statutes.

An example of this phenomenon can be found in the laws regulating wiretapping. Under Title III, law enforcement is required to show more than mere "probable cause" before conducting this type of surveillance. Instead, it must meet a much higher standard, including demonstrating that normal investigative procedures are inadequate[30] and that the surveillance will be conducted in a way that minimizes the interception of irrelevant communication.[31] These Title III requirements have never been reviewed by the Supreme Court, but they have been unanimously approved by the appellate courts

---

[26] *Id.* at 43, 64.

[27] 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B) (Supp. 2011).

[28] Mayfield v. United States, 504 F. Supp. 2d 1023, 1032, 1042-43 (D. Or. 2007), *vacated on other grounds by* Mayfield v. United States, 599 F.3d 964, 973 (9th Cir. 2010).

[29] *Mayfield*, 599 F.3d at 973.

[30] 18 U.S.C. § 2518(3)(c) (2006).

[31] 18 U.S.C. § 2518(5) (2006). Title III also limits the use of wiretapping to investigations of certain enumerated crimes, requires authorization by a high-level Justice Department official, and limits the duration of the order to thirty days (with the possibility of an extension). 18 U.S.C. §§ 2518(3)(a), 2516(1), 2518(5) (2006).

as *sufficient* to satisfy the Fourth Amendment.[32] Thus, it remains unknown whether they are *required* in order to satisfy the Fourth Amendment. As a result, when political tides shifted in the wake of the September 11th attacks, Congress felt free to relax some of the requirements of Title III.[33] Many were outraged by these changes,[34] partly because of the presumption that protections against unreasonable searches and seizures are based on the Constitution and, thus, insulated from the political whims of Congress. But, as Congress intervenes more and more often to regulate surveillance, we need to adjust to a new paradigm—one in which the balance that is struck between the needs of law enforcement and the privacy rights of individuals is constantly updated according to the prevailing political mood.

In theory, the Fourth Amendment still provides a baseline minimum of privacy, protected by the courts. In practice, however, a more subtle shift is occurring—as Congress becomes more and more involved in this field, the Supreme Court is showing more and more deference to congressional rules about the appropriate level of regulation. This increased deference is discussed in Part III of this Article.[35]

Scholars are currently engaged in a debate as to whether the increase in congressional involvement is a positive or a negative trend. Proponents of judicial supremacy in this realm, such as Lawrence Lessig, have argued that courts must apply consistent constitutional values to all types of surveillance, whether or not the surveillance involves new technologies.[36] Professor Orin Kerr has taken the opposite view, arguing that the legislature is better

---

[32] *See, e.g.*, United States v. Tortorello, 480 F.2d 764, 774-75 (2d Cir. 1973); United States v. Cafero, 473 F.2d 489, 501 (3d Cir. 1973); United States v. Cox, 462 F.2d 1293, 1304 (8th Cir. 1972); United States v. Cox, 449 F.2d 679, 687 (10th Cir. 1971).

[33] The PATRIOT Act, for example, allowed wiretapping under much lower FISA standards as long as the "significant" purpose of the surveillance was counterintelligence, rather than the "sole" purpose. *See* USA PATRIOT Act, tit. 2, § 218, 115 Stat. 272, 291 (2001). The Protect America Act of 2007 allowed warrantless wiretapping of United States citizens if the call began or ended in a foreign country. *See* Pub. L. No. 110-55, § 2, 121 Stat. 552, 553-55 (2007) (codified as amended at 50 U.S.C. § 1805 (2006)).

[34] *See, e.g.*, *ACLU Response to the Protect America Act of 2007*, ACLU (Aug. 7, 2007), http://www.aclu.org/national-security/aclu-fact-sheet-%E2%80%9Cpolice-america-act.

[35] *See infra* notes 56-64 and accompanying text.

[36] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 216 (1999).

equipped to determine the proper balance between the needs of law enforcement and the privacy rights of individuals.[37] But regardless of whether this is a desirable trend, it seems certain to continue or even accelerate in the future; meaning that scholars, judges, and law enforcement officers must be well-versed in both Fourth Amendment jurisprudence and the myriad of congressional provisions that regulate high-tech surveillance.

