

**THE FOG OF CLOUD COMPUTING: FOURTH AMENDMENT
ISSUES RAISED BY THE BLURRING OF ONLINE AND OFFLINE
CONTENT**

*R. Bruce Wells**

INTRODUCTION

Today you can have ubiquitous access to your data. You can stream one digital copy of your favorite album to your stereo, television, car, computer, and phone. You can retrieve your latest memo from any of the same, or from any PC in the world with an Internet connection. The advantages of such connectivity may seem apparent,¹ but what protection does the Constitution afford your information? Under current law, very little.

The law must adapt to a world where the location of information, the means by which it travels, and the medium in which it resides have dwindling importance. The Constitution protects privacy through the Fourth Amendment,² and this Comment addresses such rights as they apply to data stored online on remote servers—what is known today as the “cloud.”³ The lines between traditional computing and cloud computing are blurring: whether or not you store your data locally or remotely is increasingly irrelevant and indistinguishable, and this advancement exposes a flaw in the Fourth Amendment’s “Reasonable Expectation of Privacy” doctrine.

* J.D. Candidate, University of Pennsylvania Law School, Class of 2010. B.A., English and History & Sociology of Science, University of Pennsylvania, 2006. I would like to thank Professor David Rudovsky for his continued help with this topic.

¹ See, e.g., Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1975, 1980 (2006) (“Generativity denotes a technology’s overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences. . . . [T]he Internet has developed in such a way that it is consummately generative.”). But see Jeff Zeleny, *Lose the Blackberry? Yes He Can, Maybe* N.Y. TIMES, Nov. 16, 2008, at A1 (noting President Obama’s dependency on his Blackberry).

² U.S. CONST. amend. IV (“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause . . .”).

³ See, e.g., Steve Jobs, Chief Executive Officer, Apple Inc., Keynote Address at the World Wide Developers Conference 2008 (June 9, 2008) (explaining MobileMe, Apple’s implementation of “cloud computing,” in which a user stores all of his or her data on Apple’s servers, and has instant access via a Mac, PC, or iPhone).

Part I traces some unwieldy history of the Fourth Amendment. Under the Supreme Court's search and seizure doctrine, police intrusion is not considered a "search" (requiring a warrant and probable cause) if one does not have a reasonable expectation of privacy in the observed property or communication.⁴ For example, officers can read the outside of a mailed envelope, but not its contents.

Part II further explores this muddled case law. Congress made a wide-ranging statutory attempt to set clearer privacy standards for new technologies through the Electronic Communications Privacy Act of 1986 ("ECPA"),⁵ specifically Title II, the Stored Communications Act ("SCA").⁶ These laws determine the government's ability to search data on remote servers. Congress enacted them over two decades ago, but the question of whether email has a reasonable expectation of privacy remains unresolved. Has one "knowingly exposed" her information to the public by storing her email on remote servers, thereby eliminating an objective expectation of privacy? Analogies from court decisions regarding bank and phone records would suggest yes,⁷ which would mean that government intrusions of email do not require a warrant. A recent Sixth Circuit opinion addressed the issue but was vacated on other grounds.⁸

I would like to see such data protected by the Fourth Amendment, and to add to the discussion I analyze a new technological development—the blurring of online and offline applications—that raises a similar but distinct legal question than that raised by email.⁹ Part III of this Comment explains that development, and describes new kinds of technologies offered by Google, the Mozilla Foundation, and others. Part IV then shows how casual computer users might not be able

4 See *Katz v. United States*, 389 U.S. 347 (1967) (holding that the government violated the Fourth Amendment when it eavesdropped without a warrant on a telephone booth conversation).

5 Pub. L. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

6 18 U.S.C. §§ 2701-2712 (2006).

7 See *United States v. Miller*, 425 U.S. 435, 443 (1976) (holding that a bank depositor has no expectation of privacy in bank records because he "takes the risk, in revealing his affairs to another [e.g. the bank], that the information will be conveyed by that person to the Government").

8 See *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007) (holding that email is protected by the Fourth Amendment), *vacated in part*, 532 F.3d 521 (6th Cir. 2008) (en banc).

9 I would like to acknowledge a similar law review note: Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. REV. 1043 (2008). Because both pieces focus on Fourth Amendment protections of electronically stored information, there is necessarily overlap in background information. However, Mr. Oza's Note focuses specifically on email, whereas my Comment expands the issue to include additional kinds of remote data.

to distinguish these new programs from traditional programs. This could result in a reasonable belief that the users' data is on their computers, when it is in fact stored remotely. Such a belief indicates a need for Fourth Amendment protection of this data.

Finally, Part V suggests solutions. Having argued that online data should be protected, I offer three routes that courts could take to so hold. The first follows the current doctrine and attempts to distinguish online data from analogous cases of phone and bank records (neither of which are protected).¹⁰ The second suggests an overhaul of the Fourth Amendment's "reasonable expectation of privacy" doctrine. The third and most radical approach suggests an overhaul of the entire Fourth Amendment doctrine, shifting the focus from privacy to security.

I. BACKGROUND

A. "Searches" Under the Fourth Amendment

In a case involving a potential breach of the Fourth Amendment, we first ask whether a search or seizure has taken place.¹¹ If not, we can ignore whether the action was performed reasonably or was supported by a warrant. Whether it is a search depends on the "reasonable expectation of privacy" standard.

