

First Principles of Communications Privacy

Susan Freiwald*

January, 2007

DRAFT ONLY --- DRAFT ONLY --- DRAFT ONLY

I. Introduction

Recent clashes between administration officials intent on rooting out terrorism and those who decry intrusions on personal privacy have raised questions about the constitutional regulation of electronic surveillance. For example, the NSA recently claimed that the president's inherent powers under Article II justified its domestic wiretapping program. A district court in Detroit disagreed, and determined that the program violated the First and Fourth Amendments and separation of powers.¹

Yet when it comes to challenges to electronic surveillance for law enforcement purposes, the cases have largely involved interpretations of the Electronic Communications Privacy Act ("ECPA"), a law passed in 1986 to bring surveillance regulation into the age of electronic communications.² Since the Supreme Court delineated what procedural safeguards the Fourth Amendment imposed on traditional wiretapping, back in the 1967 cases of *Katz v. United States*³ and *Berger v. New York*,⁴ courts have avoided subjecting questions about modern electronic surveillance practices

* © 2000, Susan Freiwald. Professor, University of San Francisco School of Law. I thank Alex Miller and John Cannavino for their excellent research assistance.

¹ See *American Civil Liberties Union v. National Security Agency*, 438 F. Supp. 2d 754 (E.D. Mich. 2006).

² Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of U.S.C.).

³ *Katz v. United States*, 389 U.S. 347, 361 (1967).

⁴ *Berger v. New York*, 388 U.S. 41, 60 (1967).

to constitutional scrutiny. In *Katz* and *Berger*, the Supreme Court established that electronic eavesdropping constituted a Fourth Amendment search. Because of the particular dangers of abusing electronic surveillance, the Court required that agents who wanted to conduct it had to pass over several procedural hurdles significantly more demanding than the probable cause warrant needed to search a home.⁵ Congress incorporated those hurdles into the Wiretap Act that it passed the next year.⁶

But the Supreme Court has stayed out of the regulation of modern electronic surveillance as use of the internet and related electronic communications has supplanted use of the telephone. Lower courts have avoided constitutional review as well. In fact, a case currently pending in the 6th Circuit, *Warshak v. United States*,⁷ poses the first constitutional challenge to the Stored Communications Act, which is a subset of the ECPA that was passed in 1986.⁸ No Article III court has yet established whether or when users entertain a reasonable expectation of privacy in their e-mails, which a court must do if it is to impose the warrant requirement on surveillance.⁹

One could imagine that the courts have refrained from opining on the constitutional requirements for surveillance of modern electronic communications, or online surveillance, because the applicable statute has raised no constitutional questions.

⁵ See *infra* Part IVA for a discussion of those requirements.

⁶ Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Title III, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2522).

⁷ See *Warshak v. United States*, Order Granting in Part and Denying in Part Plaintiff's Motion for TRO, Case no. 1:06-cv-357, Southern District of Ohio, July 21, 2006 (available at www.cdt.org/security/20061127order.pdf)

⁸ See Stored Wired and Electronic Communications and Transactional Records Access, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (codified as amended at 18 U.S.C. §§ 2701-12).

⁹ So far two military courts have found a reasonable expectation of privacy in stored e-mail and imposed a warrant requirement on government access to it. See *United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006); *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996).

But that would be far from the truth. The ECPA, because it permits a substantial amount of surveillance to proceed without the requirement of a warrant, let alone the heightened procedural safeguards that apply to wiretapping, should have been quite vulnerable to constitutional challenges.¹⁰ In addition, while the ECPA covers several forms of modern electronic surveillance, there are whole categories of information that it leaves unregulated so we should have expected cases raising the question of what the Constitution requires for acquisition of that information.¹¹ Moreover, the ECPA provides no statutory suppression remedy for victims of improperly acquired electronic communications, though it provides one for victims of improper wiretapping.¹² Because targets may obtain an exclusionary remedy only after establishing the violation of a Fourth Amendment right, we should have seen more direct constitutional challenges to electronic surveillance practices rather than fewer.

In a series of recent cases, courts have imposed a warrant requirement on the government's acquisition of information from cell phones that discloses users' location.¹³ Although those cases have subjected the governments' claims to searching review, they have largely confined their analysis to an interpretation of the ECPA, and avoided the deeper constitutional question lurking in the background.

¹⁰ The scope of what the ECPA permits without a warrant is the subject of much current debate, including in the *Warshak* case.

¹¹ See Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9 (2004) (describing and discussing the ECPA's weak and incomplete coverage).

¹² See 18 U.S.C. §§ 2515, 2518.

¹³ See, e.g., *In the Matter of the Application of the United States for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device*, 441 F.Supp.2d 816, 836 (S.D. Tex. 2006) [hereinafter "Houston Pen/Trap"] (discussing government access to post-cut-through dialed digits and to cell site location information and noting that "[b]oth issues of electronic surveillance law are decided here as matters of statutory interpretation only").

In the *Warshak* case, the government claims that the SCA permits law enforcement agents to demand stored e-mails from service providers without first obtaining a probable cause warrant.¹⁴ The plaintiff in that case, Steven Warshak, argues that the court must either interpret the SCA to require a probable cause warrant for the acquisition of stored e-mails, or find its provisions unconstitutional if they cannot bear that interpretation.¹⁵ Amici law professors argue that the Fourth Amendment should require that stored e-mails be protected with the same heightened procedural safeguards, beyond a probable cause warrant, afforded to telephone conversations.¹⁶ The case thus asks the Sixth Circuit, for the first time, to subject the SCA to constitutional review.

This essay explores why it has taken so long for courts to address the constitutional protection of electronic communications. The explanation, I believe, comes in two parts. First, although the analogy between telephone communications and electronic communications such as e-mail seems quite direct, significant differences between the two forms of communication make it difficult to apply the wiretap precedents directly to modern surveillance practices. Therefore courts may not rely on a straightforward analogy to determine the constitutional status of modern communications, instead they must apply the constitutional test anew. Second, the constitutional test that courts apply, the reasonable expectation of privacy test, is unworkable, particularly in the context of modern electronic communications.

¹⁴ See Government Brief in Warshak case available at www.cdt.org/headlines/951.

¹⁵ Note that under the canon of constitutional avoidance, courts should choose statutory interpretations that do not raise constitutional problems, if possible. See *Houston Pen/Trap*, 441 F.Supp.2d at 837.

¹⁶ See law professors' amicus brief in Warshak case. Patricia Bellia and I were the two chief authors' of the law professors' brief, which attracted 13 other signatories.

Courts have largely avoided conducting a reasonable expectation of privacy analysis for modern electronic communications because the analysis pushes them beyond their competence.¹⁷ It requires them to first analyze society's views about the intricacies of new technologies that most users, including judges, do not understand. Properly done, the reasonable expectation of privacy analysis also requires that courts supplement that positive finding with a normative inquiry into the role of new communications technologies and whether users should be entitled to believe such communications are private.¹⁸ Courts have either avoided the reasonable expectation of privacy analysis, or have cut short the analysis, because they lack adequate empirical data for the positive inquiry and adequate guidance for the normative one.¹⁹

I argue that courts should largely abandon the positive inquiry into whether users actually expected their communications to be private, except for the most obvious cases of disingenuous claims. Courts should focus on the normative inquiry into whether users should be entitled to view their communications as private, but in doing so they should shift the inquiry away from users' apparent knowledge about whether their communications are vulnerable to interception. Instead, courts should resume their historical role mediating the tension between law enforcement's interest in obtaining as much information as possible and users' interest in avoiding excessive government

¹⁷ For an argument that criticizes Courts' competence to determine communications privacy rights but concludes that the legislature should bear responsibility for it, see Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004).