II. FROM A BINARY ANALYSIS TO A SPECTRUM OF STANDARDS

The increase in congressional involvement in regulating surveillance of new technologies has accelerated another important trend in this field: the shift from a binary analysis, in which courts would simply decide whether or not a "search" has occurred, to an ever-expanding spectrum of choices, in which courts (or legislatures) must determine the level of invasiveness of the surveillance and then determine what requirements law enforcement must meet in order to conduct the surveillance. Only a few decades ago, there was only one question courts had to answer: did the surveillance implicate the Fourth Amendment? If so, a warrant (supported by probable cause) was required. If not, the surveillance was completely unregulated by law.

Perhaps the most famous recent Fourth Amendment case concerning new technologies involved such a binary analysis. In *Kyllo v. United States*,[38] the Supreme Court decided whether law enforcement officers conducted a "search" when they used a thermal imager to detect telltale signs of heat lamps used to grow marijuana inside a house.[39] But *Kyllo*, and the analysis that the Court conducted to decide the case, are now the exception in surveillance regulation. In most modern cases, especially those involving new technologies, courts may decide that the surveillance implicates the Fourth Amendment but not to the

---

[37] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 864-82 (2004). Kerr notes that technological change advances quite rapidly, and legislatures, not courts, are in the best position to respond to this rapid change, since they (1) can make policy decisions before cases and controversies arise, rather than being reactive; (2) can change statutory regulation much more quickly than courts can change doctrine; and (3) have access to broad inputs of information not available to courts. *Id.*

[38] 533 U.S. 27 (2001).

[39] *Id.* at 29-30.

degree that probable cause is required—or perhaps to such a great degree that something *more* than probable cause is required. And, as we have seen in the previous Section, the surveillance may not implicate the Fourth Amendment, but it may be regulated by any number of statutes, which set out a variety of different standards for law enforcement to satisfy.

To be sure, neither Congress nor new surveillance technologies began this trend. The first real break from the binary analysis was in *Terry v. Ohio*,[40] in which the Supreme Court famously held that "a rigid all-or-nothing model of justification and regulation under the [Fourth] Amendment" was inadequate.[41] Instead, the Court took a broader view of "reasonableness" and applied the concept not merely to determine whether a search occurred, but also to conduct a balancing test between the intrusiveness of the search and the needs of law enforcement.[42] The result was a new standard: reasonable suspicion that "criminal activity may be afoot and that the persons with whom he is dealing may be armed and presently dangerous."[43] Other deviations from the binary analysis can also be found outside the context of new technologies, such as no-knock search warrants[44] and bodily intrusions,[45] both of which require a stronger showing than mere probable cause.

But, it is the context of new technologies—both those used by suspects and those used by investigators—which has provided the most frequent source of new standards for surveillance analysis. We have already seen that wiretapping and video surveillance are only permissible if law enforcement can satisfy the rigorous requirements of Title III—either because Title III directly applies (as in wiretapping) or because the courts have imported the high standards of Title III into constitutional law (as in video surveillance). Taken with the *Terry* doctrine, the Title III requirements result in four different "levels" of surveillance: those which are unregulated by the Fourth Amendment (such as

---

[40] 392 U.S. 1 (1968).
[41] *Id.* at 17.
[42] *Id.* at 19-20.
[43] *Id.* at 30.
[44] Wilson v. Arkansas, 514 U.S. 927, 934 (1995).
[45] Winston v. Lee, 470 U.S. 753, 759 (1985).

surveillance from an aircraft[46]); those which require reasonable suspicion (such as a *Terry* stop); those which require probable cause and a warrant (such as a standard search of a home); and those which must meet the Title III requirements (such as covert video surveillance).

As noted in the above section, Congress has stepped in to add many more "levels" of searches. When law enforcement is seeking "address" information, such as the phone numbers dialed by a suspect or the "from" line of an e-mail, the investigator must only demonstrate "certified relevance,"[47] and the judicial role in reviewing this standard is "ministerial in nature."[48] If law enforcement is seeking "historic information" (such as subscriber records in an online database, or a stored e-mail which has already been opened by the recipient), the investigator must show "specific and articulable facts."[49] However, if the e-mail has not yet been opened, a warrant is required,[50] and if the e-mail is captured "in transit" as it is being sent, then it is considered "electronic communication" and a Title III warrant is required.[51] To further complicate the matter, new congressional acts can change the standards required for any particular kind of search, as we saw in the previous Section when the PATRIOT Act modified the rule for wiretapping telephone calls if a "significant purpose" of the surveillance was counter-intelligence.[52]

This shift raises two interesting questions. The first question is whether this "sliding scale" of surveillance regulation is an improvement on either the binary analysis of the past or the tertiary analysis that existed post-*Terry*. Certainly the new regime may be problematic for law enforcement officers who have to decode and memorize an ever-increasing number of standards and digest even more case law surrounding the standards. Fourth Amendment jurisprudence was already challenging enough when police officers on the street seeking to search a car or an

---

[46] *See* California v. Ciraolo, 476 U.S. 207 (1986).