Justice Harlan sowed this rule in his concurrence in *Katz v. United States*.¹² The case asked whether the Fourth Amendment protected phone booth conversations; FBI agents had placed an electronic "bug" on the outside of a public booth in order to record the defendant therein.¹³ The majority declined to frame the issue in terms of a constitutionally protected space, noting that "the Fourth Amendment protects people, not places."¹⁴ It also declined to frame a general "right to privacy."¹⁵ Instead, the majority found a Fourth Amendment violation, but did so without articulating a general rule, noting only

¹⁰ See *Smith v. Maryland*, 442 U.S. 735 (1979) (finding no privacy protections for records of phone numbers dialed); *Miller*, 425 U.S. 435 (finding no privacy protections for bank records including checks and deposit slips).

¹¹ U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable *searches and seizures*, shall not be violated . . .") (emphasis added).

¹² 389 U.S. 347 (1967).

¹³ *Id.* at 348.

¹⁴ *Id.* at 351.

¹⁵ *Id.* at 350–51.

that “[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.”¹⁶

But having a definite rule is critical because a reasonable expectation of privacy not only determines whether a “search” has taken place, but often also determines whether a defendant has standing to challenge an intrusion under the Fourth Amendment.¹⁷ And if a defendant was not “searched” or does not have standing, he cannot access the most powerful weapon against Fourth Amendment violations: the exclusionary rule.¹⁸

B. *The Reasonable Expectation of Privacy Rule*

Harlan’s *Katz* concurrence articulated a test later adopted by the Court to establish a search: “[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”¹⁹

The Supreme Court eventually adopted this as the rule, but not after some uncertainty. For example, in *Oliver v. United States*, the Court held that a police trespass did not constitute a search, despite the fact that the defendant had posted “No Trespassing” signs surrounding a highly secluded and remote area.²⁰ Surely the defendant had an actual, subjective expectation of privacy in such an area, so the Court must have thought that an expectation of privacy in “open fields” is unreasonable to the populace.²¹ Over the years, the Court addressed the privacy question repeatedly, and mostly chipped away at Fourth Amendment protection in a variety of contexts.²² Often,

¹⁶ *Id.* at 359.

¹⁷ *See Rakas v. Illinois*, 439 U.S. 128 (1978) (holding that the exclusionary rule only excludes evidence discovered by a search or seizure that violated the rights of the defendant who invokes it).

¹⁸ *See Mapp v. Ohio*, 367 U.S. 643, 655 (1961) (declaring that “the Fourth Amendment’s right of privacy [is] enforceable against the States through the Due Process Clause of the Fourteenth [Amendment]”); *Weeks v. United States*, 232 U.S. 383 (1914) (holding that evidence seized in violation of the Fourth Amendment should be excluded from use at trial).

¹⁹ *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

²⁰ 466 U.S. 170, 184 (1984).

²¹ *See William C. Heffernan, Fourth Amendment Privacy Interests*, 92 J. CRIM. L. & CRIMINOLOGY 1, 36 (2001) (explaining that “each condition [is] necessary for establishing a valid privacy claim”).

²² *See Florida v. Riley*, 488 U.S. 445, 450–51 (1989) (aerial observation of curtilage not a search); *California v. Greenwood*, 486 U.S. 35, 41 (1988) (no protection for garbage properly put out on the curb); *California v. Ciraolo*, 476 U.S. 207, 214 (1986) (aerial surveillance generally not a search); *Oliver*, 466 U.S. at 183 (open fields not protected, de-

technological developments provided these new contexts, like the privacy interest in the heat emitted from one's home, which police can observe with infrared imaging.²³

Harlan's language returned in two major opinions. The fractured decision in *Florida v. Riley*²⁴ furthered the doctrine but exemplified the confusion. There, a police helicopter flew over a greenhouse and spotted, through two broken roof panels, marijuana growing inside.²⁵ The plurality emphasized that the police flew at a legal altitude, and that therefore "[a]ny member of the public could legally have been flying over Riley's property [at that altitude] and could have observed Riley's greenhouse."²⁶ But Justice Blackmun's dissent noted a common thread woven through a majority of the Court:

Like Justice Brennan, Justice Marshall, Justice Stevens, and Justice O'Connor, I believe that [whether there was a "search"] depends upon whether Riley has a "reasonable expectation of privacy" that no such surveillance would occur, and does not depend upon the fact that the helicopter was flying at a lawful altitude A majority of this Court thus agrees to at least this much.²⁷

The Court reiterated and solidified the rule in *Bond v. United States*.²⁸ Citing *Riley*, it stated: "First, we ask whether the individual, by his conduct, has exhibited an actual expectation of privacy Second, we inquire whether the individual's expectation of privacy is 'one that society is prepared to recognize as reasonable.'"²⁹

spite "No Trespassing" signs); *United States v. Knotts*, 460 U.S. 276, 281 (1983) (no reasonable expectation of privacy in one's car movements); *United States v. Place*, 462 U.S. 696, 710 (1983) (canine "sniff test" not a search); *Smith v. Maryland*, 442 U.S. 735, 745 (1979) (no reasonable expectation of privacy in phone records); *United States v. White*, 401 U.S. 745, 753 (1971) (recordings of conversations with informants not a search); *Hoffa v. United States*, 385 U.S. 293, 303 (1966) (no protection for conversations with informants); *Lopez v. United States*, 373 U.S. 427, 440 (1963) (informant's recording of a conversation not a search); *On Lee v. United States*, 343 U.S. 747, 754 (1952) (informant's secret radio transmission of a conversation not a search). *But see* *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (police use of a device that is not in general public use, to explore details of the home that would be unknowable without physical intrusion, is a search); *Bond v. United States*, 529 U.S. 334, 339 (2000) (manipulation of the exterior of luggage is a search); *United States v. Karo*, 468 U.S. 705, 716 (1984) (automobile tracking becomes a search once an officer continues to monitor the electronic device after defendant has entered his residence).

