

**NELCO**  
**NELCO Legal Scholarship Repository**

---

New York University Public Law and Legal Theory  
Working Papers

New York University School of Law

---

6-1-2011

# Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change

Katherine J. Strandburg  
*NYU School of Law*, [strandburg@exchange.law.nyu.edu](mailto:strandburg@exchange.law.nyu.edu)

Follow this and additional works at: [http://lsr.nellco.org/nyu\\_plltwp](http://lsr.nellco.org/nyu_plltwp)

 Part of the [Computer Law Commons](#), [Constitutional Law Commons](#), [Criminal Law Commons](#), [Internet Law Commons](#), [Law and Society Commons](#), and the [Science and Technology Commons](#)

---

## Recommended Citation

Strandburg, Katherine J., "Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change" (2011). *New York University Public Law and Legal Theory Working Papers*. Paper 283.  
[http://lsr.nellco.org/nyu\\_plltwp/283](http://lsr.nellco.org/nyu_plltwp/283)

This Article is brought to you for free and open access by the New York University School of Law at NELCO Legal Scholarship Repository. It has been accepted for inclusion in New York University Public Law and Legal Theory Working Papers by an authorized administrator of NELCO Legal Scholarship Repository. For more information, please contact [tracy.thompson@nellco.org](mailto:tracy.thompson@nellco.org).

## HOME, HOME ON THE WEB AND OTHER FOURTH AMENDMENT IMPLICATIONS OF TECHNOSOCIAL CHANGE

KATHERINE J. STRANDBURG\*

Moira wakes up in the one-bedroom apartment she shares with a roommate. She makes up the sofa bed she sleeps on in the living room and says good morning to her roommate, who is heading out the door. It is not quite time to leave for work, so she reads a novel on her Kindle for a few minutes before going online to check the weather, to look at her web-based calendar, and to check her e-mail. On her way to work, she listens to her iPod and stops at a favorite coffee shop, using her smart phone to check Foursquare just in case any of her friends are in the vicinity and want to join her for a latte. At work, Moira uses a cloud computing service to collaborate with colleagues in another state on drafting a report. During lunchtime, she orders food delivered to the office and spends some time catching up with family and friends on Facebook. She responds to her sister's wall post about Thanksgiving plans, joins a political debate with some acquaintances, posts the latest pictures from her vacation, and sends a private message to her boyfriend, who lives in another city, suggesting that they stream the same movie from Netflix that evening while simultaneously video chatting via Skype. She also posts a link to a review of a play she is interested in seeing, customizes the post so that it is visible to a Friend List she has made called "Going Out Friends," and asks whether any of those friends want to attend it the following evening. While she is online, she sees that she has two friend requests—one from a high school friend she has not seen in ten years and one from a guy she met briefly at a party last week. She "accepts" the request from the high school friend and "ignores" the request from the party guy. Meanwhile, a couple of people have responded to her post about the play. They make plans to meet after work for dinner and to go to the play. Moira posts that she will go on Yelp to find a restaurant close to the theater and will text everyone the location after work the following day. When Moira leaves a couple of days later to spend the weekend with her boyfriend, she takes her laptop, her smart phone, her iPod, and her Kindle with her. The Fourth Amendment protects Moira's

---

\* New York University School of Law. I am grateful to the participants in the NYU Faculty Workshop and the NYU Privacy Research Group, and especially to Erin Murphy, Samuel Rascoff, Stephen Schulhofer, and Jason Schultz for helpful and insightful comments. Jaime Madell provided invaluable research assistance. Finally, I acknowledge the generous support of the Filomen D'Agostino and Max E. Greenberg Research Fund.

sleeping space in the living room from warrantless government intrusions. But what of the rest of her life?

## I. INTRODUCTION

The first decade of the twenty-first century was bookended by the Supreme Court's two most recent attempts to deal with the effects of advancing technology on the law of search and seizure under the Fourth Amendment.<sup>1</sup> Both opinions notably recognize the importance of interpreting the law so as to maintain the Amendment's protection against government intrusions into personal life in the face of technological changes, yet they illustrate very different perspectives on how that should be done.

In *City of Ontario v. Quon*,<sup>2</sup> the Supreme Court faced the question of whether the Fourth Amendment protects a police officer's text messages to his girlfriend from a search by his government employer.<sup>3</sup> The factual situation was complicated by the government employment context. As a result, the unanimous holding that the search was reasonable focused on the impact of office policies about the use of the government-provided pager,<sup>4</sup> and the Court avoided deciding whether the officer had a reasonable expectation of privacy in the messages.<sup>5</sup> Nonetheless, in a part of the opinion joined by every Justice except Justice Scalia, the Court mused at length upon the reasonable expectation of privacy question.<sup>6</sup>

That discussion is notable in at least three respects. First, in a manner reminiscent of the Court's recognition of "the vital role that the public telephone has come to play in private communication" in the seminal case *Katz v. United States*,<sup>7</sup> the Supreme Court emphasized the social role played by text message communications, noting:

Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.

---

1. See *City of Ontario v. Quon*, 130 S. Ct. 2619, 2624 (2010) (considering whether the Fourth Amendment protects "text messages sent and received on a pager [an] employer owned and issued to an employee"); *Kyllo v. United States*, 533 U.S. 27, 29 (2001) (considering "whether the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a 'search' within the meaning of the Fourth Amendment").

2. 130 S. Ct. 2619.

3. *Id.* at 2624–26.

4. *Id.* at 2624–25, 2633.

5. *Id.* at 2632.

6. *Id.* at 2629–30.

7. 389 U.S. 347, 352 (1967).

... Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own.<sup>8</sup>

Second, the Court expressed discomfort with its role as arbiter of the place of new technologies in social life:

The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. In *Katz*, the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. It is not so clear that courts at present are on so sure a ground. Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.<sup>9</sup>

Third, and perhaps most remarkable in light of scholarly consternation about the possibility that the “third party doctrine” might deprive virtually all digital communications of Fourth Amendment protection,<sup>10</sup> the Court

---

8. *Quon*, 130 S. Ct. at 2629–30.

9. *Id.* at 2629 (citations omitted).

10. For generally critical discussions see, for example, CHRISTOPHER SLOBOGIN, *PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT* 17 (2007) (“Most fundamentally, this chapter argues that when contemplating surveillance (or any other investigative technique), government should be required to provide justification proportionate to the intrusiveness of the surveillance and to seek third-party authorization in all nonexigent circumstances.”); Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 149 (suggesting that reading a broad third party rule into Supreme Court jurisprudence is inappropriate); Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199, 1202 (2009) (suggesting that an alternative set of rules that produces the best mix of privacy and security is preferable to the reasonable expectations test); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. X, [22, 128–129] (2011) (discussing the inordinate appeal of the third party rule in “federal appellate resolution of the Fourth Amendment question in the location privacy cases”); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 977 (2007) (suggesting a factor-based approach to the third party doctrine); Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1247 (2009) (noting that the third party doctrine does not afford technological neutrality or ex ante clarity, as well as suggesting that an elimination of the doctrine may create socioeconomic equality); Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance*, 17 STAN. L. & POL’Y REV. 531, 546 (2006) (noting that the reasoning behind the third party doctrine is “exceptionally strained”); Ric Simmons, *From Katz to*

completely ignored the third party doctrine<sup>11</sup> and did not mention the cases upon which its application to Internet intermediaries is said to rest, *Smith v. Maryland*<sup>12</sup> and *United States v. Miller*.<sup>13</sup> Those opinions have led many to assume that activities involving intermediate storage of digital information by a service provider (essentially all online activity) would be unprotected by the Fourth Amendment.<sup>14</sup> As the Court stated in *Miller*,

This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.<sup>15</sup>

Persons making phone calls and bank deposits were said to have assumed the risk that those to whom they had, in the ordinary course of business, conveyed the numbers they dialed and the content of their bank records

---

Kyllo: *A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1321–35 (2002) (criticizing methods-based Fourth Amendment jurisprudence and instead advocating for a results-based application of the *Katz* test); Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 167–69 (2005) [hereinafter Slobogin, *Transaction Surveillance by the Government*] (arguing that “[t]he degree to which transaction surveillance is regulated” should depend on “the type of information sought” and the type of surveillance at issue); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1138 (2002) [hereinafter Solove, *Digital Dossiers*] (noting the significant privacy threat posed by a third party doctrine approach to digital information); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 748 (2005) [hereinafter Solove, *Fourth Amendment*] (noting the Supreme Court’s difficulty in applying the Fourth Amendment to information and the resultant dependence on statutes for protection); Matthew D. Lawless, Comment, *The Third Party Doctrine Redux: Internet Search Records and the Case for a “Crazy Quilt” of Fourth Amendment Protection*, UCLA J.L. & TECH., Spring 2007, at 1, 2–4, [http://www.lawtechjournal.com/articles/2007/02\\_070426\\_lawless.pdf](http://www.lawtechjournal.com/articles/2007/02_070426_lawless.pdf) (noting the inadequacy of both the statutory and constitutional regimes to address Internet privacy). For a defense of the third party doctrine, see Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563–66 (2009) [hereinafter Kerr, *Case for the Third-Party Doctrine*] (arguing that critics of the third party doctrine overlook substantial benefits); Orin S. Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy*, 24 BERKELEY TECH. L.J. 1229, 1229 (2009) [hereinafter Kerr, *Defending the Third-Party Doctrine*] (suggesting that the third party doctrine furthers technological neutrality and ensures ex ante clarity of the Fourth Amendment).