¹⁸ I use the term "positive" throughout to mean descriptive, but including a notion that what is is right. For a thorough discussion of the role of positivist and normative analysis in Fourth Amendment jurisprudence, see Silas J. Wasserstrom and Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L. J. 19 (1988).

¹⁹ For an empirical approach to reasonable expectations of privacy that illustrates the difficulties of measurement see Christopher Slobogin and Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727 (1993).

intrusion into their lives. To do that, courts need a test that focuses on the nature of the electronic surveillance practices themselves and asks whether those practices implicate Fourth Amendment concerns about intrusive government investigatory methods and therefore require the interposition of a neutral judicial officer to minimize abuse.

Just such a test can be derived from a series of cases that extended the core protections of the Wiretap Act to silent video surveillance at a time when that practice was just beginning. In the mid-1980's through early nineties, seven federal Courts of Appeal found that the Fourth Amendment regulated video surveillance of non-public places in the same heightened manner that it regulated wiretapping.²⁰ Because such video surveillance was hidden, intrusive, indiscriminate and continuous, that surveillance implicated the same privacy concerns as wiretapping, and could be conducted by law enforcement agents only according to the same heightened procedural protections as regulated traditional wiretapping.²¹ Although the courts imposed the requirements as a matter of constitutional law, they did so because the surveillance method was particularly subject to abuse, and not based on an assessment of whether the targets should have or could have known that they were being surveilled.

A court that applies this four-factor test would ask answerable questions about the ways in which the proposed surveillance implicates the Fourth Amendment's core concerns. When surveillance is hidden, the target is less able to hold government investigators accountable himself and therefore needs the court to protect his interests.

²⁰ See *United States v. Torres*, 751 F.2d 875, 882-884 (7th Cir. 1984), *cert. denied*, 470 U.S. 1087 (1985); *United States v. Biasucci*, 786 F.2d 504 (2d Cir.), *cert. denied*, 479 U.S. 827 (1986); *United States v. Koyomejian*, 970 F.2d 536 (9th Cir.) (en banc), *cert. denied*, 506 U.S. 1005 (1992); *United States v. Mesa-Rincon*, 911 F.2d 1433 (10th Cir. 1990); *United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987); *United States v. Falls*, 34 F.3d 674 (8th Cir. 1994); *United States v. Williams*, 124 F.3d 411 (3rd Cir. 1997) (assuming the validity of the approach of the other circuits).

²¹ See *infra* Part IVA.

Intrusive surveillance practices bring the police further into our private lives, and therefore require judicial intervention to ensure that government makes such intrusions only after satisfying a high level of need. Indiscriminate surveillance obtains information beyond that which is justified, and therefore requires court oversight to make sure such unjustified surveillance is minimized. Finally, continuous surveillance is more likely to be intrusive and indiscriminate because it acquires more information over a longer period of time.

The essay proceeds in Part II by explaining the ways in which modern electronic communications offer novel questions of constitutional interpretation. In particular, it discusses how law enforcement agents' ability to obtain electronic communications that have been stored gives them a tool they did not have with traditional telephone calls at the time of *Katz* and *Berger*. It then discusses how the reasonable expectation of privacy test could be applied to such stored e-mails, and demonstrates that the method is both unwieldy and misguided. Part III further illustrates the unworkability of the reasonable expectation of privacy test by describing ways in which courts have largely avoided applying it. In particular, courts have strained to apply pre-modern precedents that themselves shortcut the reasonable expectation of privacy test by ignoring the essential normative inquiry. Part IV describes the evolution of the four factor test, and then illustrates how it could determine the appropriate constitutional regulation of stored e-mails. This essay concludes that courts should use the four factor test to determine the constitutional minimums for modern electronic surveillance practices, and to ensure that the ECPA does not permit the government to sidestep essential procedural safeguards.

Part II. Reasonable Expectation of Privacy in Electronic Communications

A. From Telephone Conversations to E-mail and Internet Communications

Because e-mail correspondence seems directly analogous to telephone conversations, it seems at first obvious that courts could extend the Fourth Amendment scheme for traditional wiretapping to cover e-mail “wiretapping” as well.²² In fact, congressional drafters of the ECPA used just that logic to extend the statutory protections of the Wiretap Act to cover acquisition of electronic communications.²³ With a few exceptions, the ECPA merely added the word “electronic communication” to every instance of “wire communication” in the statute. Congress therefore imposed the same heightened requirements on law enforcement agents who intercept electronic communications as are imposed on law enforcement agents who intercept traditional telephone calls, with the notable exception of a statutory exclusionary rule.²⁴ Yet no court has grounded those requirements in the same Fourth Amendment protection that the Supreme Court afforded to telephone conversations in *Katz* and *Berger*. Courts have not been asked to extend that protection to electronic interceptions, despite the fact that victims’ lack of a statutory suppression remedy means they must establish a constitutional violation to have improperly “wiretapped” electronic communications excluded from their criminal trials.

²² See, e.g., *United States v. Maxwell*, 45 M.J. 406 (C.A.A. F. 1996) (“[t]he technology used to communicate via e-mail is extraordinarily analogous to a telephone conversation.”). One could also analogize e-mails to first class letters, sealed packages, or even post cards.

²³ See H.R. Rep. No. 99-647 (1986); S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555.

²⁴ The other two differences concern the fact that there is no limit on the predicate felonies for surveillance of electronic communications, and lower level officials may approve of applications. [cites]

The analogy between telephone communications and electronic communications actually breaks down at the point where law enforcement agents gain access to them. People converse on the telephone at the same time, but they compose e-mails to each other one at a time.²⁵ Because traditional telephone conversations occurred simultaneously, and left no record after they were finished, agents who sought the contents of those conversations had to acquire them as they happened.²⁶ Electronic mail “conversations” occur when one person sends an e-mail to another, and that e-mail is stored for later retrieval by its recipient. Because e-mails occur asynchronously, and must be stored, law enforcement agents need not acquire them as they are sent, in real time. Instead, agents may obtain electronic communications while they reside in electronic storage on the computer of the recipient, or more likely, on the server of a third party intermediary such as an internet service provider (“ISP”).²⁷

Victims of “wiretapped” e-mails have not petitioned the courts for constitutional protection because law enforcement agents generally obtain e-mails out of storage rather than in real time.²⁸ Acquisition of e-mail out of storage offers several advantages. At any given time, much more extensive e-mail correspondence may be found on an ISP’s server than may be intercepted. Were a government agent to intercept e-mails in transit she would acquire the e-mail traveling at that moment only. An agent who demands e-mails

²⁵ Text messages are more like e-mails than telephone conversations, with instant messages falling in the middle, but closer to electronic communications if they are stored on a computer.

²⁶ Whether or not the conversation was recorded for later review, it was intercepted by the agents as it transpired in real time.

²⁷ I use the term “electronic storage” throughout this paper in its common sense meaning, and do not address the question of what counts as “electronic storage” under the ECPA. See 18 U.S.C. § 2510 (17).