²³ *See* *Kyllo*, 533 U.S. at 40 (holding that use of such technology was a search).

²⁴ 488 U.S. 445. The opinion had a four-person plurality, a concurrence, and two dissents.

²⁵ *Id.* at 448.

²⁶ *Id.* at 451.

²⁷ *Id.* at 467 (Blackmun, J., dissenting).

²⁸ 529 U.S. 334 (2000) (holding that a search had occurred when an officer squeezed the defendant's luggage to find contraband).

²⁹ *Id.* at 337–38 (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)).

C. *Whether One Has “Knowingly Exposed” Information to the Public*

At the same time, the Court began a secondary line of reasoning that often determined the reasonable expectation of privacy issue. It rested on language, arguably dicta, from *Katz*: “What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”³⁰ This makes sense. For example, if one were to leave contraband in plain view of the street, even if it were behind glass and inside the home, a sighting of such would not be a search.³¹

In *United States v. White*,³² the Court expanded the meaning of knowing exposure. There a hidden agent, with his informant’s consent, overheard a conversation between the informant and defendant.³³ The agent radioed the speech to another agent outside.³⁴ The Court, drawing on precedent of cases involving informants,³⁵ held that “[i]f the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations.”³⁶ The Court stretched “knowing exposure” even further in *California v. Greenwood*.³⁷ There, investigators asked the neighborhood’s regular trash collector to pick up the defendant’s trash at the curb. The trash collector then assisted by separating the defendant’s trash for systematic search.³⁸ The Court held that the defendants “exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection.”³⁹

“Knowing exposure” means not only that which a person exposes to friends (potential informants) or to the public (like trash on the curb). It also includes that which one systematically exposes to an institution. Two such cases are especially relevant to this Comment because of the analogies that one can draw between them and the institutions of cloud computing.

³⁰ *Katz v. United States*, 389 U.S. 347, 351 (1967).

³¹ *See, e.g., Minnesota v. Carter*, 525 U.S. 83, 103 (1998) (Breyer, J., concurring) (discussing how, because the contraband in question in that case was viewable “from a public area outside the curtilage of the residence,” such a sighting did not violate the defendant’s Fourth Amendment rights).

³² 401 U.S. 745 (1971).

³³ *Id.* at 746–47.

³⁴ *Id.*

³⁵ *See, e.g., Hoffa v. United States*, 385 U.S. 293 (1966).

³⁶ *White*, 401 U.S. at 752.

³⁷ 486 U.S. 35 (1988).

³⁸ *Id.* at 37–38.

³⁹ *Id.* at 40.

In *United States v. Miller*,⁴⁰ the Court considered bank records. The defendant used a bank which later assisted in his prosecution.⁴¹ The Court held that a bank depositor has no expectation of privacy in bank records, reasoning that he “takes the risk, in revealing his affairs to another [i.e. the bank], that the information will be conveyed . . . to the Government.”⁴² And in *Smith v. Maryland*, police recorded the phone numbers dialed by a suspect.⁴³ The Court doubted “that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must ‘convey’ phone numbers to the telephone company.”⁴⁴ But does it follow that they realize the exposure to warrantless searches?

II. PROBLEMS WITH THE CASE LAW, A RESPONSE BY CONGRESS, AND THE DOCTRINE TODAY

A. Searches Involving Current Technology

Applying these rules to situations outside the physical world can be difficult. We now live in a world populated as much by bytes as it is by people. For example, what does it mean for data to be knowingly exposed when it is stored on a computer? Does it matter if it is displayed on the monitor, or if it can be accessed with just a few mouse clicks? What if the data is encrypted, or requires a password to access? Taking the idea of knowing exposure as literally as possible, what if the computer or the hard drive is deposited as trash on the curb?

Such questions highlight the complexity of searches in this area. In his comprehensive article, *Searches and Seizures in a Digital World*, Orin Kerr tackles these issues.⁴⁵ He suggests that we can make some analogies to searches in the physical world, like taking the Fourth Amendment’s heightened protection of the home and applying it to the computer.⁴⁶ Since an Internet-connected personal computer is

⁴⁰ 425 U.S. 435 (1976).

⁴¹ *Id.* at 437–38.

⁴² *Id.* at 443.

⁴³ 442 U.S. 735, 737 (1979).

⁴⁴ *Id.* at 742.

⁴⁵ 119 HARV. L. REV. 531 (2005).