11. See *Quon*, 130 S. Ct. 2619 (failing to consider the third party doctrine in the Court’s opinion).

12. 442 U.S. 735 (1979).

13. 425 U.S. 435 (1976).

14. See, e.g., Solove, *Digital Dossiers*, *supra* note 10, at 1135 (“Individuals thus probably do not have a reasonable expectation of privacy in communications and records maintained by ISPs or computer network system administrators.”).

15. 425 U.S. at 443; see also *Smith*, 442 U.S. at 744 (quoting *Miller*, 425 U.S. at 443).

would disclose them.<sup>16</sup> *Miller* and *Smith* held that this risk of disclosure vitiated an individual's expectation of privacy.<sup>17</sup>

While the *Quon* Court ultimately declined to rule on the expectation of privacy in intermediated digital communications, such as text messages and e-mail, its failure to dismiss the claim out of hand on the basis of the third party doctrine suggests that, in the long run, the Supreme Court is likely to hold that the mere fact of digital intermediation does not remove all reasonable expectation of privacy, at least in some important social contexts.

*Kyllo v. United States*,<sup>18</sup> decided at the dawn of this century, took a very different approach. There, Justice Scalia, writing for a divided Court, held that the warrantless use of a thermal-imaging device to detect suspicious heat patterns suggesting the cultivation of marijuana within a home violated the Fourth Amendment.<sup>19</sup> In asking "what limits there are upon [the] power of technology to shrink the realm of guaranteed privacy," the Court defined its role as one not of adapting to the changing role of technology, but of preserving the privacy citizens had been able to rely on in the past.<sup>20</sup> The Court opined:

[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.<sup>21</sup>

In reaffirming the central position of the home as a bastion of Fourth Amendment privacy, the majority saw itself as drawing a line at the entrance to the home that "must be not only firm but also bright."<sup>22</sup>

These two very different opinions both tend toward the protection of privacy in the face of new technology, but they take very different routes: one seeks primarily to preserve the constitutionally protected spaces of yesterday,<sup>23</sup> while the other recognizes the need to adapt to the changing

---

16. *Miller*, 425 U.S. at 443.

17. *Smith*, 442 U.S. at 744; *Miller*, 425 U.S. at 443.

18. 533 U.S. 27 (2001).

19. *Id.* at 40.

20. *Id.* at 34.

21. *Id.* (citation omitted).

22. *Id.* at 40.

23. *Id.*

social behavior engendered by technology.<sup>24</sup> In this Article, I argue that a future is nearly upon us that will make it impossible to preserve the privacy even of traditional Fourth Amendment bastions, such as the home, without considering the intertwined effects of technological and social change. Courts therefore should apply a principle of “technosocial continuity” when interpreting the Fourth Amendment’s protections in a world of rapidly evolving technology.<sup>25</sup> Technosocial continuity requires that courts consider both the ways in which technology facilitates intrusive surveillance and the ways in which technology spurs social change that may make citizens more vulnerable to existing surveillance technologies.

Though much of the discussion of digital privacy focuses on “communication,”<sup>26</sup> the Internet has evolved into a place with an exploding variety of contexts in which a full panoply of human behavior takes place. There are social network sites featuring everything from two-way communications, to gathering places for groups of friends, to political meeting spaces, to commercial fan pages. There are chat rooms, places for storing one’s personal library, documents, and financial and health records, and location-based mechanisms for moving from online interactions to real world interactions and back again.<sup>27</sup> There is every reason to believe that

---

24. *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010).

25. This approach contrasts with the “technological neutrality” principle recently advocated by Professor Orin S. Kerr. Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010) [hereinafter Kerr, *A General Approach*]. Professor Kerr focuses on the Internet as a communication technology and advocates the application of a content/noncontent distinction as a proxy for a supposed inside/outside distinction, which he argues reflects the Fourth Amendment’s application in the physical world. *Id.* at 1017–29. As discussed in Part IV, a content/noncontent distinction is not sufficiently cognizant of the complexities of technosocial changes. Professor Kerr puts too much weight on maintaining law enforcement effectiveness in response to the ways in which wrongdoers use the Internet and insufficient weight on the evolving social role of digital technology more generally. *See id.* at 1015–16, 1048. The Fourth Amendment balance is not geared toward ensuring a constant level of crime control; it is geared to ensuring “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. CONST. amend. IV. The effect of a particular type of intrusion made possible by emerging technology on “the security of the people” cannot be evaluated without an understanding of the role that the technology plays in the people’s social life. For a similar argument, see A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip and the Constitution*, 143 U. PA. L. REV. 709 (1995).

26. *See, e.g.*, Kerr, *A General Approach*, *supra* note 25, at 1007–08 (suggesting that individuals should have a reasonable expectation in the contents of their online communications, as distinguished from noncontent information).

27. For some discussions of the growth and social role of social network sites and social media in general, see, for example, Mitja D. Back et al., *Facebook Profiles Reflect Actual Personality, Not Self-Idealization*, 21 PSYCHOL. SCI. 372, 372 (2010), <http://pss.sagepub.com/content/21/3/372.full.pdf> (noting that online social networks “have become integrated into the milieu of modern-day social interactions”); H. Brian Holland, *Privacy Paradox 2.0*, 19 WIDENER L.J. 893, 894 (2010) (describing the privacy implications of the emergence of social networks); danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History,*

the social framework of the Internet will continue to evolve in complexity and variety. While early theorists of “cyberspace” saw it as a country of its own—a land with the potential to transcend many of the limitations, both physical and social, of the real world<sup>28</sup>—the Internet is evolving into a seamless part of the real world, complete with an abundant variety of social and personal contexts.<sup>29</sup> Whether we understand the goals of the Fourth Amendment in terms of privacy, autonomy and personhood, liberty, security, or power, the Fourth Amendment should be interpreted with

---

*and Scholarship*, J. COMPUTER-MEDIATED COMM. (Oct. 2007), <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html> (describing the history of social networks and their growing importance); Pedro de Gouveia, *The Four Most Popular Social Networking Sites*, BIZCOMMUNITY.COM (Dec. 14, 2007, 9:00 AM), <http://www.bizcommunity.com/Article/196/16/20623.html> (noting the popularity of social networking sites). For more specific discussions of the privacy implications of social media, see, for example, David S. Ardia, *Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law*, 45 HARV. C.R.-C.L. L. REV. 261, 262 (2010) (discussing the inadequacies of defamation law in an increasingly networked world); Lauren Gelman, *Privacy, Free Speech, and “Blurry-Edged” Social Networks*, 50 B.C. L. REV. 1315, 1319 (2009) (discussing the problems of protecting privacy in the age of social networks and the prevalence of online divulgence of personal information); James Grimmelman, *Saving Facebook*, 94 IOWA L. REV. 1137, 1141–42 (2009) (discussing various policy proposals concerning Facebook privacy); Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 65, 65 (noting that the Internet puts individuals in a better position “to compromise privacy than the government and commercial institutions”).

28. For a recent description and review of the evolution of this debate, see H. Brian Holland, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, 56 KAN. L. REV. 369 (2008) (describing the development of the Internet governance debate in terms of Internet exceptionalism and network architecture). Indeed, there are entire online worlds, in which people create elaborate simulated artifacts and engage in complex and ongoing social interactions while adopting alternative “avatar” personae. Very interesting legal questions arise in such spaces. See, e.g., JACK M. BALKIN & BETH SIMONE NOVECK, *THE STATE OF PLAY: LAW, GAMES, AND VIRTUAL WORLDS* 3, 3 (Jack M. Balkin & Beth Simone Noveck eds., 2006) (noting that millions of people “spend more time in virtual environments than they do at their real-world jobs or engaged with their real-world communities”); F. Gregory Lastowka & Dan Hunter, *The Laws of the Virtual Worlds*, 92 CALIF. L. REV. 1, 3 (2004) (questioning whether virtual objects constitute legal property and whether democracy and governance may be applied to social conflicts in the virtual world). New York Law School has held an annual conference on these issues since 2003. *State of Play*, INST. FOR INFO., L. & POL’Y, N.Y. L. SCH., [http://www.nyls.edu/centers/harlan\\_scholar\\_centers/institute\\_for\\_information\\_law\\_and\\_policy/events/state\\_of\\_play](http://www.nyls.edu/centers/harlan_scholar_centers/institute_for_information_law_and_policy/events/state_of_play) (last visited Mar. 2, 2011). But the use of avatars and virtual artifacts to make online interactions more “real” is not confined to these virtual worlds. The lines between real world and online social interactions are likely to blur even more as the technologies developed for online games migrate to other kinds of interactions. See, e.g., Marc Jonathan Blitz, *The Freedom of 3D Thought: The First Amendment in Virtual Reality*, 30 CARDOZO L. REV. 1141, 1142 (2008) (discussing three-dimensional virtual reality); M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 PENN ST. L. REV. 809, 811 (2010) (noting that humans react to technological facsimiles “as though a person were actually present”).