[47] 18 U.S.C. § 3122(b)(2) (2006). This was a provision of the 1986 ECPA.

[48] United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995).

[49] 18 U.S.C. §§ 2701-2712 (2006). These were provisions of the Stored Communication Act ("SCA"), another aspect of the 1986 ECPA.

[50] *Id.*

[51] 18 U.S.C. § 2518 (2006).

[52] *See* USA PATRIOT Act of 2001, tit. 2, § 218, 115 Stat. 272, 291 (2001).

individual had to comply with shifting standards of "reasonableness" to determine whether their actions were legal. Now, law enforcement officers who conduct electronic surveillance must learn even more law in order to ensure they are in compliance. Granted, the nature of electronic surveillance means that these decisions do not have to be made in the split-second pressures of most street encounters, but we ought to be aware that by shifting to a spectrum analysis, we are asking for a significant amount of legal expertise on the part of law enforcement officials. In other words, a tension exists between drafting the most precise rule for each situation and creating rules that are simple enough for law enforcement to apply properly and consistently.

Another concern is the effect the sliding scale has on privacy rights. Some would argue that a spectrum of different standards actually increases privacy rights because courts (and legislatures) that would be reluctant to require a full-blown warrant might be willing to regulate lower-level forms of surveillance with weaker standards. For example, Congress may not think it wise to require a law enforcement officer to obtain a warrant before she can subpoena the telephone numbers for all incoming and outgoing calls on a specific line; so if there were no lower standard available, the law enforcement officer would be able to acquire this information with no regulation whatsoever. And on the other end of the spectrum, privacy rights are certainly enhanced by requiring more intrusive searches to be regulated more tightly than a standard search of a residence.

Once the standards of probable cause and warrant get watered down, however, there is the danger of a slippery slope—more and more types of searches may be "downgraded" to an easier standard—especially as Congress begins to assert more dominance in this field. And the requirements on the lower end of this spectrum are not very impressive—a requirement of "certified relevance" or "specific and articulable facts" will not do much to protect an individual's privacy rights if law enforcement is determined to obtain the information.

The second question surrounding the shift to a spectrum analysis concerns the logical consistency of the different standards on the sliding scale. As Professor Christopher Slobogin pointed out in a recent book, the Supreme Court has not created a consistent

framework for this new spectrum of standards, nor has it explained the direct relationship between the intrusiveness of the surveillance and the standard the government must meet to conduct the surveillance.[53] And certainly, Congress has not made an effort to create such a framework; it adds on new standards for different types of searches without any need to explain how the many different standards fit together.

Professor Slobogin proposes a "proportionality principle" to deal with this question in which courts (and presumably legislatures) would assess the invasiveness of the surveillance and the needs of law enforcement before setting standards accordingly.[54] The problem with this approach is how to determine the level of "invasiveness" of each type of surveillance.[55] Are we meant to look to society's perceptions of privacy? If so, does that mean the sliding scale would need to be adjusted as perceptions of privacy change? In today's world, notions of privacy are changing rapidly as information becomes more and more accessible. Individuals put an unprecedented amount of private information into the public arena—both intentionally and unintentionally. Many individuals choose to use new technologies to make their private lives more public. Diaries, which were once kept hidden under mattresses, are now posted on blogs, along with personal pictures and messages from friends. Telephone conversations that used to occur in homes or private phone booths are now carried out on the street and in malls, stores, and other public areas.

On the other side of the balance of proportionality, how do we evaluate the needs of law enforcement? In many ways, technology has actually *increased* our ability to keep things secret from the

---

[53] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 38 (2007).

[54] *Id.* at 31. Slobogin proposes five different levels of standards: (1) no regulation at all, (2) "relevance" (which translates roughly to a 5% chance criminal activity will be detected), (3) "reasonable suspicion (30% chance), (4) probably cause (50%), and (5) clear and convincing (75%). *Id.* at 38-41.