⁴⁶ *Id.* at 538.

the portal to one's home in the digital world, we can take the notion of "home as castle" and extend it towards "hard drive as castle."⁴⁷

But there are problems with leaving it up to the courts to move this doctrine into the digital world. We have seen the Fourth Amendment's piecemeal growth, and the whimsical definition of "reasonableness." For example, Justice Souter's dissent in *Illinois v. Caballes*⁴⁸ pointed out a flaw in the majority's reasoning: "The [holding] rests . . . [on a premise] that experience has shown to be untenable, the assumption that trained sniffing dogs do not err. . . . The infallible dog, however, is a creature of legal fiction."⁴⁹ Such per se rules, like those concerning open fields,⁵⁰ can dismiss Fourth Amendment protection even when a defendant had what many would consider a perfectly reasonable expectation of privacy.

And technology can only make things more confusing. For example, in *Kyllo v. United States*,⁵¹ the Court dealt with a novel style of investigation. Police used a thermal imager to examine the amount of heat emanating from a suspect's home.⁵² The Court held that where the government uses a device that is "not in general public use," the surveillance is presumptively a search.⁵³ This raises the question: which technologies are "in general public use"? Today one can affordably purchase infrared equipment at many sporting goods stores.

While privacy advocates may see *Kyllo* as a ray of hope, it highlights how abruptly the case law can change course. Other problems with case law include the need to educate the judiciary regarding nascent technologies, and the need for a case or controversy before the doctrine can be furthered through judicial opinions.

B. A Solution by Congress: the Electronic Stored Communications Act

In 1986 Congress enacted the Electronic Communications Privacy Act⁵⁴ to comprehensively confront privacy in the digital age. Section 2703 of the ECPA, part of the Stored Communications Act,⁵⁵ allows a

47 The recent developments of offline/online applications require an expansion of this protection to include not only local hard drives, but also remote storage mediums, as discussed *infra* Part III.

48 543 U.S. 405 (2005) (holding that a dog sniffing for drugs was not a search).

49 *Id.* at 410–11 (Souter, J., dissenting).

50 *See* *Oliver v. United States*, 466 U.S. 170 (1984).

51 533 U.S. 27 (2001).

52 *Id.* at 29–30.

53 *Id.* at 34.

54 Pub. L. 99–508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

55 18 U.S.C. §§ 2701–2712 (2006).

court to order an Internet Service Provider (“ISP”) to turn over emails and other electronic records, without notifying the suspect, if they have resided on an external server for more than 180 days.⁵⁶ It has yet to be challenged under the Fourth Amendment in the Supreme Court.

C. *Warshak v. United States*

Whether email has a reasonable expectation of privacy is still unresolved. The most recent major case on point is *Warshak v. United States*,⁵⁷ last argued before the Sixth Circuit in mid-2008. It challenged section 2703(d) as violating the Fourth Amendment.⁵⁸

The initial Circuit panel held that “individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP.”⁵⁹ One of the factors that the panel weighed was the type of agreement that a given user had with his or her ISP.⁶⁰ The court upheld a preliminary injunction of the government from “seizing . . . the contents of any personal e-mail account” unless the government provides prior notice to the e-mail user or shows that the user has no reasonable expectation of privacy vis-à-vis the ISP.⁶¹ In effect, the court held that section 2703(d) was unconstitutional.⁶²

However, the panel was soon reversed en banc.⁶³ There the Circuit avoided the ECPA issue by reversing on other grounds.⁶⁴ Thus, protection for email remains uncertain.

III. THE TECHNOLOGICAL DEVELOPMENTS OF “BLURRING”

Technology can conflate the contexts of our lives. For example, it is becoming increasingly difficult to separate work information from personal information, as people take their laptops and Blackberries

⁵⁶ 18 U.S.C. § 2703 (2006).

⁵⁷ 532 F.3d 521 (6th Cir. 2008) (en banc) (vacating in part 490 F.3d 455 (6th Cir. 2007)).

⁵⁸ 490 F.3d at 460–61.

⁵⁹ *Id.* at 473.

⁶⁰ *Id.* at 475.

⁶¹ *Id.*

⁶² *See id.* (“[S]ubpoenaing the entity with mere custody over the documents is insufficient to trump the Fourth Amendment warrant requirement.”).

⁶³ *Warshak v. United States*, 532 F.3d 521 (6th Cir. 2008).

⁶⁴ *See id.* at 525 (holding that the claim was not yet ripe for adjudication).

home with them.⁶⁵ Even more radically, personal identity can become blurred, as people spend more time online, often using aliases and alternate personas.⁶⁶ But two types of blurring are especially relevant to the application of the Fourth Amendment and section 2703(d) to digitized data: the blurring of online and offline applications, and the blurring of what we consider to be communications.

A. *The Blurring of Online and Offline Applications*

Most computer users know that offline applications—traditional programs like Microsoft Word, Adobe Photoshop, etc.—reside on their hard drives, along with all the applications' associated data. Online applications—webmail, Google Documents, Yahoo Calendar, etc.—store their information in the “cloud”: the entire application and its associated data reside on remote servers owned by providers like Microsoft and Google. The idea behind the cloud is that users seem to save and access their information to and from the ether: no matter where they are, they can conjure up what they need. Users do not need to know or see the physical medium in which their data is stored; the content becomes entirely independent of the hardware. Cloud computing is greatly building up steam, with Apple launching its MobileMe service,⁶⁷ Google enabling offline access to potentially any kind of online application,⁶⁸ and the largest distribution of Linux advancing a new cloud computing initiative.⁶⁹

65 See William A. Herbert, *The Electronic Workplace: To Live Outside the Law You Must Be Honest*, 12 EMP. RTS. & EMP. POL'Y J. 49 (2008) (examining legal issues pertaining to the use of Internet and email use at work).