²⁸ One recent case considered whether e-mails obtained before arriving in the recipient’s mailbox were obtained out of electronic storage, but that case involved interception by a private person rather than the government. See *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005).

from an ISP, however, may obtain all the e-mails stored there. ISP's may store extensive amounts of e-mail, both sent and received by the account holder; some new services appeal to potential customers by telling them that they will never have to delete an e-mail again, because the service will retain it indefinitely.²⁹ In addition, to acquire e-mail out of storage, law enforcement agents may ask the ISP to provide it, rather than using technological measures to extract e-mail moving over a network.

Because the courts have yet to address it, we do not know what procedural safeguards the Constitution provides e-mail residing in the hands of third party ISP's. As a result, we do not know whether the statutory provisions that govern that exchange fulfill constitutional prerequisites. What we do know is that the ECPA affords dramatically less protection to stored e-mails than it does to e-mails acquired in transit. That scheme should be counterintuitive because, as just described, law enforcement agents may acquire more electronic communications more easily by obtaining them out of storage, and, in fact, many have criticized the SCA for its anemic protections.³⁰ A large part of the problem is that Congress devised the SCA's framework and terms in 1986, when networked computing was in its infancy. Congress has not meaningfully updated the SCA since its passage, and government lawyers have exploited out-of-date terms to press courts to provide minimal protections.³¹

Wherever the fault lies for the weak protection of stored e-mails, however, it is much easier both in fact and under the law to obtain e-mails out of storage rather than

²⁹ Google advertises g-mail that way.

³⁰ See, e.g., Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004).

³¹ See Freiwald, *supra* note 11, at 44-74 (for a critique of both the SCA and law enforcement interpretations of it).

according to a “wiretap-like” procedure. Yet the ECPA presupposes that only e-mails acquired in transit are entitled to the highest protection of the Wiretap Act, minus the statutory exclusionary remedy. For the vast majority of stored electronic communications data, the statute affords at most the protection of a warrant based on probable cause, and in some cases less. As noted, the ECPA should certainly be vulnerable to constitutional challenges for affording law enforcement access to rich electronic communications data in storage upon less than a warrant, much less the full protections of the Wiretap Act.

Courts have not properly determined what the Constitution requires when law enforcement agents acquire modern electronic communications out of storage. They have not yet evaluated how the reasonable expectation of privacy test applies to stored e-mails. The problem, I suggest, inheres in the difficulty of applying that test properly.

B. What the Reasonable Expectations of Privacy Test Requires

Since *Katz*, courts have used the reasonable expectation of privacy test to determine whether a particular investigatory technique constitutes a search under the Fourth Amendment, and if so, to accord appropriate procedural safeguards. In the communications context, the reasonable expectation of privacy test endeavors to identify those law enforcement investigations that intrude upon private communications and thereby implicate constitutionally protected rights. The Fourth Amendment generally requires that agents obtain a probable cause warrant approved by a neutral judicial officer before they conduct a search, unless an exception applies. To engage in particularly

intrusive electronic surveillance, such as wiretapping, agents have to satisfy more demanding prerequisites.³²

The reasonable expectation of privacy inquiry asks whether the target of an investigation entertains an actual expectation of privacy in the object of the search (subjective prong), and whether that expectation of privacy is one that society deems reasonable (objective prong).³³ The subjective prong denies constitutional protection to those who did not themselves view the object of the investigation as private. The objective prong withholds protection from subjective claims that go too far, such as claims that information disclosed to the general public merits constitutional protection. To require that government agents refrain from viewing information disclosed to the public is both unfair and unnecessary. It is unfair because the government should not be disadvantaged vis-à-vis the average member of the public. It is unnecessary because we assume that before people make information publicly available they have either determined the repercussions of that disclosure to be harmless, or have assumed the risk of those repercussions.³⁴ The Constitution does not protect information that one has “knowingly expose[d] to the public.”³⁵

Critics have faulted the reasonable expectation of privacy test for being self-defining. The presence of “reasonable” in both the name of the test and its definition

³² See *infra* Part IVA.

³³ See *Kyllo v. United States*, 533 U.S. 27, 32-33 (2001); *Katz v. United States*, 389 U.S. 347, 361 (1967).

³⁴ The application of an assumption of risk analysis to disclosures to the general public, which is what I mean by “public,” seems appropriate. As I discuss below in Part III, problems with reasonable expectations of privacy emerge when the assumption of risk analysis is extended beyond the truly “public” context.

³⁵ *Katz*, 389 U.S. at 351.

makes the test circular: reasonable expectations are reasonable.³⁶ When commentators criticize the circularity of legal test, they typically take issue with the unfettered discretion that it affords judges. But many legal tests afford judges discretion; unconscionable contracts are those the court deems to be unconscionable, for example. The problem with the reasonable expectations of privacy test is not that it requires judicial discretion, but that it requires both a positive and normative inquiry that challenges courts' competence. Moreover, the test, as courts currently interpret it, misplaces the focus on what the target knew or should have known instead of the intrusive nature of the surveillance itself.

1. Positive Inquiry

To assess whether a target had a reasonable expectation of privacy in her electronic communications, a court must determine what the target believed. When a target claims that her constitutional rights were violated, surely she will know enough to claim that she thought she had such a privacy right in the first place. In the absence of lie detector data or the target's admissions to the contrary, law enforcement agents will counter that the target could not have believed that her communications were private, because it is not reasonable to do so. The question then quickly shifts to what reasonable people believe about the privacy of those electronic communications. In other words,

³⁶ See, e.g., Wasserstrom and Seidman, *supra* note 18, at 69 (discussing the “notorious circularity” of the reasonable expectation of privacy test).

almost all of the analysis will concern the objective prong, which asks whether society deems a subjective claim of privacy, on the facts presented, to be reasonable.³⁷

Unfortunately, there is no well established method to determine whether society deems any particular expectation of privacy to be reasonable. Although the objective test seems to call for empirical studies, they would be difficult to conduct as surveys of popular beliefs. For stored e-mails, the survey question would have to be something like “Do you believe that, before law enforcement agents may lawfully acquire the contents of your e-mails out of the electronic storage of your service provider, they must first obtain a wiretap-like court order, a probable cause based warrant, or some lesser procedural hurdle?” The need to explain both the method of acquisition and the legal choices would be both too complicated and too easily skewed by the questioner.

One could more easily conduct empirical studies of common behaviors, and try to extrapolate from those what people must believe to be a reasonable expectation of privacy.³⁸ In the recent case of *Google v. DOJ*, Judge Ware demonstrated what such an inquiry might look like when he observed that users’ tendencies to search for pornography online suggested that they regarded those searches to be private.³⁹ That analysis was admirably innovative, and could likely be replicated on a larger scale. In other words, it seems safe to assume that most people use modern communications technologies in ways they would prefer not to have broadcast to the world. If that were

³⁷ See Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974) (discussing problems with the subjective prong); 1 W. LAFAVE, SEARCH AND SEIZURE § 2.1 (4th. ed. 2007) (“[L]ittle attention has been given [by courts] to the independent significance of the first factor or to precisely how it is to be interpreted”).

³⁸ That seems to be the approach courts have taken in other reasonable expectation of privacy assessments. Whether it works well in those contexts, which is much debated, it is particularly ineffective in the online environment.

³⁹ See *Gonzales v. Google*, 234 F.R.D. 674, 687-88 (N.D.Ca. 2006) (describing data about online searches for pornography as “generally not information that anyone wishes to reveal publicly”).

true, then an individualized reasonable expectations of privacy inquiry would not be needed to deem modern communications technologies worthy of constitutional protection.