29. See, e.g., de Gouveia, *supra* note 27 (noting the popularity of social networking websites).

sensitivity to the social significance of each of these contexts if we are to effectuate its guarantees.<sup>30</sup>

In the context of the home, *Kyllo*'s mistake in attempting to articulate a rule for updating traditional protections is in assuming that a line which is "firm" in protecting the traditional social role of the home can also be "bright" at the doorstep of a physical residence.<sup>31</sup> *Kyllo*'s bright line at the door of the physical home, which seeks simply to protect the traditional locus of privacy from technological encroachment,<sup>32</sup> will be insufficient if we hope to extend meaningful Fourth Amendment protection into a networked world in which technology and social behavior are co-evolving.<sup>33</sup> Rather, courts should adopt an approach of technosocial continuity, recognizing that intertwined technological and social changes require not only the protection of privacy in conventional social contexts against technological intrusions, but also the adaptation of privacy protections to the evolution of social context and governing social norms. As in *Kyllo*, courts should not assume that every technological means of tracking or analyzing data that is available to the government is constitutionally reasonable without appropriate legal justification (a warrant, reasonable suspicion, or some other Fourth Amendment standard). As in *Katz v. United States*,<sup>34</sup> courts should be sensitive to the ways in which technology frames social behavior.

In this Article, I exemplify the technosocial continuity principle with a specific application to cloud computing and social media in relation to the

---

30. The principle of technosocial continuity advocated here is not intended as a new theory of the Fourth Amendment in the sense of delineating its proper goals, though my applications of the principle to the home and office in Part V necessarily rely on judgments about the values underlying traditional Fourth Amendment protections of those arenas. The technosocial continuity principle is consistent with and arguably necessary to implement a variety of theories, such as those focusing on protecting privacy, limiting government power, increasing the security of the citizenry, and so forth. See, e.g., Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After Lawrence*, 57 UCLA L. REV. 1 (2009) (focusing on liberty); Christian M. Halliburton, *How Privacy Killed Katz: A Tale of Cognitive Freedom and the Property of Personhood as Fourth Amendment Norm*, 42 AKRON L. REV. 803, 812 (2009) (considering Margaret Radin's property and personhood paradigm); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 104 (2008) (focusing on the "a right of security" and the prohibition on general warrants); Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002) (discussing the Fourth Amendment's protection from government "power" as opposed to "privacy"). The principle is inconsistent only with the most strictly textualist approach, which would foreclose the Court's ruling in *Katz*, as well.

31. See *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (noting that the line drawn at the doorstep of the home should be "firm" as well as "bright").

32. *Id.*

33. See Kerr, *A General Approach*, *supra* note 25, at 1018 (suggesting a content/noncontent distinction in the online world in place of the inside/outside distinction in the physical world).

34. 389 U.S. 347 (1967).

home and office. Part II discusses the rise of social media and cloud computing. It makes two related points: First, the Internet and other digital technology have had dramatic effects on daily life and social interactions. Second, and at the same time, Internet exceptionalism is no longer a viable position. The Internet is not a separate and distinct place. It is neither a cyberspace utopia<sup>35</sup> nor a realm in which citizens should have to accept that they “have zero privacy” and “[g]et over it.”<sup>36</sup> It is a part of the social realm, in which courts will have to struggle with the same kinds of questions about privacy and government intrusion that they have always confronted. Part III describes the ways in which the co-evolution of technology and society raises two intertwined challenges to the Fourth Amendment’s application. Part IV considers the infamous third party doctrine, which is the basis for most Internet exceptionalism claims on both sides of the digital Fourth Amendment debate. It argues that aggressive interpretations are overblown in light of Supreme Court case law in the offline world and unlikely to prevail in the long (or even short) run. It also rejects the argument that a “content/noncontent” distinction will be sufficient to deal with the Fourth Amendment in the Internet context.<sup>37</sup> Part V focuses on two core Fourth Amendment protected areas, the home and the office. It argues that technosocial continuity requires that conceptions of the home and office be extended to encompass certain digital social contexts. It then applies these ideas specifically to two issues: the plain view doctrine in the context of cloud computing and the application of the Fourth Amendment to undercover policing and the use of informants on social network sites. Part V identifies some of the complexities surrounding extension of the protection of the home into the networked world. Part VI concludes.

## II. THE SEAMLESS WEB

Not so long ago the world wide web seemed like a relatively simple place (though it may not have been so simple even at the time!).<sup>38</sup> There were websites, which displayed content that was posted by website owners

---

35. Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210, 217–18 (2007) [hereinafter Cohen, *Cyberspace*] (noting the interconnectedness of cyberspace and real space).

36. See Polly Sprenger, *Sun on Privacy: “Get Over It,”* WIRED (Jan. 26, 1999), <http://www.wired.com/politics/law/news/1999/01/17538> (internal quotation marks omitted) (reporting widely quoted comment by Sun Microsystems CEO Scott McNealy).

37. See, e.g., Kerr, *A General Approach*, *supra* note 25.

38. See Kai Zhu, *Bringing Neutrality to Network Neutrality*, 22 BERKELEY TECH. L.J. 615, 616 (2007) (“The architects of the original internet did not and could not envision the many new technologies and applications that are now common for the internet.”).

and visible to anyone with an Internet connection and a browser.<sup>39</sup> There was e-mail, which was hosted by commercial Internet service providers (“ISPs”) or private entities, such as corporations and universities.<sup>40</sup> Eventually, there were search engines that helped people to find websites in which they were interested.<sup>41</sup> Socially, the Internet was a discrete place to which one went for specific purposes: to search for news or commercial information, to check e-mail, or perhaps to participate in a chat room or electronic bulletin board on a topic of interest.<sup>42</sup>

In the past few years all of that has changed at an absolutely dizzying pace. Commercial transactions have moved online to the point where one can (and many do) order virtually any product—including books, movies, groceries, restaurant take-out, airline tickets, hotel reservations, and prescription drugs—over the Internet.<sup>43</sup> Personal and business activities blur the line between online and offline.<sup>44</sup> Documents are created, edited, and stored, and computations are performed “in the cloud.”<sup>45</sup> Online banking, including bill payment, is routine.<sup>46</sup> Books are read on various electronic devices, synchronized by records kept online.<sup>47</sup> The bookcase, the CD shelf, and the DVD collection are being supplemented—and in some cases supplanted—by online archives and delivery services.<sup>48</sup>

---

39. Alfred C. Yen, *Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace*, 17 BERKELEY TECH. L.J. 1207, 1214–16 (2002) (providing a brief overview of the history of the Internet).

40. *Id.*

41. *Id.*

42. And, of course, as *Avenue Q* has reminded us beginning in 2002, “The Internet is for porn.” AVENUE Q, *The Internet Is for Porn*, on AVENUE Q: THE MUSICAL, ORIGINAL BROADWAY CAST RECORDING (RCA Victor 2003). AVENUE Q’S light-hearted take on this issue is itself sadly anachronistic in light of the serious issues with online harassment of women and minorities that have accompanied the evolution of the internet into a social space. See, e.g., Danielle Keats Citron, *Cyber Civil Rights*, *Cyber Civil Rights*, 89 BOSTON U. L. REV. 61 (2009).

43. See, e.g., CASS R. SUNSTEIN, *REPUBLIC.COM 2.0*, at 19 (2007) (“If you are interested in anything at all—from computers to linens to diamonds to cars to medical advice—an online company will be happy to assist you.”).

44. *Id.* at 19–20.

45. See *infra* text accompanying notes 211–216.

46. See *News Release: ABA Survey Shows More Consumers Prefer Online Banking*, AM. BANKERS ASSOC. (Sept. 30, 2010), <http://www.aba.com/Press+Room/093010PreferredBankingMethod.htm> (stating that online banking is most customers’ preferred method of banking).

47. See Bob Minzesheimer, *E-Book Wave Now a Tsunami*, CHI. SUN-TIMES (Nov. 5, 2010, 12:12 PM), <http://www.suntimes.com/business/2829174,CST-NWS-ebook24.article> (noting that e-book sales are up 193% over a year ago).

48. See Jeffrey O. Valisno, *The Day the Music [Store] Died*, BUS. WORLD WEEKENDER (Oct. 7, 2010, 6:12 PM), <http://www.bworldonline.com/weekender/content.php?id=19104> (calling “the advent of portable digital music players . . . the greatest upheaval in music retailing since video killed the radio star”).