66 See, e.g., Paul Ham, *Warrantless Search and Seizure of E-Mail and Methods of Panoptical Prophylaxis*, 2008 B.C. INTELL. PROP. & TECH. F. & J. 090801 (discussing the differences between the perception of privacy and the actual privacy of e-mail communication).

67 See Steve Jobs, CEO, Apple, Keynote Address at the World Wide Developers Conference 2008 (June 9, 2008). Here Jobs announced Apple's MobileMe service. It automatically synchronizes contacts, calendars, emails, and photos between a user's computer, iPhone, and the Internet. All of the user's data is stored on remote servers, and is accessible through several types of user-friendly portals.

68 In May 2007, Google introduced an open platform called Google Gears. See Aaron Boodman and Erik Arvidsson, *Gears API Blog: Going Offline with Google Gears*, GEARS API BLOG, May 30, 2007, <http://gearsblog.blogspot.com/2007/05/posted-by-aaron-boodman-and-erik.html>. Developers of online applications can employ this platform to enable users to access their information regardless of whether their computer has an Internet connection. Gears does this by copying information from the cloud and storing a copy on the user's hard drive. If the Internet connection fails, applications can seamlessly switch into “offline mode” and the user can continue to edit her data with little variation in usage.

69 See Posting of Mark Shuttleworth, mark@ubuntu.com, to ubuntu-devel-announce@lists.ubuntu.com, <https://lists.ubuntu.com/archives/ubuntu-devel-announce>

The issue I would like to address is the merging of these two types of technology. In September 2008, Google introduced its new web browser, Chrome,⁷⁰ which gained very favorable reviews from the outset.⁷¹ With Chrome, a user can “create” a desktop version of any on-line application. In his review of Chrome, David Pogue of *The New York Times* described that process as follows:

When you click [the “Create application shortcuts” command], the corresponding site opens without the usual address bar and buttons—in other words, it now works exactly like a regular desktop program. For services like Gmail or blogging software,⁷² this feature further blurs the line between online and offline software.

He concluded his review by noting that, with Chrome, Google is building a platform for running software, which may “de-emphasiz[e]” traditional operating systems.⁷³ This would consequently downplay the traditional PC in favor of the cloud. In fact, Google has recently announced a forthcoming, entirely cloud-based operating system based on Chrome.⁷⁴

In many ways, online applications have already become almost indistinguishable from their offline counterparts. Chrome and similar projects such as Mozilla Prism⁷⁵ seek to completely integrate online applications with the desktop. Some online applications, like Microsoft’s online version of Outlook, look just like their desktop counterparts, pixel for pixel. But while people using email must realize that their message travels over the Internet and through an ISP’s servers, it is likely that many people using an online calendar or online documents do not realize that their information is on a remote server rather than on their computer.

/2008-September/000481.html (Sept. 8, 2008) (“Another goal is the the [sic] blurring of web services and desktop applications.”). However, the idea of cloud computing has been around for a while. See, e.g., John Markoff, *An Internet Critic Who Is Not Shy About Ruffling the Big Names in High Technology*, N.Y. TIMES, Apr. 9, 2001, at C6 (“For Microsoft, the idea behind Net is software programs that do not reside on any one computer but instead exist in the ‘cloud’ of computers that make up the Internet.”).

70 Press Release, Google, Google Chrome: A New Take on the Browser (Sept. 2, 2008), available at http://www.google.com/intl/en/press/pressrel/20080902_chrome.html.

71 See, e.g., Walter S. Mossberg, *Google Redefines Web Browser*, WALL ST. J., Sept. 3, 2008, at D1 (“Chrome is a smart, innovative browser, but this first version is rough around the edges.”).

72 David Pogue, *Serious Potential in Google’s Browser*, N.Y. TIMES, Sept. 3, 2008, at C1.

73 *Id.*

74 Google, *Introducing the Google Chrome OS*, THE OFFICIAL GOOGLE BLOG, July 7, 2009, <http://googleblog.blogspot.com/2009/07/introducing-google-chrome-os.html>.

75 Prism, introduced in October 2007, is an add-on for Mozilla’s free, open-source browser, Firefox, which acts very much like Chrome’s desktop application feature. See Mozilla Labs, *Introducing Prism* (Oct. 24, 2007), <http://labs.mozilla.com/2007/10/prism/>.

The central issue is, therefore, whether a user has a reasonable expectation of privacy in content that she sensibly believes is on her computer's hard drive, when it in fact may be located on a remote server. That belief will become increasingly reasonable as developers continue to make online and offline applications indistinguishable. And such is the trend across cloud providers who wish to thereby make the cloud experience more familiar and enjoyable.⁷⁶

B. The Blurring of "Communications"

Over the past decade, the Internet has undergone another major shift: towards "Web 2.0," an increasingly interactive, information-sharing Internet. Web projects like Wikipedia depend on the collaboration of millions of different users to generate content.⁷⁷ Sites like Flickr make it easy for users to share photos and pool their work using tags.⁷⁸ And social networking sites like Facebook allow people to edit their friends' pages.⁷⁹ Sharing information, with dozens or millions of people, is becoming second nature on the Internet.