[55] To be fair, this is a problem inherent in any attempt to impose an overarching framework on the spectrum of surveillance types. Slobogin himself acknowledges some critics say his proposal "would convert the Fourth Amendment 'into one immense Rorschach blot.'" *Id.* at 46 (quoting Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 393 (1974)). Amsterdam also called the proportionality principle "splendid in its flexibility [but] awful in its unintelligibility, unadministrability, unenforcibility and general ooziness." Amsterdam, *supra*, at 415.

government. Take two simple examples: data storage and communications. Only 150 years ago, a diary writer or record keeper had very limited options as to how to secretly record and store his writings. In modern times, the diary or records could be written on a laptop computer, accessible only by someone with the password or stored on a hard drive the size of a pen and hidden almost anywhere. The same analysis holds true for the confidentiality of communication. Two hundred years ago, a person who wished to communicate with someone else had to either travel to their house in person or send a letter with the address of the letter visible for all to see and the contents accessible by merely ripping open the envelope. Modern communications involve cell phones, e-mails, and encrypted information—all of which require sophisticated technical equipment to intercept and decode. Meanwhile, the Internet allows individuals to stay in the privacy of their own homes to conduct many activities which formerly had to be done in public: shopping, searching for information, downloading pictures and movies, and so on. Only twenty years ago, almost any of these tasks required the average person to leave her home and publically visit any number of businesses, which would have subjected the person to easy (and unregulated) surveillance by law enforcement.

Thus, what at first seem to be insidious new methods of eavesdropping and snooping—wiretapping phones, monitoring e-mails, searching computer hard drives—are simply remedial measures on the part of the government in an attempt to maintain the appropriate balance between individual privacy and effective law enforcement. In other words, privacy-enhancing technology has arguably increased (and will continue to increase) the justification for law enforcement surveillance.

These concerns are still problematic in a one-size-fits-all binary analysis, but to a much smaller degree. Most types of surveillance are either clearly "searches" requiring warrants or are not, and, therefore, not subject to regulation. Under such a simplified regime, evolutions of technology only rarely—as in the *Kyllo* case—bring new challenges. In short, the new (and expanding) spectrum of surveillance standards brings us better precision, but it is vulnerable to confusing ambiguity, especially as

societal perceptions of privacy change and privacy-enhancing technology increases the justification for invasive surveillance.

III. INCREASED DEFERENCE

A third trend in the regulation of new surveillance technology—one which also has been accelerated by the increased activity of Congress in this area—is the greater level of deference courts give to Congress and to law enforcement. We have already seen Congress enact numerous statutes to regulate new surveillance technologies, in some cases replacing the Fourth Amendment as the primary source of protection against invasive searches. This increased involvement leads courts to defer to Congress in two ways: first, courts are increasingly likely to stand back and wait for Congress to act when new surveillance technologies arise; and second, when courts do act, they occasionally borrow Congress's own regulatory scheme in interpreting the Fourth Amendment.

An example of the first type of deference to Congress can be found in the regulation of wiretapping, an area where Congress has been especially active. As the Fourth Amendment scholar Orin Kerr has argued, "the existence of the statutory Wiretap Act effectively displaces any constitutional remedies that in theory should exist under cases like *Katz* and *Berger*."[56] Kerr gives the example of the wiretapping of cordless phone calls. Congress originally did not extend Title III protection to these calls, creating a significant gap in the law, since "conversations on land-line phones were protected by the Wiretap Act while conversations on cordless phones were not."[57] An active judiciary that was aggressively enforcing a minimum level of privacy rights that was guaranteed by the Fourth Amendment would have closed this gap, but the courts refused to do so.[58] Instead, the Fourth Circuit warned against "wield[ing] the amorphous 'reasonable expectation of privacy' standard in a manner that nullifies the balance . . . struck by Congress in Title III"[59] and affirmed that "the primary

---

[56] Kerr, *supra* note 37, at 853.

[57] *Id.* at 852.

[58] *Id.*

[59] United States v. McNulty (*In re* Askin), 47 F.3d 100, 105-06 (4th Cir. 1995) (citation omitted).

job of evaluating [new technologies'] impact on privacy rights and of updating the law must remain with . . . the legislature."[60] This and other examples led Kerr to conclude that "wiretapping law may be constitutional in theory, but it is statutory in practice."[61]

A more dramatic instance of courts' deference to Congress occurred when courts sought to define the scope of constitutional parameters for covert video surveillance. As in the case of cordless phones, Congress failed to act in this area, since Title III explicitly excludes video surveillance from its purview.[62] But this time, instead of waiting for Congress to act, the courts showed even greater deference to Congress by holding that the Fourth Amendment protections for video surveillance were *identical* to the statutory requirements already set out by Congress for wiretapping. In *United States v. Torres*, the Seventh Circuit explained that it was "borrow[ing] the warrant procedure of Title III, a careful legislative attempt to solve a very similar problem, and hold[ing] that it provides the measure of the government's constitutional obligation of particular description in using television surveillance to investigate crime."[63] Since *Torres*, six other federal circuits have used the Title III safeguards to define the scope of the Fourth Amendment warrant requirement in the context of video surveillance.[64]