The social Internet expands at an equally amazing rate.<sup>49</sup> E-mail is supplemented by instant messaging, text messaging, video chat, sharing of cell phone photos and videos among families and friends, and on and on. Social media from MySpace to Facebook to Twitter to Foursquare and beyond offer a growing variety of ways to socialize, conduct business, and organize political and other groups. These online social connections are not divorced from the real world. Instead, they mirror and enhance offline connections, allowing families, friends, and colleagues to remain in touch over the years in a highly mobile society.<sup>50</sup> Of course, intimate relationships also make use of all these means of keeping in touch.<sup>51</sup> Although such things as “sexting,” the sharing of sexually explicit photos, and the use of webcams for sexual interactions make headlines in connection with child pornography, pedophilia, and concerns about early teenage sexuality,<sup>52</sup> there is every reason to think that digital modes of interaction are part of many legitimate adult sexual relationships as well.<sup>53</sup> Online patterns of association are increasingly linked to users’ activities in the offline world: Individuals carry the Internet with them in their pockets linked via smart phones, iPads, and Kindles. These devices not only bring

---

49. See *supra* notes 27–29 and accompanying text.

50. See, e.g., KEITH N. HAMPTON ET AL., PEW INTERNET & AM. LIFE PROJECT, SOCIAL ISOLATION AND NEW TECHNOLOGY: HOW THE INTERNET AND MOBILE PHONES IMPACT AMERICANS’ SOCIAL NETWORKS 3–4 (Nov. 2009), available at [http://www.pewinternet.org/~media/Files/Reports/2009/PIP\\_Tech\\_and\\_Social\\_Isolation.pdf](http://www.pewinternet.org/~media/Files/Reports/2009/PIP_Tech_and_Social_Isolation.pdf) (noting that Internet users have a more diverse social network and participate more in public places); MARY MADDEN, PEW INTERNET & AM. LIFE PROJECT, OLDER ADULTS AND SOCIAL MEDIA: SOCIAL NETWORKING USE AMONG THOSE AGES 50 AND OLDER NEARLY DOUBLED OVER THE PAST YEAR 2–3 (Aug. 27, 2010), available at <http://pewinternet.org/~media/Files/Reports/2010/Pew%20Internet%20-%20Older%20Adults%20and%20Social%20Media.pdf> (noting that older Internet users have been especially enthusiastic in recent years); Jeffrey Boase & Barry Wellman, *Personal Relationships: On and Off the Internet*, in THE CAMBRIDGE HANDBOOK OF PERSONAL RELATIONSHIPS 709, 715–17 (Anita L. Vangelisti & Daniel Perlman eds., 2006) (noting that the Internet is most often used to contact those with whom people have offline relationships); Barry Wellman, *Studying the Internet Studies Through the Ages*, in THE HANDBOOK OF INTERNET STUDIES 17 (2009).

51. See *supra* note 50.

52. See, e.g., Clay Calvert, *Sex, Cell Phones, Privacy, and the First Amendment: When Children Become Child Pornographers and the Lolita Effect Undermines the Law*, 18 COMMLAW CONSPICUOUS 1, 9–11 (2009) (discussing the prevalence of sexting among teenagers); Amy F. Kimpel, *Using Laws Designed to Protect as a Weapon: Prosecuting Minors Under Child Pornography Laws*, 34 N.Y.U. REV. L. & SOC. CHANGE 299, 323–26 (2010) (discussing the prosecution of minors under child pornography laws for possessing or distributing explicit images of themselves); danah michele boyd, Taken Out of Context: American Teen Sociality in Networked Publics 151–67 (2008) (unpublished Ph.D. dissertation, University of California, Berkeley), available at <http://www.danah.org/papers/TakenOutOfContext.pdf> (discussing privacy and safety concerns with increased teenager involvement on social networking websites).

53. Indeed, even a recent episode of the NBC network television show *Parenthood* alluded to “Skype sex” in a serious long-distance relationship. *Parenthood: I Hear You, I See You* (NBC television broadcast Sept. 14, 2010).

the online world to their users but also make location data available for various purposes ranging from restaurant recommendations, to advertising, to facilitating offline social interactions.<sup>54</sup>

As is the case with any new arena for social interaction, whether it is a new geographic location or a new technological platform, society carries with it the potential for antisocial and criminal behavior.<sup>55</sup> Of course, that antisocial and criminal behavior adapts to the technological and social context, creating both new and unsurprising problems.<sup>56</sup>

This story is far from over (and probably out of date even as this is published). And it means that both those who took the Internet exceptionalism position and those who insisted that the Internet was just a new means of communication got it partly right. In some respects, “the more things change the more they stay the same” still rings true. The Internet is not “the wild, wild West” any more than the West remained that way for long.<sup>57</sup> But it is not a simple replica of the pre-Internet offline world either. It is not just that “the Internet is different”; it is that the Internet, like every major advance in infrastructural technology before it, has made everything different.

### III. THE INTERTWINED STRANDS OF TECHNOLOGICAL CHANGE

Advancing technology raises two analytically distinct concerns regarding Fourth Amendment protection of private life from government intrusion. First, technology might enable government to intrude into traditional private arenas. Second, there are increasing opportunities for intrusion made possible by technology-mediated social change. Though analytically distinct, these concerns are not separate and have different valence in different contexts. Often, both are salient, as in the context of locational tracking.

---

54. See, e.g., Janice Y. Tsai et al., *Location-Sharing Technologies: Privacy Risks and Controls*, 6 I/S: J.L. & POL’Y FOR INFO. SOC’Y 119, 120–23 (2010) (“These technologies, also referred to as mobile location technologies, social mobile applications, or simply location-based services (“LBS”), typically allow users to share their real-time or historical location information online.”).

55. See, e.g., Kerr, *A General Approach*, *supra* note 25, at 1044–48 (discussing the difficulties of the warrant requirement when dealing with Internet criminals); Peter Swire, *No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime*, 7 J. TELECOMM. & HIGH TECH. L. 107, 119–20 (2009) (discussing the difficulty of tracking Internet criminals because they are more similar to “mice” than “elephants” like Amazon and eBay).

56. Cf. *supra* note 55.

57. Danielle Keats Citron, *Law’s Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 401 (2009) (“The West is no longer wild: society long ago subjected it to the rule of law.”).

The first concern is that technology might enable government to intrude more easily, cheaply, or deeply into private life.<sup>58</sup> This concern motivated the Supreme Court's ruling in *Kyllo* and Justice Scalia's desire that the line at the entrance to the home remain "not only firm but also bright."<sup>59</sup> This concern also motivated Justice Brandeis's memorable lines in his dissent in *Olmstead v. United States*,<sup>60</sup> which denied a reasonable expectation of privacy in telephone calls:

The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. "That places the liberty of every man in the hands of every petty officer" was said by James Otis of much lesser intrusions than these.<sup>61</sup>

Technological intrusion into traditional arenas of private life would be cause for concern even if social life remained static, although it might require the rethinking of timeworn doctrines, such as the plain view doctrine.<sup>62</sup> Resistance to government use of new technologies to intrude into traditionally private arenas motivated *Silverman v. United States*,<sup>63</sup> in which the Court found the use of a "spike mike" to monitor conversations occurring among individuals within a home unconstitutional.<sup>64</sup>

The critical contribution of *Katz v. United States* was its recognition of the constitutional significance of a second and distinct concern—the intrusion made possible by technology-mediated social change. In considering telephone calls from a phone booth, the *Katz* Court struggled to deal with the way in which social behavior had lost its "fit" with the traditional contours of the public/private distinction<sup>65</sup>:

---

58. See, e.g., *Kyllo v. United States*, 533 U.S. 27, 29–30 (2001) (discussing the ease and depth of information government officials can gather with thermal imagers).

59. *Id.* at 33–40.

60. 277 U.S. 438 (1928), *overruled by* *Katz v. United States*, 389 U.S. 347 (1967), and *Berger v. New York*, 388 U.S. 41 (1967).

61. *Id.* at 474 (Brandeis, J., dissenting).

62. See, e.g., *Kyllo*, 533 U.S. at 35–40 (rethinking the plain view doctrine).

63. 365 U.S. 505 (1961).

64. *Id.* at 506, 509.

65. The somewhat cryptic nature of this formulation perhaps explains why the "reasonable expectation of privacy" formulation of Justice Harlan's concurrence has become the talismanic test of the applicability of the Fourth Amendment.

For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.<sup>66</sup>

Though scholars tend to view *Katz* primarily as a break from earlier case law emphasizing concepts of property and trespass in evaluating surveillance,<sup>67</sup> the idea that the Fourth Amendment might prohibit a search of a place in which a person has no possessory interest was not new at the time. Immediately after its statement that the Fourth Amendment “protects people, not places” the Court was able to cite a list of situations in which Fourth Amendment rights adhere despite the defendant’s lack of a possessory interest: “No less than an individual in a business office, in a friend’s apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment.”<sup>68</sup> Crucially, the Court placed the facts of the case explicitly in a social context:

One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.<sup>69</sup>

Notably, *Katz* did not involve telephone calls made from a home or an office but rather involved calls from a phone booth, a physical construct given social meaning only by the social role of the telephone itself.<sup>70</sup> Nor did the Court’s opinion inquire at any length into the specifics of the

---

66. *Katz v. United States*, 389 U.S. 347, 351–52 (1967) (citations omitted).

67. See, e.g., Halliburton, *supra* note 30, at 820–23 (explaining that *Katz* shifted the scope of Fourth Amendment jurisprudence from typical property cases to that of privacy and the person); Jed Rubenfeld, *supra* note 30, at 105–07, 115 (citing *Katz* as the beginning of the “modern Fourth Amendment doctrine” in moving from trespass to privacy); Simmons, *supra* note 10, at 1305 (arguing that courts routinely have erred in interpreting *Katz* as “merely a repudiation of the ‘trespass doctrine’”); Christopher Slobogin, Lecture, *Surveillance and the Constitution*, 55 WAYNE L. REV. 1105, 1111 (2009) (explaining that until *Katz* it was generally thought that the Fourth Amendment only dealt with privacy interests, and that *Katz* allowed for the Fourth Amendment to be implicated in cases where the government intruded on personal privacy); Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 YALE J.L. & TECH. 120, 124–26 (2007) (noting that after *Katz* the Court’s notion of physical boundaries “stretched,” thus indicating the willingness of the Court to adapt).