With such applications, it can be tricky to define what exactly a "communication" is in "Web 2.0." If I publicly post a graphic to Flickr and someone else tags it as a "goat," have we, together, communicated the idea of a goat to others? If I share my online calendar with others, and add a personal event to it, have I communicated with them, even if the event is posted for my sole benefit? If my calendar automatically emails me a reminder of an upcoming event, is that technically a communication? None of these examples is as cut-and-dry as ordinary email. Email is clearly a communication; its purpose is to send a message to someone else. With these other examples, communication with others may be incidental, collateral, or an after-thought. The ECPA should more precisely define "communications" to reflect these issues.

⁷⁶ See Stephen Baker, *Google and the Wisdom of the Clouds; A Lofty New Strategy Aims to Put Incredible Computing Power in the Hands of Many*, BUSINESSWEEK, Dec. 24, 2007, at 48 (noting Google's goals "to organize the world's information and make it universally accessible").

⁷⁷ See Wikipedia, *Five Pillars*, http://en.wikipedia.org/wiki/Wikipedia:Five_pillars (last visited Oct. 3, 2009) ("Wikipedia is free content that anyone may edit . . .").

⁷⁸ See Flickr: *Tour*, <http://www.flickr.com/tour/share/> (last visited Oct. 3, 2009) ("With millions of users, and hundreds of millions of photos and videos, Flickr is an amazing photographic community, with sharing at its heart.").

⁷⁹ See Facebook, <http://www.facebook.com/facebook?ref=pf#/facebook?v=info&viewas=0> (last visited Oct. 3, 2009) ("Facebook's mission is to give people the power to share and make the world more open and connected. Millions of people use Facebook everyday to keep up with friends, upload an unlimited number of photos, share links and videos, and learn more about the people they meet.").

IV. WHY THE CONSTITUTION SHOULD PROTECT INFORMATION IN ONLINE APPLICATIONS

A. *Two Hypotheticals and the Reasonable Expectation of Privacy*

Imagine that a young, tech-savvy teenager wants to set up a new computer for his decidedly analog uncle. He knows that computers are heading the way of the cloud, and that online applications are often free. Accordingly, he buys a computer with Google's forthcoming operating system, populating the entire desktop exclusively with online applications. The computer is always connected to the Internet.⁸⁰ His uncle then begins using the computer, taking full advantage of the applications for his calendar, documents, spreadsheets, email, and so on. It is quite possible—even reasonable—for him to mistakenly assume that all of the data is on his hard drive, safely within the confines of his home and under the full protection of the Fourth Amendment.

Now imagine another teenager and her aunt. This teen is aware of cloud computing, but cares more about her aunt's privacy, and so she opts to set up a traditional desktop system. All of her aunt's applications and data reside on her hard drive, and her aunt, correctly, believes that her data is stored in her house. The aunt has the full protection of the Fourth Amendment. The uncle, under the ECPA, does not.

These two hypothetical situations show how the law can treat identical front-ends disparately. The uncle would have a reasonable, though mistaken, belief that he has not "knowingly exposed" his data to the public.⁸¹ These divergent expectations illustrate complications inherent in applying the law to emerging technologies.

⁸⁰ This is ever more feasible and common. Not only are broadband modems connected continuously, but laptops are increasingly coming bundled with wireless cards with cellular capabilities and plans from providers like Verizon and AT&T. See, e.g., Verizon Wireless—Mobile Broadband—Overview—What Is Mobile Broadband?, <http://www.verizonwireless.com/b2c/mobilebroadband/> (last visited Oct. 3, 2009) ("Mobile Broadband service from Verizon Wireless lets you browse the Internet, download files and access email from your notebook."). Such a computer could remain online anywhere with cellular reception. *Id.* ("Our growing high-speed network covers more than 90% of the U.S. population—more than 280 million people in 259 major metropolitan areas and 250 primary airports in the U.S.—so you can stay connected even when you're on the go.")

⁸¹ Arguably the defendant in *Oliver v. United States*, 466 U.S. 170 (1984), also had a reasonable belief that his fields, secluded and surrounded by "No Trespassing" signs, were private. See *supra* notes 20–21 and accompanying text.

B. Policy Reasons for More Privacy in This Area

There is already a mountain of scholarship arguing the merits of differing degrees of privacy in our society.⁸² The focus of various arguments ranges from fears that the police will abuse high-tech surveillance,⁸³ to concerns over our society's heightened need to monitor terrorism.⁸⁴ However, I will raise a brief point particular to cloud computing: failing to acknowledge an expectation of privacy in off-line applications can disadvantage people less familiar with computers, which includes the elderly and less affluent populations.⁸⁵

What is "reasonable" must include the perspectives of these groups. While they are a minority of the online population, they are rapidly expanding their share.⁸⁶ The current economic climate is forcing the price of personal computers to plummet.⁸⁷ Additionally, consumers are now flocking to "netbooks": cheap computers that are designed primarily for web surfing.⁸⁸ These developments will cause a growing number of inexperienced PC users to work extensively with online applications. They are less likely to understand how and where their data is stored, and their reasonable expectation that their data is private should be protected.