In short, when facing a clear gap in the surveillance regulations created by statute, the courts have responded in one of two ways: either by doing nothing, assuming that the Fourth Amendment does not apply in the context at all; or, if the gap is so blatant, that the Fourth Amendment *must* apply by simply borrowing the standards crafted by Congress in a different context and elevating them to the constitutional level.

---

[60] *Id.* at 106. Congress did indeed pass legislation extending Title III protection to cordless phones in 1994. *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 202, 108 Stat. 4279, 4290-91 (1994).

[61] Kerr, *supra* note 37, at 855.

[62] *See* United States v. Torres, 751 F.2d 875, 886 (7th Cir. 1984).

[63] *Id.* at 885.

[64] *See* United States v. Williams, 124 F.3d 411, 416 (3d Cir. 1997); United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992), *cert. denied*, 506 U.S. 1005 (1992); United States v. Mesa-Rincon, 911 F.2d 1433, 1437 (10th Cir. 1990); United States v. Cuevas-Sanchez, 821 F.2d 248, 252 (5th Cir. 1987); United States v. Biasucci, 786 F.2d 504, 510 (2d Cir. 1986), *cert. denied*, 479 U.S. 827 (1986).

Courts have also shown signs of deferring to law enforcement when considering the constitutionality of a new type of surveillance, especially if the government claims to be "responding" to new technologies being used by criminals. As noted above, new technology not only allows law enforcement to conduct more intrusive levels of surveillance, but it also allows criminals to hide their activities more effectively from law enforcement and to cause more damage as a result of their criminal activity. In these cases—when the government is reacting to new crimes or techniques employed by criminals—some courts have interpreted the Fourth Amendment narrowly, deferring to law enforcement regarding what is necessary to maintain public safety or counter a particular form of criminal activity.

Part of this deference stems from a legitimate desire to allow law enforcement to keep pace with criminals in the technological arms race that occurs between police and criminals. For example, criminals are increasingly using advanced cryptography on their communications and data storage. In order to combat this encryption in one case, FBI agents acquired a warrant and installed software on a suspect's computer that recorded the keystrokes as they were being typed, thus intercepting the suspect's password as he typed it.[65] The defendant moved to suppress the evidence that was found on the grounds that the FBI was actually intercepting a "wire communication" in transit, and therefore, a Title III order—not a mere warrant—was required.[66] The court rejected the defendant's argument and then gave this rather extraordinary explanation:

> In this day and age, it appears that on a daily basis we are overwhelmed with new and exciting, technologically-advanced gadgetry. Indeed, the amazing capabilities bestowed upon us by science are at times mind-boggling. As a result, we must be ever vigilant against the evisceration of Constitutional rights at the hands of modern technology. Yet, at the same time, it is likewise true that modern-day criminals have also embraced technological advances and used them to further their

---

[65] United States v. Scarfo, 180 F. Supp. 2d 572, 574 (D.N.J. 2001).

[66] *Id.* at 581-82.

> felonious purposes. Each day, advanced computer technologies and the increased accessibility to the Internet means criminal behavior is becoming more sophisticated and complex. This includes the ability to find new ways to commit old crimes, as well as new crimes beyond the comprehension of courts. As a result of this surge in so-called "cyber crime," law enforcement's ability to vigorously pursue such rogues cannot be hindered where all Constitutional limitations are scrupulously observed.[67]

Unfortunately, this doctrine of deferring to law enforcement officers when they are pursuing criminals who are "find[ing] new ways to commit old crimes" is ultimately unworkable. The problem is that there is no meaningful way to define when a criminal is using a "new" technology to commit or conceal his crime. As noted earlier, telephone communications could be considered a "new way" to commit a crime—and perhaps that was one of the unspoken reasons why the *Olmstead* Court deferred to law enforcement's warrantless tapping of the phones in 1928. But, it would not make sense to give law enforcement extra deference regarding telephone wiretapping merely because they are countering a new technology being used by criminals. Rather, the opposite is true: because of the intrusive nature of the surveillance, telephone wiretapping undoubtedly deserves the higher standard Title III has created for it. Likewise, *Kyllo* could be considered a "responsive" use of technology by law enforcement, since the defendant was using heat lamps to grow marijuana indoors rather than the traditional method of growing it out in the open, where it could be more easily seen.[68] But the Supreme Court correctly did not give law enforcement officers any special deference when the officers responded to the heat lamps with their own type of new technology to try to see through the walls of the house.