68. *Katz*, 389 U.S. at 352 (footnotes omitted).

69. *Id.*

70. See *id.* at 348.

technology used to overhear and record the phone conversation.<sup>71</sup> Although these facts are often elided in discussions of *Katz*'s significance, they are critically important for the application of its principles to a networked society.<sup>72</sup> *Katz* was not about the evolution of invasive technological means to penetrate traditionally private spaces.<sup>73</sup> Rather, it was about the ways in which technology-mediated social change had exposed the citizenry to intrusive surveillance.<sup>74</sup>

*Olmstead*, which *Katz* overruled,<sup>75</sup> flatly rejected the need to adopt the Fourth Amendment's protections to technology-mediated social change.<sup>76</sup> In *Olmstead*, the Court famously declined to find a Fourth Amendment violation in warrantless wiretapping of telephone calls.<sup>77</sup> Although it recognized that technology had resulted in significant social change, the *Olmstead* Court was unwilling to extend the Fourth Amendment's protection to new social patterns. As the Court stated,

By the invention of the telephone, fifty years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place. The language of the Amendment can not be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched.<sup>78</sup>

By overruling *Olmstead*, *Katz* not only severed the Fourth Amendment's ties to trespass doctrine but, perhaps more importantly, established the notion that Fourth Amendment analysis must be sensitive to both the potential for increasing intrusiveness into conventional activities and the evolving landscape of social interchange.<sup>79</sup> The ubiquity of telephone

---

71. See *id.* (failing to detail the specifics of the technology used to record the phone call and referring to it merely as an "electronic listening and recording device").

72. See *supra* note 67 (generally noting the varying significances of *Katz*).

73. See, e.g., *Katz*, 389 U.S. at 352–53 (discussing the new notion of surveillance without the need for physical penetration); see also *id.* at 365 (Black, J., dissenting) (arguing that the Fourth Amendment only covers tangibles, like "persons, houses, papers and effects," leaving all those technologically mediated social constructs vulnerable to surveillance (quoting U.S. CONST. amend. IV)).

74. See *supra* note 70 and accompanying text.

75. *Katz*, 389 U.S. at 352–53.

76. See *Olmstead v. United States*, 277 U.S. 438, 465–66 (1928) (declining to adopt a policy of protecting phone conversations unless Congress adopted such protections through legislation), overruled by *Katz*, 389 U.S. 347, and *Berger v. New York*, 388 U.S. 41 (1967).

77. *Id.* at 466.

78. *Id.* at 465.

79. See *supra* note 67 and accompanying text.

conversations did not merely move conversations that would have taken place in private homes into the telephone booth, thereby making the content of the conversation more easily surveillable (because phone lines are easily wiretapped or bugged) and the noncontent information less easily surveillable (because comings and goings to the house were no longer in plain view of a police officer).<sup>80</sup> The transformation of social life was far more extensive.<sup>81</sup> People did not just converse by phone, they had entirely different conversations. They sought out local friends based more on conviviality and less on proximity, maintained long-distance relationships with friends, family, and lovers, made different decisions about where to work and live, and generally lived different lives than they otherwise would have lived.<sup>82</sup> A telephone system open to unregulated wiretapping by government (and others) would have enabled more intrusion on individual telephone calls, and perhaps people would have evolved entirely different, and more limited, relationships with the telephone, with deep societal effects.<sup>83</sup>

When technological infrastructure changes in such basic ways, the stakes can be very high. The effect of a particular type of intrusion made possible by emerging technology on “the security of the people” cannot be evaluated without an understanding of the role that the technology plays in the people’s social life.<sup>84</sup> Such sensitivity to changes in social patterns of behavior is important because decisions about the Fourth Amendment’s contours will affect not only the extent of government surveillance but also the evolving shape of society’s interactions with new technologies themselves.

To say that the issues of increased intrusion into traditional private arenas and intrusion made possible by technology-mediated social change are analytically distinct is not to say that they are independent. The same technology that educes change in social patterns of interaction and behavior

---

<sup>80</sup> See, e.g., Kerr, *A General Approach*, *supra* note 25 at 1020-22.

<sup>81</sup> See, e.g., Press Release, BBC, Inventions That Changed the World on BBC TWO (Dec. 23, 2003), [http://www.bbc.co.uk/pressoffice/pressreleases/stories/2003/12\\_december/23/inventions.shtml](http://www.bbc.co.uk/pressoffice/pressreleases/stories/2003/12_december/23/inventions.shtml) (highlighting a television program discussing the invention of the telephone and explaining that “[t]he telephone has not only changed the way we do business but also led to the development of the internet”).

<sup>82</sup> See, e.g., *Telephones Have Changed Our Lives*, TOPEKA CAP.-J., July 6, 2000, [http://findarticles.com/p/articles/mi\\_qn4179/is\\_20000706/ai\\_n11750567/](http://findarticles.com/p/articles/mi_qn4179/is_20000706/ai_n11750567/) (discussing how telephone use has advanced since the 1930s).

<sup>83</sup> This is, of course, also the case with private surveillance—a subject of great controversy in the Internet context, as well (but beyond the scope of this Article).

<sup>84</sup> See, e.g., *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010) (“The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.”).

may also make conventionally private interactions and behavior more vulnerable to government intrusion.<sup>85</sup> Additionally, as in *Katz*, new social behaviors may be inherently more vulnerable to existing means of surveillance.<sup>86</sup> The two concerns may be expected to have different valence in different contexts.

For example, as with the infrared cameras in *Kyllo*, the increasing intrusiveness of video surveillance is primarily a result of technological advances. Video devices have become cheaper, smaller, and easier to hide, and video recordings easier to store and to search, thus making conventional social behavior more amenable to surveillance.<sup>87</sup> Similar potential for invasion of privacy may accompany the deployment of “smart grid” technology for delivering electricity, which is now being tested and implemented in some areas.<sup>88</sup> Smart grid technology is aimed at promoting energy conservation and reducing peak loads by monitoring customers’ use of electricity in time increments of less than an hour.<sup>89</sup> Though the technology is intended to incentivize changes in energy consumption (by permitting prices to vary depending on the load, for example), the main privacy concern is the potential for highly invasive scrutiny of people’s conventionally private activities in their homes.<sup>90</sup>

---

85. See, e.g., *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010) (explaining that through continuous GPS surveillance “of another’s travels,” the government “can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts”), *cert. denied*, 131 S. Ct. 671 (2010).

86. See, e.g., *Katz v. United States*, 389 U.S. 347, 348–49 (1967) (explaining that FBI agents had attached a surveillance “bug” to the outside of a public telephone booth to eavesdrop on petitioner’s calls about illegal wagers and gather evidence against him).

87. For a discussion of the privacy implications of video surveillance, see, for example, Jacqueline D. Lipton, *Digital Multi-Media and the Limits of Privacy Law*, 42 CASE W. RES. J. INT’L L. 551 (2010).

88. See, e.g., Jack I. Lerner & Deirdre K. Mulligan, *Taking the “Long View” on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3, <http://stlr.stanford.edu/pdf/lerner-mulligan-long-view.pdf>.

89. See LITOS STRATEGIC COMM’N, U.S. DEP’T OF ENERGY, THE SMART GRID: AN INTRODUCTION 10–14 (2008), available at [http://www.oe.energy.gov/DocumentsandMedia/DOE\\_SG\\_Book\\_Single\\_Pages%281%29.pdf](http://www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf) (explaining that measurements of energy usage taken at precisely synchronized increments may decrease energy use and reduce high costs to meet peak demand).

90. See *id.* at 12 (noting that electricity readings “taken many times a second . . . offer[] dynamic visibility into the power system” and explaining how smart grids will “energize those utility initiatives that encourage consumers to modify patterns of electricity usage, including the timing and level of electricity demand”). Obviously, such “dynamic visibility into the power system” could raise concerns about privacy of activities in people’s homes. *Id.*

The issue of transactional surveillance is different.<sup>91</sup> Advances in information technology have made it easier and cheaper for retailers to store reams of transactional records,<sup>92</sup> thus increasing the potential for surveillance of purchasing behavior. The rise of electronic commerce also has changed shopping behavior, allowing people to make more online purchases, and thereby amplifying the use of credit cards and facilitating transactional record keeping.<sup>93</sup> The social change here may be relatively minor—perhaps people will use the Internet (or credit cards, for that matter<sup>94</sup>) to make more or less the same kinds of commercial purchases they have always made.<sup>95</sup> Even so, this minor social change combines with information processing and record keeping technologies to lead to vastly enhanced potential for surveillance.

In the context of locational tracking, both concerns are salient. Many individuals now carry location-sensitive electronic devices, such as smart phones or GPS navigation systems, for social reasons quite orthogonal to the fact that those devices facilitate tracking.<sup>96</sup> Simultaneously, technology has facilitated government surveillance of citizens' physical movements to a far greater degree than was previously possible by making it easier to install and easier to track location-sensitive "bugs."<sup>97</sup> As discussed in Part V, Fourth Amendment doctrine defining the constitutionally permissible

---

91. See Slobogin, *Transaction Surveillance by the Government*, *supra* note 10, at 167–69 (proposing regulation of transaction surveillance).