82 See, e.g., Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 519–22 (2007) (discussing a policy model of Fourth Amendment law); Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1 (1991) (describing the debate over the pros and cons of disclosure and openness); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 115 (2008) (arguing that the "privatization" of the Fourth Amendment "fails to do justice to its text"); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 539–49 (2006) (discussing blackmail, appropriation, and other problems associated with increased accessibility).

83 See generally Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9 (2004).

84 See Seth F. Kreimer, *Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War on Terror*, 7 U. PA. J. CONST. L. 133, 133–38 (2004) (describing efforts in the "war on terrorism" to increase information sharing across government agencies).

85 See Ann Bartow, *Open Access, Law, Knowledge, Copyrights, Dominance and Subordination*, 10 LEWIS & CLARK L. REV. 869, 870 (2006) (noting that wealthy people have more frequent and faster access to the Internet than poorer people); Eric L. Carlson, Note, *Phishing For Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting Them Follow*, 14 ELDER L.J. 423, 426–33 (2006) (noting that the elderly population's adoption of computers makes them more of a target for fraud).

86 See Carlson, *supra* note 85, at 425–26 (noting that "[o]lder Americans are going online in record numbers").

87 See Bruce Einhorn, *Acer's Game-Changing PC Offensive*, BUSINESSWEEK, Apr. 20, 2009, at 65 (discussing how the manufacturer Acer uses cutthroat pricing to gain market share).

88 Brad Stone & Ashlee Vance, *\$200 Laptops Break a Business Model*, N.Y. TIMES, Jan. 26, 2009, at B1 (raising the point that today's current economic climate is creating a tipping point where people will begin flocking to netbooks and free online applications).

V. THREE MODELS FOR FOURTH AMENDMENT PROTECTION OF ONLINE APPLICATIONS

Having surveyed the doctrine and argued that we should protect our online and offline data from warrantless searches, I now turn to three ways in which the law can defend that right. The first is through use of the current doctrine; despite *Smith v. Maryland*⁸⁹ and *United States v. Miller*,⁹⁰ an argument can be made that an expectation of privacy in online data, given its blurring with offline data, is reasonable. The second is to overhaul the reasonable expectation of privacy doctrine, clarifying it as not one but several standards, with *Smith* and *Miller* falling under a different standard than the standard under which cloud computing cases could fall. Finally, some have argued that the Fourth Amendment as a whole should be overhauled. Online data could be protected under an entirely new doctrine.

A. *Protection Under the Current Doctrine*

Under the current framework, courts could protect cloud data by distinguishing it from bank and phone records. *Miller* and *Smith* do not necessarily control the issue at hand, because storing one's data on a remote server is not "doing business" in the way that one interacts with a bank, nor is an IP address analogous to a telephone number, since the former is less understood in the populace.

However, a split from past doctrine might be more beneficial. The ECPA highlights a fundamental flaw with the doctrine, especially because it has gone unchallenged for so long. A drastic overhaul of either the reasonable expectation of privacy doctrine, or of the Fourth Amendment as a whole, could greatly clarify and heighten protections for communications.

B. *An Overhaul of the Reasonable Expectation of Privacy Doctrine*

As many commentators have noted, privacy "is a concept in disarray."⁹¹ Not only is the idea spread across several bodies of law,⁹² the Court has interpreted the concept in unpredictable ways. The "reasonable expectation" doctrine itself is prone to a serious problem of circularity. The judiciary can declare an expectation "reasonable," and then that expectation trickles down to the general population

89 442 U.S. 735 (1979); *see supra* notes 43–44 and accompanying text.

90 425 U.S. 435 (1976); *see supra* notes 40–42 and accompanying text.

91 Solove, *supra* note 82, at 477.

92 *Id.* at 483 (noting privacy interests in tort, property, and evidence law).

where it eventually becomes reasonable, regardless of whether it actually was reasonable to begin with.⁹³ The unpredictability and arbitrariness of the doctrine is equally distressing.⁹⁴

However, clarity can be achieved and seemingly inconsistent results can be harmonized if we attempt to break down the Supreme Court's rulings into distinct categories with different standards of "reasonableness." Professor Kerr has attempted to do so by breaking down the approaches of the Court into four models of Fourth Amendment Protection: the probabilistic model (considering the likelihood that information will become known to others or the police), the private facts model (asking whether the government's conduct reveals particularly private or personal information), the positive law model (considering whether a government search interferes with property rights or other legal standards), and the policy model (which asks whether a particular type of police conduct should be regulated).⁹⁵

These models provide flexibility for the Court to distinguish between invasions that are "reasonable per se" and invasions that are "reasonable only if the government has a countervailing interest such as probable cause."⁹⁶ The advantage of making this distinction using four different models is that the Court, when confronted with a novel case, can pick whichever model provides the best proxy for determining whether a particular police activity is troublesome.⁹⁷

Smith and *Miller* were decided under the probabilistic model: "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."⁹⁸

However, as exposure of information becomes less "knowing," as it does as online and offline content increasingly blur, the probabilistic model provides a less exact proxy. In such cases, the Court can resort to the private facts model, which it has done when considering new technologies.⁹⁹ Under such a model, courts would likely find

93 See Rubinfeld, *supra* note 82, at 106–07 (explaining the circularity problem in detail).

94 See discussion *supra* Part II.

95 Kerr, *supra* note 82, at 506.

96 *Id.* at 525.