In short, courts have slowly abdicated their authority with regard to regulating new surveillance technologies. Some aspects of this deference, such as waiting for Congress to fill an obvious gap in existing legislation, may make sense. Other aspects, such

---

[67] *Id.* at 583 (citation omitted).

[68] *See Kyllo v. United* States, 533 U.S. 27, 29-30 (2001).

as courts giving law enforcement officers greater leeway if they are "responding" to new technologies, may be more problematic.

IV. DOCTRINES OF CONFUSED FORMALISM

One final trend we can see in the regulation of new surveillance technology is courts occasionally demonstrate a lack of understanding about how these technologies actually work. These misunderstandings can lead to nonsensical, formalist legal doctrines, which may take decades to correct.

We have already seen one example of this in *Olmstead*; the Supreme Court held that because the defendant was "project[ing] his voice to those quite outside" the house, he had no privacy rights in the communication.[69] In other words, the Court saw the telephone more like a radio transmitter, sending information out into the world for public consumption. This may have been a misunderstanding of the technology of the telephone, or perhaps a misunderstanding of how telephone communications were perceived by society. But either way, it was a serious—and fateful—misunderstanding. The *Olmstead* decision created a formalist, "property-centered" doctrine of Fourth Amendment rights—one which would last for forty years—in which the Court would determine whether there was a violation of a defendant's Fourth Amendment rights merely by looking to whether a defendant's property rights had been infringed upon.[70]

Olmstead's mistake was eventually corrected,[71] but a danger still exists of formalist doctrines arising as a result of a court's misunderstanding the nature of new technology. The most infamous of these doctrines can be found in the case of *Smith v. Maryland*.[72] In *Smith*, police officers—acting without a warrant or court order—instructed the telephone company to record all of the telephone numbers the defendant dialed from his telephone line.[73]

---

[69] Olmstead v. United States, 277 U.S. 438, 466 (1928); *see also supra* notes 14-15 and accompanying text.

[70] *See, e.g.*, Silverman v. United States, 365 U.S. 505, 511-12 (1961); Goldman v. United States, 316 U.S. 129, 135 (1942).

[71] Its specific holding was reversed by the Federal Communications Act of 1934, 47 U.S.C. § 605 (2006); its doctrine was reversed by the "reasonable expectations of privacy" test of *Katz v. United States*, 389 U.S. 347, 353, 360 (1967).

[72] 442 U.S. 735 (1979).

[73] *Id.* at 737.

The Supreme Court held no warrant was necessary since the defendant had "voluntarily conveyed to [the phone company] information that it had facilities for recording and that it was free to record."[74] In this case, the Court's *holding* was probably correct—an individual has no reasonable expectation of privacy in the phone numbers he or she dials, any more than the individual has a reasonable expectation of privacy in the address on a letter (or the address on an e-mail). In fact, such "addressing" information is now explicitly covered by statute and is given one of the lowest levels of protection, requiring only a showing of "certified relevance."[75] But, the Court's *reasoning* in the *Smith* case was calamitous—just as calamitous (and for the same reason) as its reasoning in *Olmstead* over fifty years before. Under the *Smith* doctrine, an individual loses all privacy rights to any information that he or she voluntarily conveys to a third party. Even in 1979, this was a dubious rationale since many people stored confidential information (such as bank records)[76] with third parties or passed such information on to others using third parties (such as telephone companies or private messenger services). In modern times, when many people use cloud computing for storing data and third-party ISPs for transmitting, this rationale is patently absurd.

Luckily, some modern courts have recognized this absurdity and found ways to reject the *Smith* doctrine. In the recent case of *United States v. Warshak*,[77] the Sixth Circuit held that a third party's access to stored e-mail does not eliminate the warrant requirement.[78] The *Warshak* court first looked to "the prominent role that e-mail has assumed in modern communication,"[79] stating:

> People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with

---

[74] *Id.* at 745.

[75] *See* 18 U.S.C. § 3122(b)(2) (2006); *see also supra* note 47 and accompanying text.

[76] *See* United States v. Miller, 425 U.S. 435, 442 (1976).

[77] 631 F.3d 266 (6th Cir. 2010).