92. See, e.g., KENNETH J. BALDAUF & RALPH M. STAIR, *SUCCESSING WITH TECHNOLOGY: COMPUTER SYSTEM CONCEPTS FOR REAL LIFE* 383 (2008) (discussing the advantages of an electronic "database approach").

93. *Id.*

94. See Nielsen, *875MM Consumers Have Shopped Online—Up 40% in Two Years*, *MARKETING CHARTS* (Jan. 29, 2008), <http://www.marketingcharts.com/direct/875mm-consumers-have-shopped-online-up-40-in-two-years-3225/> (reporting that "[m]ore than 85% of the world's online population has used the internet to make a purchase" and that "[c]redit cards are by far the most common method of payment").

95. See *id.* ("Globally, the most popular and purchased items over the internet are books (41% purchased in the previous three months), clothing/accessories/shoes (36%), videos/DVDs/games (24%), airline tickets (24%) and electronic equipment (23%).").

96. See *National Study Shows GPS Adoption Rates Relatively Low, but Offers Recommendations to Accelerate Market Penetration*, *HARRIS INTERACTIVE* (Aug. 15, 2007), <http://www.harrisinteractive.com/NEWS/allnewsbydate.asp?NewsID=1241> (noting that as far back as mid-2007, "one in six (17%) U.S. adults [already] own[ed] or use[d] a GPS location device or service" and that "nine percent of adults indicate that they are very or extremely likely to purchase [one] in the next 12 months").

97. See, e.g., David Kravets, *Feds: Privacy Does Not Exist in "Public Places,"* *WIRED* (Sept. 21, 2010, 3:29 PM), <http://www.wired.com/threatlevel/2010/09/public-privacy/> (reporting that "[t]he Obama administration has urged a federal appeals court to allow the government, without a court warrant, to affix GPS devices on suspects' vehicles to track their every move" and warned that "Americans should expect no privacy while in public").

scope of government tracking of physical movement is being reconsidered as a result of these technological advances.<sup>98</sup>

Email and text messaging fall more toward the social end of the technosocial spectrum. Just as the Supreme Court in *Katz* emphasized the social importance of the telephone, courts should recognize the important part that e-mail and text messaging now play in private communication.<sup>99</sup> Once courts recognize this (as they are beginning to do) it becomes clear that the content of these communications must come under the wing of the Fourth Amendment.<sup>100</sup> The intrusiveness of the technology is not entirely irrelevant, however, as it sets the parameters of the debate about where to draw the line between protected (such as the conversations overheard in *Katz*) and unprotected (such as the phone numbers deemed unprotected in *Smith v. Maryland*<sup>101</sup>) information in digital communications.<sup>102</sup>

Social media technologies, on which I focus in the latter part of this Article, are bound to raise tricky questions because they combine significant social change with increased ease of surveillance (due to the data trails they generate).<sup>103</sup> The Fourth Amendment's application to these products of technosocial change will have to be determined. Justice Scalia was certainly right in his partial concurrence in *Quon* when he criticized the Court's reluctance to take on the issues raised by digital technology. He stated:

The Court's implication that where electronic privacy is concerned we should decide less than we otherwise would (that

---

98. See, e.g., *United States v. Maynard*, 615 F.3d 544, 562–63 (D.C. Cir. 2010) (discussing how under the government's "mosaic theory," an individual's movements can reveal private information), *cert. denied*, 131 S. Ct. 671 (2010).

99. See, e.g., Kathy Buckner & Mark Gillham, *Using Email for Social and Domestic Purposes: Effectiveness in Fulfillment of Interpersonal Communication Motives* 13–14 (unpublished manuscript presented at the Home Oriented Informatics and Telematics Conference, Apr. 6–8, 2003), available at <http://www.crito.uci.edu/noah/HOIT/HOIT%20Papers/Using%20email%20for%20social%20and%20domestic%20purposes.pdf> (describing the role of e-mail in "fulfillment of interpersonal communication motives" and e-mail's importance in "friendship development").

100. See *Rehberg v. Paulk*, 611 F.3d 828, 843–44 (11th Cir. 2010) (collecting cases that "address the issue of Fourth Amendment protection of email content" and noting that the Supreme Court has yet to rule on the issue), *cert. granted*, 2011 WL 940891 (U.S. Mar. 21, 2011).

101. 442 U.S. 735, 742–46 (1979).

102. See generally Kerr, *A General Approach*, *supra* note 25, at 1019–22 (discussing how "[a]ccessing the contents of communications should ordinarily be a search," while "access to non-content information should be treated like access to evidence found outside"). The technology's intrusiveness would, therefore, partially determine accessibility.

103. See Mark Glaser, *Your Guide to Online Privacy*, PBS (Feb. 13, 2008), <http://www.pbs.org/mediashift/2008/02/your-guide-to-online-privacy044.html> ("As we share more information online via myriad site registrations, online social networking profiles, e-commerce sites and search engines, the desire by companies and governments to mine that information is increasingly at odds with the desire of users to protect it.").

is, less than the principle of law necessary to resolve the case and guide private action)—or that we should hedge our bets by concocting case-specific standards or issuing opaque opinions—is in my view indefensible. The-times-they-are-a-changin’ is a feeble excuse for disregard of duty.<sup>104</sup>

As noted in and exemplified by *Katz*, the Court has repeatedly had to concern itself with extending traditional Fourth Amendment concepts, such as the protection afforded to the home, office, and postal mail, to new, but related, circumstances.<sup>105</sup> The principle of technosocial continuity is an important tool for that task.<sup>106</sup>

#### IV. THE AGGRESSIVE THIRD PARTY DOCTRINE AND STEPS TOWARD TECHNOSOCIAL CONTINUITY

Before discussing how a principle of technosocial continuity would frame Fourth Amendment applications to social networks and cloud computing, it is necessary to clear out a bit of underbrush concerning the current state of the law and to illustrate the way in which some courts, in interpreting the Fourth Amendment, are already beginning to move away from a rigid and aggressive third party doctrine and toward an approach consistent with the principle of technosocial continuity.

Beginning in 2002 with articles by Professors Daniel Solove<sup>107</sup> and Ric Simmons,<sup>108</sup> scholars of information privacy law and Internet law have spilled a large amount of ink (or perhaps more accurately devoted a large number of bytes to) bemoaning the dismal implications for privacy in the Internet era of what has been called the “third party doctrine” of Fourth

---

104. *City of Ontario v. Quon*, 130 S. Ct. 2619, 2635 (2010) (Scalia, J., concurring in part and concurring in the judgment) (citation omitted).

105. *See Katz v. United States*, 389 U.S. 347, 353 (1967) (affirming that “the Fourth Amendment protects people—and not simply ‘areas’—against unreasonable searches and seizures,” implying that as technology expands, so must Fourth Amendment protections).

106. *See supra* note 30.

107. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083 (2002).

108. Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 *Hastings L.J.* 1303 (2002).

109. *See, e.g.*, Simmons, *supra* note 10 at 1339 (describing how the third party doctrine allows the government to search every single piece of e-mail); Solove, *Digital Dossiers*, *supra* note 10, at 1101–04 (explaining that the government’s ability to gather information from third party records without Fourth Amendment protection can create a Big Brother state and constrain democracy while failing to ensure government accountability).

109. *See, e.g.*, Simmons, *supra* note 10 at 1339 (describing how the third party doctrine allows the government to search every single piece of e-mail); Solove, *Digital Dossiers*, *supra* note 10, at 1101–04 (explaining that the government’s ability to gather information from third party records without Fourth Amendment protection can create a Big Brother state and constrain democracy while failing to ensure government accountability).

Amendment jurisprudence.<sup>109</sup> According to what was, for a time at least, the accepted wisdom, there is virtually no Fourth Amendment protection for any information conveyed over the Internet or other digital intermediary.<sup>110</sup>

The argument proceeded in two steps. First, it was argued that relying on an intermediary means that an individual assumes the risk of disclosure by that intermediary. This is primarily because digital activities generally require that intermediaries make, process, and store, at least temporarily, copies of the information.<sup>111</sup> Second, and importantly, it was argued that disclosure to *any third party* removes any reasonable expectation of privacy with respect to *anyone* and therefore removes the information from the realm of Fourth Amendment protection entirely.<sup>112</sup>

When one looks more closely, however, this aggressive version of the third party doctrine, in which any disclosure to any third party vitiates Fourth Amendment protection entirely, has a very narrow purview. Indeed, its presumed applicability to all intermediated digital activity betrays myopia about the social role of such activity, which was understandable early in this century but is now untenable.

The first, “assumption of risk,” step of the third party doctrine argument is pervasive in Fourth Amendment law. It underlies cases such as those involving searches of garbage left for pickup,<sup>113</sup> undercover policing and use of informants,<sup>114</sup> and law enforcement “flyovers” of residential

---

109. See, e.g., Simmons, *supra* note 10 at 1339 (describing how the third party doctrine allows the government to search every single piece of e-mail); Solove, *Digital Dossiers*, *supra* note 10, at 1101–04 (explaining that the government’s ability to gather information from third party records without Fourth Amendment protection can create a Big Brother state and constrain democracy while failing to ensure government accountability).

110. See, e.g., Solove, *Digital Dossiers*, *supra* note 10, at 1135 (“*Miller and Smith* establish a general rule that if information is in the hands of third parties, then an individual can have no reasonable expectation of privacy in that information, which means that the Fourth Amendment does not apply. Individuals thus probably do not have a reasonable expectation of privacy in communications and records maintained by ISPs or computer network system administrators.” (footnotes omitted)).