The chief difficulty with the reasonable expectations of privacy test, however, is that it poses a question for which there is no answer. A person asked whether he thought that government agents could access his e-mail account would probably have never thought about it before. Most likely he would believe that law enforcement agents would be unlikely to take the time to access his communications, and so he would not have worried about it. Even if the person queried had heard about the NSA's domestic surveillance program, he would still be unlikely to assume that he had been a target.⁴⁰ Moreover, just because a person knows that law enforcement agents have the technological capability to access electronic communications, that does not mean that he would be unperturbed to find out that they actually accessed his.

Courts may safely assume that a person who speaks out in public waives the right to complain if a police officer is present in the crowd. But there is no analogy between speaking openly to a crowd and sending a message to someone else over the internet. If users of e-mail need to choose the words of their private e-mails as carefully as if they were speaking to a large crowd, then the internet will lose much of its value.⁴¹ That law enforcement agents have the technical capability to access e-mails, which is by no means

⁴⁰ *But see* American Civil Liberties Union v. National Security Agency, 438 F. Supp. 2d 754, 767-70 (E.D. Mich. 2006) (granting standing to plaintiff group of journalists, academics, and lawyers whose professional work was damaged because their witnesses, sources and clients saw themselves as targets of NSA surveillance program).

⁴¹ *Cf.* Amsterdam, *supra* note 37 (discussing pernicious effects of assumption of risk analysis on society).

universally known, cannot mean that a user assumes the risk that agents will access whatever e-mails they choose, independent of any judicial oversight.

As I discuss in the next Part, some courts have applied the faulty reasoning just described to deny constitutional protection to aspects of modern communications technologies. They have concluded that, because particular communications can be intercepted by law enforcement agents as a matter of fact, they may be intercepted without constitutional regulation as a matter of law. In conducting that “fact-of-interceptibility” analysis,⁴² however, courts have taken an impermissible short cut. They have made finding a reasonable expectation of privacy in particular communications dependent on the public’s opinion that those communications are invulnerable to acquisition. That result conflicts with *Katz*, where the Supreme Court established that courts must not conclude a reasonable expectation of privacy analysis without engaging in a normative inquiry.

2. Normative Inquiry

When the Supreme Court formulated and applied the reasonable expectation of privacy test in *Katz*, it found the expectation of privacy in telephone calls to be reasonable, despite public awareness of the vulnerability of those calls to interception. In the several years preceding *Katz*, the public had learned of rampant illegal wiretapping from numerous influential books, scholarly articles, and newspaper accounts. At the same time, during the period in which it considered legislation to fix the problem, Congress had convened numerous hearings and commissioned lengthy expert reports that

⁴² See Susan Freiwald, *supra* note 11, at 38-39 (2004) (defining and discussing the term “fact-of-interceptibility”).

detailed communications' vulnerability.⁴³ Thus, not only were telephone conversations not private in fact, in the sense of being invulnerable to surveillance, but it is likely that most members of the public were aware of this vulnerability at the time. Nonetheless, the *Katz* Court found warrantless wiretapping to be unconstitutional, without actually considering the depth of the public's understanding about the telephone's vulnerability.⁴⁴

Rather than survey users for their views about privacy, or protect only invulnerable communications, the Supreme Court in *Katz* based constitutional protection of telephone calls on the overriding importance of the telephone. The Court majority noted that “[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.”⁴⁵ In other words, whatever people actually thought or knew about the privacy of their telephone calls, they were *entitled to believe* in the privacy of telephone calls, because any other result would be destructive of society's ability to communicate. The Supreme Court made the normative finding in *Katz* that one who places a telephone “call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.”⁴⁶

Justice Harlan, the author of the concurring opinion which formulated the reasonable expectation of privacy test, himself recognized that the ultimate question required a value judgment by the Court. In a case coming just four years after *Katz* that addressed the transmission of a conversation taped by a government informant, Justice Harlan wrote,

⁴³ *See id.* at 74-75.

⁴⁴ *See id.* at 38.

⁴⁵ *Katz*, 389 U.S. at 352.

⁴⁶ *Id.*

Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society. The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens, the risks of the electronic listener or observer without at least the protection of the warrant requirement.⁴⁷

In a later case involving application of the reasonable expectation of privacy test, the Supreme Court elaborated on the need for a normative inquiry. The Court noted that one could not deny constitutional protection merely because the government had announced that the target of their search was not private.⁴⁸ To do otherwise would place constitutional rights at the mercy of the executive branch, an entity which the Fourth Amendment was specifically designed to constrain.

To deny constitutional protection to e-mail and other modern electronic communications information because of its vulnerability to interception would make the very mistake the Court avoided in *Katz*.⁴⁹ Constitutional rights constrain both abusive government practices and new technological tools that facilitate abuse. Government tools and practices may not constrain constitutional protections. Indeed, to conduct the appropriate analysis, a court must determine what users of modern electronic communications are “entitled to believe” about those communications and whether those

⁴⁷ *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting). Justice Harlan also noted in that case that “the Fourth Amendment is principally concerned with protecting interests of privacy, rather than property rights.” *Id.* at 781.

⁴⁸ *See Smith v. Maryland*, 442 U.S. 735, 739 n.5 (1979) (recognizing that the expectation of privacy analysis must be replaced by a normative analysis when “subjective expectations had been ‘conditioned’ by influences alien to well-recognized Fourth Amendment freedoms.”)

⁴⁹ *See White*, 401 U.S. at 786 (Harlan, J., dissenting) (“The analysis must, in my view, transcend the search for subjective expectations or legal attributions of assumptions of risk.”); W. LAFAYETTE, *supra* note 37 (discussing the evolution in Justice Harlan’s thinking).

communications have assumed a vital role in our lives.⁵⁰ Even though we have not used electronic communications nearly as long as users had used telephones at the time of *Katz*, were a modern court to try to assess the contribution of electronic communications to modern life, it would likely find them at least as crucial as the public telephone in 1967.

But a general finding that electronic communications are vital to modern society does not address specific questions about how to parse the reasonable expectation of privacy test in all aspects of those communications. Networked computing has changed considerably in the last decade, and its most recent incarnations permit the storage of limitless electronic communications data on third party systems. Similarly, the World Wide Web continues to evolve, and it is difficult to predict what form communications will take in the very near future. A modern court would surely find it difficult to determine exactly which communications forms and attributes have attained the same vital role in private communications as the public telephone in *Katz*. That suggests that the type of normative inquiry conducted in *Katz* does not translate well into the modern age.

I believe that difficulty with the reasonable expectation of privacy test has led courts to avoid using it to resolve the constitutional status of modern communications technologies. But the answer cannot be to withhold constitutional protection from electronic communications, as courts do when they fail to act. Congress has already shown itself incapable of providing adequate protection by allowing the ECPA to fall out of touch with modern practices. Much of what the statute protects it does so weakly, and

⁵⁰ See, e.g., White, 401 U.S. at 786 (Harlan, J., dissenting) (“Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present.”); Amsterdam, *supra* note 37, at 403 (“The ultimate question, plainly, is a value judgment”).

there is much it does not protect. If courts do not establish constitutional protections for the electronic communications that are now central to our lives and work, then we will have afforded law enforcement surveillance powers of Orwellian magnitude.

Seizing upon the difficulty of determining whether users enjoy a reasonable expectation of privacy in their electronic communications, government lawyers have urged courts to work around it. The Department of Justice (“DOJ”) has argued that precedents from the pre-modern age apply and answer the question (in the negative). In doing so, the government encourages courts to make two significant errors. First, it encourages them to extend precedents past the point that the analogy supports, and second, it encourages them to short cut the reasonable expectation of privacy test by avoiding the crucial normative inquiry.