[78] *Id.* at 286-88.

[79] *Id.* at 284.

> the click of a mouse button. . . . In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities.[80]

After analyzing the generally accepted uses and expectations for e-mail, the *Warshak* court analogized e-mail to the content of telephone calls or traditional letters[81] and concluded "the ISP is the functional equivalent of a post office or a telephone company."[82] The court also analogized the relationship between an ISP and its stored e-mails to the relationship between a hotel and the rooms it rents to its guests, thus establishing that neither the ability nor the right to access the stored information by a third party nullifies the owner's reasonable expectation of privacy.[83] Finally, the court rejected applying the precedent of *United States v. Miller*,[84] a pre-cursor of *Smith* in which a bank depositor was held to have no privacy rights in the information he conveyed to his bank.[85] According to the *Warshak* court, *Miller* was distinguishable because the bank was the ultimate end recipient of the information, while the ISP in *Warshak* was an intermediary.[86]

In short, the *Warshak* court made the effort to truly understand how stored e-mails are used and perceived by modern society, instead of merely relying on the formalist third-party doctrine that was crafted in a different context (storage of bank records) and then clumsily pasted onto a new technology (as in *Smith*).

Other courts have also rejected the easy formalism that has plagued this area of the law. A district court in New York recently had to determine how much protection to give "pass-through" digits in a telephone call. Pass-through digits are the numbers

---

[80] *Id.*

[81] *Warshak*, 631 F.3d at 285-86.

[82] *Id.* at 286.

[83] *Id.* at 287 (citing United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997)).

[84] 425 U.S. 435 (1976).

[85] *Id.* at 442-43.

[86] *Warshak*, 631 F.3d at 288.

dialed on a telephone after a connection is made—for example, digits that navigate through a phone tree or digits that communicate the caller's social security number or account number.[87] Although the government argued that these numbers should only receive the low-level protection afforded to dialed telephone numbers under the Pen/Trap statute,[88] the court looked to the *content* of the information being provided, which included "sensitive and personal" information such as "[b]ank account numbers, pin numbers and passwords, prescription identification numbers, social security numbers, credit card numbers, and so on . . . ."—the "functional equivalent" of what callers used to tell human operators.[89] When this information was considered in the proper context, the court had no problem confirming individuals had a reasonable expectation of privacy in the pass-through digits.[90]

Another recent case from the District of Massachusetts[91] also engaged in an admirably sensible—even prescient—analysis of a new technology. In this case, the question was the privacy afforded "historical cell site information"—that is, information subpoenaed from the cell phone company about the location of a cell phone at a time when a call is placed. The government argued these records were governed by the low standards of the SCA, requiring only a showing of "specific and articulable facts"[92] since it was only seeking stored "historical information" about the location of a caller at some time in the past when a call was placed.[93] The court, however, looked not to how the information was classified, but to how it would actually be used by the government as a tracking system, saying:

> In reality, the Government is seeking the issuance of an order that would technically permit the Government access to cell site information as early as one second prior to the

---

[87] *See In re* Applications for Pen Registers & Trap & Trace Devices, 515 F. Supp. 2d 325, 328 (E.D.N.Y. 2007).

[88] *Id.*; *see also* 18 U.S.C. § 3122 (2006).

[89] *In re Applications for Pen Registers*, 515 F. Supp. 2d at 336.

[90] *Id.*

[91] *In re* Applications for Historical Cell Site Info., 509 F. Supp. 2d 64 (D. Mass. 2007).

[92] *Id.* at 66; *see also* 18 U.S.C. § 2703(d) (2006).

[93] *In re Applications for Historical Cell Site Info.*, 509 F. Supp. 2d at 69.

> Court's issuance of the order. . . . it is unrealistic to believe that in the explosive world of technological advancement, the Government would not some day (if not now) be able to receive a signed order at 4:00 p.m., e-mail or fax the order to a telecommunication service provider by 4:05 p.m., and receive a cell phone's "historical" cell site information from 3:59 p.m., dramatically narrowing if not pinpointing a location. If this example is not *de jure* "real time" tracking, it is certainly *de facto* "real time" tracking.[94]

Given this fact, the court concluded that "the distinction between cell site data and information gathered by a tracking device has practically vanished"[95] and the government was required to meet the higher standard of probable cause that was statutorily required for using real-time tracking devices.[96]