111. See Simmons, *supra* note 10, at 1339 (explaining that all electronic data is sent through independent third parties capable of recording the address and content of the data).

112. See, e.g., *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (stating that when petitioner dialed a phone number, he assumed the risk that the phone company would hand this information over to the government); *cf. id.* at 750 (Marshall, J., dissenting) (“[W]hether privacy expectations are legitimate within the meaning of *Katz* depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society.”).

113. See, e.g., *California v. Greenwood*, 486 U.S. 35, 37 (1988) (holding that the Fourth Amendment does not prohibit “the warrantless search and seizure of garbage left for collection outside the curtilage of a home”).

114. See, e.g., *United States v. White*, 401 U.S. 745, 751 (1971) (finding no constitutional violation when police informants or agents secretly record conversations within a home, even without a warrant); *Hoffa v. United States*, 385 U.S. 293, 302–03 (1966) (finding that the Fourth

areas.<sup>115</sup> In such cases, the Supreme Court holds that an individual assumes the risk that a law enforcement official will do what another third party might reasonably be expected to do—look at something in plain view even if looking requires going to some effort to peek, befriend an individual and then betray her criminal behavior to the government, obtain information about someone by talking to her friends and neighbors, and so forth. This first step itself is controversial, especially when law enforcement officers break generally applicable laws in their searching, and has limits, whether based on the use of particularly advanced surveillance technology, as in *Kyllo*, or on reasonable social expectations, as in *Katz*.

The second step in the logic of the aggressive digital third party doctrine is nearly *sui generis*. It stems from two Supreme Court cases from the 1970s, both of which have been subsequently cabined by statute. The seminal case upon which the argument rests, *United States v. Miller*,<sup>116</sup> concerned a defective subpoena for bank records in a case involving evasion of the whiskey tax.<sup>117</sup> The Supreme Court, relying on earlier

---

Amendment does not protect a wrongdoer's misplaced confidences); *Lopez v. United States*, 373 U.S. 427, 438 (1963) (finding that IRS officer's entry into an office under the pretext of offering a bribe was not an unconstitutional intrusion).

115. See, e.g., *Florida v. Riley*, 488 U.S. 445, 450 (1989) ("Because the sides and roof of his greenhouse were left partially open, however, what was growing in the greenhouse was subject to viewing from the air."); *California v. Ciraolo*, 476 U.S. 207, 211 (1986) ("Yet a 10-foot fence might not shield these plants from the eyes of a citizen or a policeman perched on the top of a truck or a two-level bus.").

116. *Miller* attracted strong dissents from Justices Brennan and Marshall, was legislatively cabined by the Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, § 1100–22, 92 Stat. 3641, 3697–3710 (codified at 12 U.S.C. §§ 3401–22 (2006)), and a number of states have declined to follow it in interpreting their state constitutions, Henderson, *supra* note 10, at 985–1018 (describing jurisprudence of states that have declined to follow the Supreme Court's third party doctrine in interpreting similar state constitutional provisions). Despite its rather expansive language, *Miller* has not been the basis for a vast contraction of reasonable expectations of privacy any time anyone shares private information with a third party. Two cases citing *Miller* involved the specific issue of financial records. In those cases, the Supreme Court followed its holding in *Miller*. See *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735 (1984); *United States v. Payner*, 447 U.S. 727 (1980). As of October 30, 2010, neither case has been relied on by the Court to expand *Miller's* approach. The only other Supreme Court case, besides *Smith v. Maryland*, to rely on *Miller* in any relevant way cited *Miller* for the proposition that the government could search a package after the private freight company charged with transporting it had already opened it. See *United States v. Jacobsen*, 466 U.S. 109 (1984). The Court did not suggest that law enforcement could have opened the package if the private party had not or could simply have demanded that the freight company open it, which would be the conclusion under the aggressive third party doctrine. Indeed, the Court confirmed that the appropriate scope of the government search was confined to the scope of the actual private search. Since 1980, *Miller* has never been cited in a Supreme Court majority or plurality opinion. Significantly, the two most recent citations to *Miller*, in *Georgia v. Randolph*, 547 U.S. 103 (2006), and *Ferguson v. City of Charleston*, 532 U.S. 67 (2001), were by dissenting Justices who argued that the majorities had failed to extend the logic of *Miller* in those cases. *Randolph*, 547 U.S. at 132–33 (Roberts, C.J., dissenting); *Ferguson*, 532 U.S. at 94 (Scalia, J., dissenting).

117. *United States v. Miller*, 425 U.S. 435, 436 (1976).

precedent involving information obtained by government informants through conversation, held that there was no reasonable expectation of privacy in the bank records and hence no Fourth Amendment interest in preventing government from obtaining them by using a statutorily defective subpoena.<sup>118</sup> The *Miller* Court reasoned that (1) bank records “contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business” and (2) “[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”<sup>119</sup> Importantly, the Court distinguished precedent providing Fourth Amendment protection to “a man’s private papers” by construing the financial records as “business records of the banks.”<sup>120</sup>

*Smith v. Maryland*,<sup>121</sup> the other pillar of the second element of the aggressive third party doctrine, considered whether a telephone subscriber

---

118. *Id.* at 437, 442–43.

119. *Id.* at 442–43.

120. *Id.* at 439–40 (quoting *Boyd v. United States*, 116 U.S. 616, 622 (1886), *overruled by* *Warden v. Hayden*, 387 U.S. 294 (1967)). The Court also referred to the documents as having been “voluntarily conveyed” to the government by the bank, arguably, if rather implausibly, limiting even this case to “step one” of the third party doctrine logic. *Id.* at 442.

121. Three Justices dissented from the majority opinion in *Smith*, and Congress legislatively cabined it by enacting the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, sec. 301, 100 Stat. 1848, 1868–73 (codified as amended at 18 U.S.C. §§ 3121–27 (2006)), which requires a certification to a court that “the information likely to be obtained is relevant to an ongoing criminal investigation” before a law enforcement officer can deploy a pen register or trap and trace device. 18 U.S.C. § 3122(b)(2). Some states also provide more protection to dialed numbers under their state constitutions. *See, e.g.*, *Henderson*, *supra* note 10, at 1007 n.186 (describing how the State of Washington used its state constitution to restrict law enforcement’s access to dialed telephone numbers); *cf., e.g.*, *State v. Reid*, 914 A.2d 310, 317 (N.J. Super. Ct. App. Div. 2007) (describing how New Jersey’s state constitution protects a reasonable expectation of privacy in an individual’s ISP account information), *aff’d*, 945 A.2d 26 (N.J. 2008).

*Smith* has also had quite a lackluster career in the Supreme Court’s later opinions. It has been cited substantively in only three majority opinions, the most recent of which was more than twenty years ago. *See California v. Greenwood*, 486 U.S. 35, 41 (1988) (citing *Smith* for the proposition that recording the telephone numbers dialed by an individual through a pen register device does not violate the Fourth Amendment); *United States v. Jacobsen*, 466 U.S. 109, 122–23 n.22 (1984) (same); *United States v. Knotts*, 460 U.S. 276, 283 (1983) (same). Although the Court has cited *Smith* in twelve majority opinions, it is frequently invoked only in passing as authority for the two-part reasonable expectation of privacy test derived from Justice Harlan’s concurrence in *Katz*. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27, 32–33 (2001) (explaining that the Court applied Justice Harlan’s reasonable expectation of privacy test in *Smith*).

Interestingly, while the majority in *Kyllo* only cited *Smith* in passing, it was relied on more extensively by the dissent, which argued unsuccessfully that the collection and analysis of thermal radiation was no more intrusive than the collection and analysis of phone numbers in *Smith*. *Kyllo*, 533 U.S. at 44 (Stevens, J., dissenting). *Kyllo* is an exploration of the limits of the plain view doctrine, which may be thought of as a version of the third party doctrine in which the third party is often the public at large. As the discussion by the dissenting Justices correctly implies,

had a legitimate expectation of privacy in the phone numbers he had dialed.<sup>122</sup> The defendant argued, based on *Katz*, that Fourth Amendment protections applied to telephone calls and that he had a reasonable expectation of privacy in the phone numbers he dialed from his home.<sup>123</sup> The Court distinguished *Katz*, emphasizing that pen registers (devices for recording phone numbers being dialed) “do not acquire the contents of communications.”<sup>124</sup> The Court also emphasized the uses for which pen registers were “regularly employed” and opined that “it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.”<sup>125</sup> Citing *Miller*, the Court argued that “petitioner voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business.”<sup>126</sup> The Court noted that “[p]etitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy” and was “not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.”<sup>127</sup> In the statement most frequently quoted in describing the aggressive third party doctrine, the Court said, “This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”<sup>128</sup> Notably, however, the cases cited in support of this proposition, other than *Miller*, all deal with situations in

---

*Kyllo* itself belies the validity of any all or nothing assertion that third party access to data removes all reasonable expectation of privacy.

122. See *Smith v. Maryland* 442 U.S. 735, 736 (1979) (“This case presents the question whether the installation and use of a pen register constitutes a ‘search’ within the meaning of the Fourth Amendment, made applicable to the States through the Fourteenth Amendment.” (footnotes omitted)).