Part III – Short Cutting the Reasonable Expectation of Privacy Test

Thus far I have identified as an open constitutional question the level of Fourth Amendment protection afforded to stored electronic communications. This Part argues that in urging courts to deny meaningful constitutional protection to stored e-mails, the government pushes for a short cut around a proper reasonable expectation of privacy analysis. The past willingness of some courts, including the Supreme Court, to take that short cut further illustrates the weakness of the reasonable expectation of privacy test and the need for an alternative.

In the *Warshak* case pending in the 6th Circuit, government lawyers argue that law enforcement demands for electronic communications stored on third party servers do not

intrude upon any reasonable expectations of privacy. They claim that because law enforcement investigators obtained Warshak's e-mails from his ISPs rather than from him, they did so free of the warrant requirement, and certainly free of the constitutional hurdles placed on would-be wiretappers.⁵¹ The government claims the right to obtain stored opened e-mails using a simple subpoena or a court order based on simple relevance, and that the most the Constitution requires is that the government's methods be "reasonable."⁵²

The DOJ bases its claim on an expansive interpretation of *United States v. Miller*, a 1976 case in which the Supreme Court used the reasonable expectation of privacy test from *Katz* to withhold constitutional protection from financial records held by a bank. In *Miller*, the Court opined that, because bank customers knowingly permitted bank employees to view records of their transactions, customers could have no "legitimate expectation of privacy" in those records.⁵³ The DOJ asks the Sixth Circuit to extrapolate from *Miller* and find that e-mail users also lack a reasonable expectation of privacy in their e-mails, because they knowingly store them with their ISP.⁵⁴

⁵¹ Based on its reading of the ECPA, the government distinguishes between e-mails that have not been opened, accessed or downloaded, and those that have, and appears to believe a warrant protects the former. See Government's Brief in Warshak, available at www.cdt.org/headlines/951. Rather than bring that discussion into this paper, when I refer to stored e-mails, I mean all e-mails in storage, whether or not they have been accessed. For a critique of the government's distinction, see the Law Professors' amicus brief in Warshak.

⁵² Whether the Fourth Amendment should be interpreted to require "reasonableness" rather than a warrant is beyond the scope of this paper. Compare Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994) (criticizing the historical basis for the warrant requirement and promoting a "reasonableness" approach) with Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547 (1999) (refuting the historical case for "reasonableness" and promoting the probable-cause warrant as key under the Fourth Amendment).

⁵³ See *United States v. Miller*, 425 U.S. 435 (1976).

⁵⁴ See Government Brief in Warshak case, available www.cdt.org/headlines/951.

Commentators have identified many problems with the Supreme Court's reasoning in *Miller*, most notably that it expanded the dubious assumption of risk approach from *Hoffa v. United States*.⁵⁵ While *Hoffa* teaches that one may not trust one's associates not to be government informants, *Miller* instructs us that we may not trust our bank employees to respect the privacy our financial records.

Here I take issue with the way the *Miller* Court cut the reasonable expectation of privacy inquiry short. While purporting to address the bank customer's reasonable expectations of privacy, the Supreme Court opted instead for a truncated positive inquiry that asked only whether the bank customers had made their records available to others.⁵⁶ From that availability, the Court presumed that bank customers expected no privacy, without inquiring into what customers actually thought about when they used banking services, and what it was reasonable to expect them to consider. Despite purporting to follow *Katz*, the Court did not consider whether banking services played such a vital role in society that customers were entitled to view their records as private notwithstanding their knowledge of third party access.

Were courts to apply *Miller*'s reasoning to e-mail they would apply a precedent that does not fit the facts. The analogy between banking records and stored e-mails does not hold. Bank customers in 1976 had to submit their transactions to bank employees for substantive review, but e-mails are processed and stored largely without the intervention of any human intermediaries. Though the assumption of risk analysis makes little sense in *Miller*, because people hardly had a choice about whether to entrust their financial

⁵⁵ *Hoffa v. United States*, 383 U.S. 293 (1966). See, e.g., Patricia L. Bellia, *Surveillance Law through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1397-1412 (2004).

⁵⁶ See *Miller*, 425 U.S. at 442-43.

records to banks, it makes absolutely no sense in the online context.⁵⁷ Although it is a significant stretch to suggest that banking customers in 1976 consciously thought about the need for banking employees to process their transactions, modern e-mail users could defensibly assume that no humans process their electronic communications.

Even if the analogy could be drawn, courts should not replicate the error in *Miller* by assuming that customer assent to access for some purposes implies assent to access for others. The DOJ asks the Sixth Circuit in *Warshak* to do just that when it urges the court to reason that because ISP's may access the e-mails they store for maintenance and security purposes, that access negates the reasonableness of any expectation of privacy in them. That approach treats the reasonable expectation of privacy as all or nothing – if a person cannot establish that his communications are invulnerable to any access, then he may not complain if law enforcement agents access those communications without satisfying constitutional prerequisites. That courts avoid the more subtle inquiry into expectations vis-à-vis law enforcement access illustrates their discomfort with the test.⁵⁸

Besides conflating access by service providers for a legitimate business purpose with government access to pursue law enforcement objectives, the *Miller* approach to stored e-mails puts the analysis exactly backward. Just because law enforcement agents may have the capability to access users' stored emails, that does not mean that the Constitution permits such access. Ever since the Supreme Court abandoned the type of textualism that inhibited it from according Fourth Amendment protection to intangible

⁵⁷ For a thorough refutation of the application of *Miller* to electronic communications stored with ISP's, see Bellia, *supra* note 55, at 1403-07.

⁵⁸ *But see United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006) (finding that reasonable expectation that service provider would monitor electronic communications did not imply expectation that provider would disclose communications to law enforcement agents investigating crime).

communications in *Olmstead*,⁵⁹ it has recognized that the Fourth Amendment must keep pace with new technologies rather than permit technologies to circumscribe its protections. In conducting constitutional privacy analysis, courts must determine what law enforcement practices are permitted. Courts must not assume that whatever practices are possible are permissible. Otherwise the Fourth Amendment will quickly fall into desuetude.

It is too soon to say whether the Sixth Circuit and courts who subsequently face the question will continue to avoid the full reasonable expectation of privacy inquiry and instead opt for a short cut. After all, it is much easier to determine whether a third party has access to the communications at issue than it is to conduct the in depth positive and normative inquiry required by the reasonable expectation of privacy test. The Supreme Court's avoidance of a full inquiry in *Miller* certainly demonstrates the difficulty of the task.

Since *Miller*, numerous courts have similarly truncated the reasonable expectation of privacy analysis in the case of "non-contents" communication information. Those cases further illustrate the difficulty applying a full reasonable expectation of privacy analysis.