Unfortunately, the kind of formalism we saw in *Olmstead* and *Smith* still appears in some modern cases. In *United States v. Scarfo*,[97] as previously discussed,[98] a district court in New Jersey was faced with the government's use of a key logger system (KLS)—software that transmitted to law enforcement every keystroke the computer user typed into his computer.[99] In order to get around the provisions of Title III, the government designed its KLS to only intercept keystrokes when the defendant's modem was turned off.[100] In this way, the government was able to intercept every piece of information the defendant typed into his computer—even information that was ultimately destined to be included in an e-mail, or information (such as a password) that would give the government access to e-mail, as long as the modem was not operational at the time the defendant typed the letters. The court accepted this clever scheme, noting that "[s]ince Scarfo's computer possessed no other means of communicating with

---

[94] *Id.* at 75 (footnote omitted).

[95] *Id.* at 70 (quoting *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 754 (S.D. Tex. 2005)) (internal quotation marks omitted).

[96] *In re Applications for Historical Cell Site Info.*, 509 F. Supp. 2d at 75-76; *see* 18 U.S.C. § 3117(b) (2006).

[97] 180 F. Supp. 2d 572 (D.N.J. 2001).

[98] *See supra* notes 65-67 and accompanying text.

[99] *Scarfo*, 180 F. Supp. 2d at 574.

[100] *Id.* at 582.

another computer save for the modem, the KLS did not intercept any wire communications" and Title III did not apply.[101] In truth, however, this kind of ongoing, overbroad surveillance (which by its nature intercepts far more than the particular information that the government has cause to search for) is exactly the type of surveillance that Title III was meant to restrict. Thus, the KLS is functionally much more like a wiretap than it is like a traditional search, but the court only considered a narrow view of how the KLS could be classified rather than how it functioned in reality.

A similar example of formalism can be found in *United States v. Ropp*,[102] in which a defendant was accused of violating the Wiretap Act[103] when he placed his own version of a KLS on a victim's computer and recorded the e-mails she was typing.[104] The court concluded that the defendant had not violated the Act because the KLS recorded the e-mail *before* the victim pressed the "send" key—that is, before any "wire transmission" occurred.[105] While this may be a correct holding given the specific language found in the Wiretap Act (especially given the need to interpret criminal statutes narrowly), the *reasoning* of the *Ropp* court was troubling, since the court put great emphasis on the fact the KLS was installed on the cable that attached the victim's keyboard to her central processing unit (CPU), rather than the cable that attached the CPU to the Internet:

> [T]he communication in question is not an "electronic communication" within the meaning of the statute because it is not transmitted by a system that affects interstate or foreign commerce. The "system" involved consists of the local computer's hardware—the Central Processing Unit, hard drive and peripherals (including the keyboard)—and one or more software programs including the computer's operating system . . . and either an e-mail or other communications program being used to compose messages. Although this system is connected to a larger system—the

---

[101] *Id.* (citation omitted). The court concluded that a search warrant was sufficient. *See id.*

[102] 347 F. Supp. 2d 831 (C.D. Cal. 2004).

[103] *See* 18 U.S.C. § 2511(1)(a) (2006).

[104] *Ropp*, 347 F. Supp. 2d at 831.

[105] *Id.* at 837.

> network—which affects interstate or foreign commerce, the transmission in issue did not involve that system.[106]

The implication is that if the defendant had placed his KLS on a different cable—perhaps the one that connected the CPU to the Internet and was therefore integral to the "larger system"—he would have been guilty of violating the Wiretap Act, even though he was recording exactly the same information in almost exactly the same way.

CONCLUSION

New technology has impacted the law of surveillance regulation in significant ways. Most of these changes have been predictable and, perhaps, inevitable. It is no surprise, for example, that Congress would step in to set out its own regulations in this area, given the rapid pace of change and the occasional missteps by the courts in attempting to keep up with this pace. And since different methods of surveillance involve different levels of intrusion into individual privacy, it should be expected that the courts and Congress would set up various different standards for each of these methods. Increased congressional involvement, along with the greater dangers posed by criminals who use technology for committing their crimes, can lead to courts becoming overly deferential to the other branches of government.

These trends all seem to be destined to continue into future decades. Congress has created a comprehensive framework of statutes regulating technological surveillance, and the courts have come to rely on—and even borrow from—these statutes. The differing standards created by these statutes have been approved by the courts and even—in the case of video surveillance—transformed into constitutional requirements. Given their past record, courts are likely to continue to misunderstand how new surveillance technologies work. The good news is that Congress is ready and more than willing to step in to correct these mistakes.

---

[106] *Id.* at 837-38.