97 *Id.* at 543.

98 *United States v. Miller*, 425 U.S. 435, 443 (1976) (citing *United States v. White*, 401 U.S. 745, 751–52 (1971)); see *Smith v. Maryland*, 442 U.S. 735, 744 (1979) ("[P]etitioner assumed the risk that the [phone] company would reveal to police the numbers he dialed.").

99 See Kerr, *supra* note 82, at 544 ("[T]he private facts model works independently of the technology and thus permits a stable rule that remains constant as technology changes.

that email, and other data stored in the cloud, will likely contain facts of the most private kind. They could therefore find a reasonable expectation of privacy in online applications without disturbing *Smith* or *Miller*.

C. An Overhaul of the Entire Fourth Amendment

As just demonstrated, maintaining the current regime of privacy requires considerable intellectual gymnastics. One might instead ask whether the Fourth Amendment should focus on privacy at all, given that neither it, nor any other part of the Constitution, mentions the word “privacy.”¹⁰⁰ Academics have called for an overhaul of the Fourth Amendment that focuses on other concepts that are more explicit in the text, such as liberty and security.¹⁰¹

Professor Rubenfeld argues that the Fourth Amendment explicitly states that security should be the focus of the doctrine.¹⁰² He notes the problems of circularity,¹⁰³ the flaws in a legal concept of privacy based on widely shared social expectations,¹⁰⁴ and the untenability of the Stranger Principle.¹⁰⁵ and develops a test to replace the reasonable expectation of privacy test. His test of “generalizability” asks whether a given state practice, such as wiretapping, would become oppressive if enacted extensively and in a manner similar to the abhorrent general warrant of colonial times.¹⁰⁶

Given that, it should be unsurprising that the Supreme Court gravitated towards the private facts model in cases that involve technological surveillance.”); *see also, e.g.*, *Kyllo v. United States*, 533 U.S. 27 (2001) (dealing with a novel style of investigation, use of a thermal imager to examine the amount of heat emanating from a suspect’s home, and holding that where the government uses a device that is “not in general public use,” the surveillance is presumptively a search).

¹⁰⁰ *See* U.S. CONST. amend. IV.

¹⁰¹ *See, e.g.*, Rubenfeld, *supra* note 82, at 104 (urging a shift to a focus on security).

¹⁰² Rubenfeld, *supra* note 82, at 104 (“The Fourth Amendment does not guarantee a right of privacy. It guarantees—if its actual words mean anything—a right of *security*.”). The Fourth Amendment states: “The right of the people to be *secure* in their persons, houses, papers, and effects . . . shall not be violated.” (emphasis added).

¹⁰³ *See supra* note 93 and accompanying text.

¹⁰⁴ *See* Rubenfeld, *supra* note 82, at 107–09 (noting that the “social expectations” of privacy in a given situation will always depend on specific facts about the situation and the people involved).

¹⁰⁵ *Id.* at 131 (arguing that “the Stranger Principle is completely untenable. It implies that, once an individual has exposed information to a third party, the government may seize that information—*with or without* that third party’s assistance”).

¹⁰⁶ *See id.* (“A single arrest on suspicion may have a negligible or nonexistent effect on popular security. But a general warrant is different. It is, precisely, a warrant authorizing the police to arrest or invade homes *generally* on mere suspicion.”).

The facts of *Katz* are clearly an invasion under this test, since a systematically and pervasively wiretapped populace would certainly feel less secure from, and more oppressed by, the State. A search of on-line material is similarly impermissible under this test, since a systematic search of the general population's online information would be equally oppressive.

Of course, the interest sought to be protected in both *Smith* and *Miller* could also potentially be impermissible under the generalizability test: would public discourse and feelings of security be crushed by systematic searches of bank records and phone numbers? One could argue either way, but there is no doubt that current case law would be greatly unsettled by the adoption of the generalizability test at the expense of the privacy doctrine.

VI. CONCLUSION

A discussion of such a radical overhaul should give us pause—a chance to ask what the Fourth Amendment currently protects, and what it should protect. We have come a long way from the enactment of the Bill of Rights, when government agents were only concerned with “persons, houses, papers, and effects.”¹⁰⁷ While emails have been around for a while, this blurring of online and offline applications is relatively new, and computing will continue in this direction for the foreseeable future. The complete integration of web applications into the desktop, through the likes of Google Chrome and Mozilla Prism, is a young phenomenon.¹⁰⁸

Eventually, the Court will address the question of the protection of email. I urge that the blurred and nascent landscape of online applications be included in the discussion. That phenomenon will grow to include an ever greater range of information, and the protections afforded it by the Fourth Amendment should be seriously considered.

¹⁰⁷ U.S. CONST. amend. IV.

¹⁰⁸ Chrome is just a year old. See Google, *A Fresh Take on the Browser*, THE OFFICIAL GOOGLE BLOG, Sept. 1, 2008, <http://googleblog.blogspot.com/2008/09/fresh-take-on-browser.html> (announcing Chrome's launch). Prism is in beta and is still not yet widely implemented. See Mozilla Labs, *Introducing Prism* (Oct. 24, 2007), <http://labs.mozilla.com/2007/10/prism/> (outlining the goals of the Prism beta releases).