In *Smith v. Maryland*, decided in 1979, the Supreme Court again cut off the reasonable expectation of privacy analysis at the positive stage. Applying *Miller's* logic, the Court opined that telephone users lack a reasonable expectation of privacy in the telephone numbers they dial because they convey them to the telephone company, which has recording facilities. As in *Miller*, the Court presumed that callers took the

⁵⁹ *Olmstead v. United States*, 277 U.S. 438, 464-65 (1928).

vulnerability of their telephone numbers into account when making their calls. That presumption was even more strained in *Smith*, however, because the Court based user's supposed knowledge of phone company practices on rather obscure notices in telephone books that disclosed telephone companies' ability to trace calls in cases of harassment, and on the fact that toll call telephone numbers appeared on customers' bills.⁶⁰

Whatever the merits of the Court's positive findings, it completely avoided the normative inquiry required by *Katz*. The *Smith* majority did not discuss whether the vital nature of the telephone system required the protection of telephone numbers no matter what individual users thought or knew about the phone company's capacity to record those numbers. The Court did not consider whether telephone users should be entitled to expect their telephone numbers to remain protected by the Fourth Amendment, just as their accessible and potentially recorded telephone conversations were. Justice Marshall, in dissent, chided the Court for tying privacy protection to what risks a person may be "presumed to accept" instead of tying it to "the risks he should be forced to assume in a free and open society."

Since *Smith*, several courts have extended its reasoning well beyond its narrow application to dialed telephone numbers. Courts have found no reasonable expectation of privacy in modern electronic communications data such as subscriber information and records of electronic mail correspondence because they have analogized that information to the telephone numbers in *Smith*.⁶¹ One court recently used *Smith* approach to find no

⁶⁰ See *Smith*, 442 U.S. at 742-43. Several commentators have criticized the reasoning in *Smith*. See, e.g., Scott E. Sundby, "Everyman's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen," 94 COLUM. L. REV. 1751, 1757-58, 1794-95 (1994); Bellia, *supra* note 55.

⁶¹ See, e.g., *Guest v. Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001) (denying the suppression of passwords, names, addresses and birthdates because they were provided to a third party); *United States v. Hambrick*, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000), *cert. denied*, 531 U.S. 1099

privacy interest in data about a user's location that was transmitted to his cellular phone provider.⁶² Courts in these cases have chosen an easy short cut. They have largely avoided determining how society views the type of information at issue. More importantly, they have sidestepped the normative question of whether users may rely on the privacy of the information at issue because of the vital nature of that aspect of modern communications.⁶³ Because it is easier to identify information as not contents than it is to conduct a full reasonable expectation of privacy analysis, courts have stretched the *Smith* precedent well past what its reasoning supports.

Smith, Miller and their progeny suggest the appeal of taking short cuts rather than engaging in a thorough reasonable expectation of privacy analysis. They also reveal the danger of that approach. By focusing merely on whether third parties have access to our communications data, or whether that data can be characterized as not contents, courts have authorized increasingly powerful surveillance methods without any judicial oversight. But if the problem stems from the constitutional test, then the answer must be a new test that courts may actually use to translate Fourth Amendment values into the age of modern electronic communications.⁶⁴

Part IV. The Four Factor Test

(2001) (denying suppression of e-mail address, name, billing address, credit card number, and IP connection information); *United States v. Kennedy*, 81 F. supp. 2d 1103, 1110 (D. Kan. 2000) (denying suppression of subscriber information).

⁶² *See* *In re Application for an Order for Disclosure of Telecommunications Records*, 405 F. Supp.2d 435, 449-50 (S.D.N.Y. 2005).

⁶³ The court in *Hambrick* recognized the need to make a "value judgment" about "how much privacy we should have as a society," and then deferred to the weak protections of the ECPA as indicating a lack of privacy. *Hambrick*, 55 F. Supp. 2d at 506-07. *See infra* text accompanying notes 77-80 for a discussion of why it is inappropriate to defer to Congress on questions of Fourth Amendment value.

⁶⁴ *See* LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999) (discussing the need to translate constitutional values to modern technologies) (2.0?).

Courts have asked whether communications *are* vulnerable to interception, instead of whether they *should* be vulnerable to interception. In limiting their inquiry to what is possible rather than what should be constitutional, judges inappropriately yield the evolution of communications privacy to the vagaries of technological developments and neglect the essential role of the law in shaping practices rather than merely reflecting them. To fulfill their constitutional obligations, courts must adopt a test that they are willing to apply and that makes sense to apply. A four factor test that determines constitutional regulation of an investigative technique by evaluating whether it is a hidden, intrusive, indiscriminate and continuous method of surveillance makes sense to apply because it correctly places the focus on law enforcement's methods. That seven Courts of Appeal used the test to extend the core protections of the Wiretap Act to targets of video surveillance demonstrates that courts are willing to apply the test as well.

A. The Video Surveillance Cases

In *Berger*, the Supreme Court set forth the constitutional requirements for any statute that purported to authorize law enforcement's use of electronic surveillance of telephone communications. To avoid giving investigators a "roving commission" to search any and all conversations, the *Berger* court required applications for court orders to establish not just probable cause but also to identify both the person targeted and the conversations sought. In addition to requiring the active involvement of a judge in granting court orders, the Court required that the warrant be returned to the granting

judge, so that the officer alone would not decide how to use any conversations seized. Overall, the Court emphasized the need for “adequate judicial supervision or protective procedures.”⁶⁵ Six months later, in *Katz*, the Court affirmed that suppression remedies would be afforded to victims of unlawful surveillance so that after-surveillance review could ensure that officers had complied with the Fourth Amendment requirements.

In *Berger* and *Katz*, the Supreme Court clearly established that the Fourth Amendment does not trust the executive branch to review its own electronic surveillance practices. In fact, after the majority in *Berger* described the high hurdles law enforcement agents would have to get over before their surveillance could pass constitutional muster, two dissenters accused the majority of trying to prohibit such electronic surveillance altogether.⁶⁶ Nonetheless Congress succeeded in designing a constitutionally sufficient regulatory scheme for traditional electronic surveillance, the Wiretap Act of 1968. The Wiretap Act incorporated the highly protective and demanding procedural safeguards required by *Berger* and *Katz*.

When seven Courts of Appeals considered how to regulate silent video surveillance in the mid-1980’s and early 1990’s, they determined that video surveillance also requires a heightened level of judicial oversight.⁶⁷ Like wiretapping, and unlike one-shot physical searches for which a traditional warrant usually suffices, video surveillance is hidden, intrusive, indiscriminate, and continuous and therefore particularly susceptible

⁶⁵ See *Berger*, 388 U.S. at 56-60.

⁶⁶ See *Berger*, 388 U.S. at 71 (Black, J., dissenting); *id.* At 111 (White, J., dissenting).

⁶⁷ See cases cited in note 20. See also Kent Greenfield, *Cameras in Teddy Bears: Electronic Visual Surveillance and the Fourth Amendment*, 58 U.CHI. L. REV. 1045 (1991).

to abuse.⁶⁸ In other words, video surveillance divulges a wide range of private information over a significant period of time, unbeknownst to the target of that surveillance, and could excessively intrude on privacy rights if not kept in check. For that reason, seven federal appellate courts agreed that video surveillance must be subject to the same core constitutional protections as wiretapping.⁶⁹

Because the four factors identified made video surveillance, like wiretapping, particularly susceptible to abuse, the Courts of Appeals imposed those provisions of the Wiretap Act that they viewed as incorporating the Fourth Amendment particularity requirement.⁷⁰ The Courts of Appeals held that as a matter of constitutional law, agents seeking to use video surveillance would need to establish the enhanced probable cause described above.⁷¹ In addition, they would have to demonstrate that video surveillance was to be used as a last resort, because other less intrusive surveillance would not work; they would have to terminate the surveillance as soon as its objective was met, and within 30 days unless the order was extended; they would have to minimize the surveillance of non-incriminating information, and the order would have to particularly describe the place to be searched and the things to be seized.⁷²

⁶⁸ See Freiwald, *supra* note 11 (discussing these cases and characteristics in the wiretap, video surveillance and online context).

⁶⁹ See cases cited *supra* note 20.

⁷⁰ There is some debate as to whether the Wiretap Act provisions that the Courts of Appeal adopted to video surveillance exactly matched the constitutional requirements set out in *Berger*. See *United States v. Koyomejian*, 970 F.2d 536 (9th Cir.) (*en banc*), *cert. denied*, 506 U.S. 1005 (1992) (Kosinski, J., dissenting), Ric Simmons, *Can Winston Save Us From Big Brother? The Need for Judicial Consistency in Regulating Hyper-Intrusive Searches*, 55 RUTGERS L. REV. 547 (2003).

⁷¹ The Wiretap Act requires that a reviewing judge find probable cause to believe the target “is committing, has committed, or is about to commit” a particular enumerated offense and that the surveillance will contain incriminating communications about the offense. See 18 U.S.C. § 2518(3).

⁷² See, e.g., *United States v. Torres*, 751 F.2d 875, 882-884 (7th Cir. 1984); *United States v. Biasucci*, 786 F.2d 504 (2d Cir. 1986); *United States v. Koyomejian*, 970 F.2d 536 (9th Cir.) (*en banc*), *cert. denied*, 506 U.S. 1005 (1992).

Because the federal statutes did not cover silent video surveillance for domestic law enforcement purposes, the courts of appeal wrote on a clean slate.⁷³ Yet while their decisions came after *Katz*, *Miller*, and *Smith*, the Courts of Appeal avoided the reasonable expectation of privacy analysis altogether. Instead, the Courts assessed the characteristics of video surveillance against the characteristics of wiretapping. They extended heightened constitutional privacy protection to targets in a safe house, a warehouse, a backyard, and an apartment building, without deep analysis into what those occupants should have thought about whether they were vulnerable to filming. When it did consider the reasonable expectation of privacy, one court suggested that a more intrusive search, such as one that filmed the inside of a private home, might have to be subjected to even further constraints, such as a ban.⁷⁴

Instead of applying a strained assumption of risk analysis, or settling for a superficial inquiry into whether the targets were somehow subject to view by others, the Courts of Appeal assessed the nature of the surveillance method itself in light of Fourth Amendment values. The Courts considered what impact it would have on society if they were to leave video surveillance, with its high potential for abuse, unregulated. In several of the cases, the courts recalled Orwell's dystopian vision of a surveillance state in their analysis. Were law enforcement agents able to make their own decisions, independent of judicial involvement, about whom to film, when to film, what to film and where to film, that would present an unacceptable risk of an Orwellian state. In sum, the courts shifted

⁷³ Though Congress omitted video surveillance from the ECPA in 1986, the House Report accompanying the Act spoke approvingly of the appellate courts' approach. See H.R. Rep. No. 99-647, at 18 & n.11 (1986) (approving of the approach as an effort to provide "legal protection against unreasonable use of new surveillance techniques"); *id.* at 36 (approving of the court-derived rules); see also Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of E-mail*, 10 MICH. TELECOMM. & TECH. L. REV. 1, 57 (2003) .

⁷⁴ See *Torres*, 751 F.2d at xx.

their focus away from an unmanageable inquiry into just what the targets believed about surveillance they did not know about and considered the nature of the government's surveillance practice in light of the rights the Fourth Amendment was designed to secure.

B. The Four Factor Test

Scholars and judges agree that the Fourth Amendment was designed to prevent the use of general warrants and writs of assistance that the British had abused in the years leading up to the American Revolution.⁷⁵ General warrants provided excessive executive authority to search private places, such as a home, without any particularized reason to believe that the such searches would be fruitful. The Fourth Amendment, from its clear language, requires that whenever warrants are issued, they must be issued on the basis of particularized facts and probable cause. History also establishes the longstanding constitutional mandate that law enforcement officers should not have unfettered discretion to intrude upon private areas, even though such intrusions could yield incriminating information. As the Supreme Court recognized in a case involving domestic wiretapping for national security purposes, “the historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and over look potential invasions of privacy and protected speech.”⁷⁶ As a result, courts have long played a role in confining law enforcement investigative powers within constitutional bounds.

⁷⁵ See, e.g., Amsterdam, *supra* note 37; James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward and Expanded Vision of Fourth Amendment Privacy Province*, 36 HASTINGS L. J. 645 (1985).

⁷⁶ *United States v. United States Dist. Ct.*, 407 U.S. 297 (1972).

It is important to recognize another aspect of the historical record. Both the framers and the Supreme Court have appreciated the need for courts to invalidate, on constitutional grounds, congressional legislation that insufficiently reigns in executive search and surveillance authority. Professor Thomas Davies, in a comprehensive overview of the period leading up to the passage of the Bill of Rights, found that a significant motivation for the Fourth Amendment was the framers' concern that Congress might authorize general warrants by statute.⁷⁷ The framers intended the Fourth Amendment to not only rule out executive branch use of general warrants, but also congressional authorization of such use.⁷⁸ Almost two hundred years later, the Supreme Court realized that vision in *Berger v. New York*, when it struck down a state's wiretapping statute for violating the Fourth Amendment. The Court determined that the legislation's insufficient procedural safeguards meant that it effectively permitted law enforcement agents to use a general warrant for wiretapping.⁷⁹

With that history in mind, courts should subject those laws Congress passes to regulate modern electronic surveillance practice to searching constitutional review. It is wholly inappropriate to defer to Congress' interpretation of what the Fourth Amendment requires; that puts the cart of statutory law before the horse of the constitutional minimums that constrain that law.⁸⁰ Courts must determine for themselves what the Constitution requires before law enforcement investigators may access new electronic communications technologies. Because the technologies themselves, the information

⁷⁷ See Thomas Y. Davies, *supra* note 52, at 619-68.

⁷⁸ See *id.*

⁷⁹ *Berger v. New York*, 388 U.S. 41, 64 (1967).

⁸⁰ Of course it makes even less sense to defer to the executive branch's interpretations of those provisions, particularly when they press for granting law enforcement expansive powers at the expense of constitutional rights.

available, and the methods of its acquisition are all new, courts may not take shortcuts by applying inappropriate analogies. Instead, they must step back and consider the constitutional question with reference to core Fourth Amendment concerns. The four factor test does just that.

The next section discusses how each of the four factors promotes Fourth Amendment values. It uses the four factor test to address whether stored e-mails enjoy the protections of the Fourth Amendment against government demands to produce them. Application of the four factor test to the question posed in the *Warshak* case illustrates the applicability of the test to a pending question about the constitutional regulation of a modern government investigative method.

1. Hidden

It should be obvious that those government searches that proceed in secret have a greater need for judicial intervention and approval than those that do not. Those investigative methods that operate out in the open may be challenged at the time of the search by those who observe it. The target of the search is likely to find out about it, and she in turn can challenge the search in court. Both the target and other observers may pressure law enforcement agents to conform their investigation to whatever legal authority they have, such as a warrant, or to act within appropriate bounds if the investigation does not require a warrant. On the other hand, in the absence of judicial oversight, victims of hidden surveillance must rely on self-disclosure by law enforcement agents of the fact and nature of the surveillance they have undertaken. Surveillance that is hidden therefore requires judicial intervention to ensure that it proceeds only after

appropriate justification, only within justified bounds, and only with proper provision of notice to the target after the fact.

When law enforcement agents demand that ISPs disclose their users' electronic communications, the ECPA permits them to request that those providers keep their compliance secret.⁸¹ In that way, law enforcement acquisition of stored e-mails can be quite hidden, and certainly as hidden as either traditional wiretaps or silent video surveillance. In fact, the target of a traditional wiretap or video surveillance likely has a better chance of discovering that he was targeted than someone whose e-mails are disclosed. Targets of traditional wiretapping and video surveillance could sometimes observe agents installing the device or otherwise detect its presence. But law enforcement agents may obtain stored e-mails from a service provider without coming anywhere near the target himself.

2. Intrusive

The intrusiveness factor identifies those investigations that give law enforcement access to information about people that implicates Fourth Amendment concerns. While the intrusiveness inquiry requires a judgment about levels of intrusiveness, that does not make it entirely open-ended. When the Seventh Circuit first established that video surveillance was intrusive, the courts of appeals that followed did not need to redo the analysis. That the video cameras filmed people's activities in places that were not open to the general public was sufficient for them to be considered intrusive. No individualized inquiry into what the filmed topics were actually doing was necessary.

⁸¹ ECPA cite.

In implementing the intrusiveness factor of the four factor test, courts should assess the richness of the information acquired, and not the physical intrusiveness of the surveillance. *Katz* repudiated the need to have a physical trespass in order to implicate the Fourth Amendment, so a focus on physical intrusions is entirely misplaced. The Courts of Appeal, in evaluating video surveillance, assessed the quality of the information provided by it, and observed that video surveillance yields at least as much information as a wiretap, and likely more. In fact, law enforcement agents used video surveillance in some cases specifically because they worried that they would not be able to gather the evidence they needed using only audio surveillance. They worried that the targets would operate in silence, or against a cover of noise, so that they needed the enhanced record that video surveillance provided.

Because e-mails typically contain more personal data than analogous phone calls or even videos, acquisition of stored e-mail intrudes more on personal privacy than does a wiretap or video surveillance. A simple e-mail message has textual header information that discloses the time it was composed, its subject line and any attachments, and the electronic addresses of the sender, the recipient, any who receive courtesy copies of it. E-mails often include prior messages in their text, and analysis may reveal the computer on which the e-mail was composed, its path through the network, and the times the e-mails are opened, deleted, or forwarded. People reveal in their e-mails more about their political opinions, religious beliefs, personal relationships, intellectual interests, and artistic endeavors than they ever revealed over the telephone. Stored e-mails contain a vast archive of people's past activities.

3. Indiscriminate

Indiscriminate investigations implicate the core concerns of the Fourth Amendment. If law enforcement agents must intrude upon private activities to perform their jobs, that harm is minimized to the extent the investigation reaches no further than necessary to uncover incriminating evidence. For example, in the wiretap context, reports to Congress disclose the percentage of incriminating conversations tapped, so that Congress may monitor whether the executive branch may continue to use such an intrusive, hidden method of investigation. Further, the Constitution requires that government wiretappers minimize the acquisition of non-incriminating communications to reduce the indiscriminate nature of the investigation. The Fourth Amendment strikes a balance between law enforcement's interest in information and society's interest in avoiding a surveillance state. More indiscriminate searches bring us closer to Orwell's dystopian vision.

Because of the extra richness of e-mails as compared to telephone conversations, there is every reason to believe that e-mail surveillance will be just as indiscriminate in the sense that it will disclose information about innocent people or innocent activities. In the *Warshak* case, the plaintiff claims that government agents acquired thousands of his personal e-mails, "without any particularization or limitation as to time frame, parties to the communication, or the subject matter of the communication."⁸² Surveillance activity that can easily acquire information that is not directly related to the search justification requires judicial intervention to minimize the acquisition of non-incriminating communications.

⁸² Warshak, Plaintiff's Motion to Stay Preliminary Injunction at 4 (11/2/06).

4. Continuous

Investigations that run continuously are more likely to be both incriminating and intrusive. It is just a matter of logic that the longer an investigation runs, the more likely it is to rope in innocent communications and the more likely it is to intrude upon the target's privacy. For example, in one case in which law enforcement agents placed video surveillance cameras in a warehouse to uncover evidence of counterfeiting, the tape ran long enough to record a person, apparently unrelated to the suspects, engaging in an intimate sex act.⁸³ The constitutionally-derived limits on the duration of wiretap and video surveillance investigations reflect the concern with overlong surveillance.

As previously discussed, while a wiretap that remains installed over a period of time may acquire a continuous record of the targets' conversations, an e-mail search can accomplish the same thing in a single shot. For example, a wiretapper may obtain a continuous record of a target's communications from January 1 to March 31st by installing a tap on January 1 and running it for three months. To obtain the same record of electronic communications, however, an agent may merely wait until after March 31st and then obtain all e-mail correspondence conducted back to January 1. That the investigation runs retrospectively rather than prospectively does not make it any less continuous. And the fact that e-mail searches may as easily cover long periods of time as short ones compels the need for judicial oversight to ensure they stay within justified limits.

⁸³ See *United States v. Mesa- Rincon*, 911 F.2d 1433 (10th Cir. 1990).

C. Stored E-mail and Other Contexts

The four factor test evaluates those aspects of an investigative method that most implicate the concerns that underlie Fourth Amendment jurisprudence. The test has courts focus where they should -- on the nature of the surveillance, its power, its susceptibility to abuse, and its concomitant need for judicial intervention to keep it within appropriate bounds.

Because acquisition of stored e-mail from a third party system shares all the features of being hidden, intrusive, indiscriminate, and intrusive that wiretapping and video surveillance does, it should be subject to the same heightened constitutional protections. In fact, acquisition of stored e-mail may raise an even stronger case for heightened protection than does acquisition of e-mail in transit, because the former establishes each factor more definitively.

While the previous discussion has evaluated government access to stored e-mail in the hands of third parties, the four factor test may profitably be applied to other types of modern online surveillance. Those investigations that share the four factors should be accorded the highest level of constitutional protection. Though it is currently unlikely that law enforcement agents would choose to intercept real-time e-mails that can be obtained from storage, the analysis should nonetheless apply to real-time acquisition of ephemeral communications that are not stored. By the same token, stored or real-time acquisition of other electronic communications information, besides contents, could well warrant heightened protection.⁸⁴

⁸⁴ See Freiwald, *supra* note 11 (critiquing the content versus non-content split); Susan Freiwald, *Uncertain Privacy: Communications Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (1996) (same).

Those investigatory methods that share only some, but not all, of the four factors could be protected with lesser standards, including the probable cause warrant that law enforcement must generally obtain before searching physical places. Those searches that do not divulge information over a period of time, and so lack the continuity feature, seem the most analogous to a traditional search. For example, demanding information from a service provider about an instance of Internet communication could likely proceed with a simple warrant.

Significantly less intrusive investigations, such as those that acquire static facts about a subscriber, rather than information pertaining to communications, could likely be protected with looser requirements, such as an administrative subpoena or court order based on less than probable cause.

Conclusion

The four factor test that assesses whether law enforcement's proposed investigative method is hidden, intrusive, continuous, and indiscriminate has a lot to recommend it. When courts use it to determine constitutional protections, as the Courts of Appeal did for video surveillance, they focus on those factors that make law enforcement investigations particularly prone to abuse, and therefore most in need of the judicial intervention that constitutional protection provides. Much more so than the reasonable expectations of privacy test, the four factor test offers a workable means to bring modern investigative methods in line with Fourth Amendment rights.