123. See *id.* at 741 (“Petitioner’s claim . . . is that . . . the State, as did the Government in *Katz*, infringed a ‘legitimate expectation of privacy’ that petitioner held.”).

124. *Id.* (emphasis omitted).

125. *Id.* at 742–43.

126. *Id.* at 743–45 (citing *United States v. Miller*, 425 U.S. 435, 442–44 (1976)).

127. *Id.* at 744–45. Regardless of what one thinks of the result in this case, the Court’s reasoning, which concludes that the adoption of less intrusive technology (here automated call processing) could not raise a reasonable expectation of privacy, reveals the pitfalls of any “technological neutrality” principle, see Kerr, *A General Approach*, *supra* note 25, that does not sufficiently account for technology-mediated social change. One might equally well have argued from technological neutrality that the change from party lines to individual phone lines should not have raised expectations of privacy in the content of telephone conversations, since it would have decreased the ease with which law enforcement could monitor such conversations and increased the potential for telephone calls to be employed to facilitate criminal acts. Such an approach would neglect the social reality that the advent of individual phone lines dramatically increased the social value of the telephone system, as well.

128. *Smith*, 442 U.S. at 744–45.

which the government obtained the information via the voluntary actions of the third party in question (“step one,” assumption of risk, cases).<sup>129</sup>

Pushed to their outer limits, *Smith* and *Miller* have been argued to stand for two propositions. First, the proposition that merely by sharing information (such as the financial records of *Miller* or the dialed numbers of *Smith*) with a third party, an individual assumes the risk that the information will be disclosed to the government by the third party.<sup>130</sup> Second, the far more radical proposition that any information in the hands of a third party is open to government scrutiny even if the third party does not wish to turn it over.<sup>131</sup> Under this more radical perspective, e-mail, which is stored at least temporarily on the servers of an Internet service provider would be unprotected by the Fourth Amendment. The same would be true for all transaction data, cell phone location data, social network information, text messages, and data stored in the cloud, leaving only the content of telephone conversations (presumed to be ephemeral and hence not in the hands of the phone company) protected under *Katz*.

The distinction between the ephemeral and the stored has, however, proven entirely unstable in the face of technosocial changes in communication behavior, including the use of e-mail, text messaging, online chat, and voice over internet protocol telephony. The digital communications network that includes the Internet is no longer reasonably viewed as simply a “communication provider” like the telephone company (indeed, in light of mobile smart phones and locational technology even the phone company is no longer a simple communication provider). The cyberspace exceptionalists were on to something after all: Cyberspace has become a space for social life. But it is not a separate or exceptional space. Rather, the digital and physical social realms are inextricably intertwined.

Applications of the Fourth Amendment to shared sociality in the physical world are deeply inconsistent with the aggressive third party doctrine.<sup>132</sup> Indeed, a contention that sharing a physical space with others deprives an individual of Fourth Amendment protection against all warrantless government intrusion seems ludicrous. The Fourth Amendment

---

129. *Couch v. United States*, 409 U.S. 322, 335–36 (1973); *United States v. White*, 401 U.S. 745, 752 (1971); *Hoffa v. United States*, 385 U.S. 293, 302 (1966); *Lopez v. United States*, 373 U.S. 427 (1963).

130. See text accompanying notes 113–**Error! Bookmark not defined.**

131. See text accompanying notes 116–129.

132. Professor Jed Rubenfeld also makes this point as part of a broader argument that “[t]he Fourth Amendment must cut anchor with the expectation-of-privacy apparatus” and focus instead on the Amendment’s guarantee of security. Rubenfeld, *supra* note 30, at 115. One need not sign on to Professor Rubenfeld’s broader argument against privacy as the touchstone of Fourth Amendment analysis to adapt a technosocial principle of analysis. Privacy itself need not—and should not—be seen as an “either or” proposition. See generally, e.g., HELEN NISSENBAUM, *PRIVACY IN CONTEXT* (2009).

protects against government intrusion in many circumstances in which individuals are engaged in the social aspects of life.<sup>133</sup> Most recently, in *Georgia v. Randolph*,<sup>134</sup> the Court held that one occupant of a shared residence may not consent to a search over the objection of a co-tenant who is present and making his objections known.<sup>135</sup> In reaching this conclusion, the Court relied on social norms, stating that “[t]he constant element in assessing Fourth Amendment reasonableness in the consent cases, then, is the great significance given to widely shared social expectations.”<sup>136</sup> Both tenants maintained a reasonable expectation of privacy in the shared residence even though the Court previously had held that one tenant could consent to police entry and search in the absence of the other tenant.<sup>137</sup>

This accommodation to social context has deep roots in Fourth Amendment doctrine. The Court has found a reasonable expectation of privacy in a number of types of temporary quarters that an owner or landlord undoubtedly had some concurrent ability to access, in items given to a third party for storage or transportation, and in various closed containers which were accessible to third parties.<sup>138</sup> As Justice Scalia wrote in his concurrence in the judgment in *O’Connor v. Ortega*,

---

133. For discussions from various perspectives of the Court’s treatment of shared privacy, see, for example, Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 28–32 (2005) (concluding that the Court grounds “Fourth Amendment privacy upon spatial constraints” and intrusions into private places); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL’Y 211, 245–65 (2006) (arguing that the Court’s post-*Katz* opinions are inconsistent with the history of Fourth Amendment jurisprudence of a privacy interest in transactional data); Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 120–24 (2002) (describing the Court’s decisions as consistently eroding privacy and promising to eliminate the concept altogether); Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CALIF. L. REV. 1593, 1593–1600 (1987) (arguing “that current fourth amendment jurisprudence is impoverished and distorted by neglecting the ways in which privacy embodies chosen sharing”); Crocker, *supra* note 30, at 2–9 (explaining that current Fourth Amendment jurisprudence undermines “the conditions of ordinary personal life shared in the company of others, assumed to be secure in the blessings of liberty”).

134. 547 U.S. 103 (2006).

135. *Id.* at 106.

136. *Id.* at 111.

137. This was the case even if the other tenant was absent because police had arrested him and placed him in a police car nearby. *United States v. Matlock*, 415 U.S. 164, 166–67 (1974). *But see* *Chapman v. United States*, 365 U.S. 610, 611–18 (1961) (finding consent of landlord insufficient). For an overview of the development of the Supreme Court’s consent jurisprudence, see Tracey Maclin, *The Good and Bad News About Consent Searches in the Supreme Court*, 39 MCGEORGE L. REV. 27, 36–46 (2008).

138. *See, e.g.*, *Flippo v. West Virginia*, 528 U.S. 11, 12, 15 (1999) (per curiam) (vacationer had a reasonable expectation of privacy in cabin at state park); *Minnesota v. Olson*, 495 U.S. 91, 93 (1990) (overnight guest had reasonable expectation of privacy in host’s home); *O’Connor v. Ortega*, 480 U.S. 709, 712–14 (1987) (doctor had a reasonable expectation of privacy in his desk,

It is privacy that is protected by the Fourth Amendment, not solitude. A man enjoys Fourth Amendment protection in his home, for example, though his wife and children have the run of the place—and indeed, even though his landlord has the right to conduct unannounced inspections at any time. Similarly, in my view, one’s personal office is constitutionally protected against warrantless intrusions by the police, even though employer and co-workers are not excluded.<sup>139</sup>

Based on this case law, Professor Susan Brenner has argued that “these entities [digital service providers] are functionally analogous to ‘servants’ who are also encompassed by this conception of shared privacy; unlike the servants of centuries ago, they do not reside in the home, but they provide services that promote and sustain activities within the home.”<sup>140</sup> The fact that a servant, landlord, or other person providing services that might entail access to the home might see and report suspicious behavior to the police has never meant that there is no reasonable expectation of privacy barring the police from entering.<sup>141</sup>

In our digitally networked society, the protection of privacy, rather than solitude, necessitates a technosocial approach to the Fourth Amendment that continues on the path begun by *Katz*’s extension of protection to telephone calls, *Kyllo*’s protection against intrusion by devices not in general public use, and even earlier applications of Fourth Amendment protection to hotel rooms and shared offices. Once we move away from the aggressive third party doctrine, in which every activity involving a digital intermediary is open to law enforcement scrutiny (at least as far as the Constitution is concerned),<sup>142</sup> it will become necessary to

---

cabinets, and possibly some other parts of his office at a state hospital); *Stoner v. California*, 376 U.S. 483, 484 (1964) (warrantless search of defendant’s hotel room violates Fourth Amendment); *United States v. Jeffers*, 342 U.S. 48, 49–50 (1951) (warrantless search of hotel room rented and occupied by defendant’s aunts, where defendant had permission to use it and was given a key, was illegal); *McDonald v. United States*, 335 U.S. 451, 452–54, 456 (1948) (warrantless search of a rooming house was illegal where no exigent circumstances existed); *Gouled v. United States*, 255 U.S. 298, 304–06 (1921) (warrantless seizure of documents by stealth was illegal even though informant was invited into the office), *abrogated by* *Warden v. Hayden*, 387 U.S. 294 (1967); *see also* *Bellia & Freiwald*, *supra* note 10, at 152–53 (discussing and citing cases involving third parties and physical property).

139. 480 U.S. at 730 (Scalia, J., concurring in the judgment) (citing *Mancusi v. DeForte*, 392 U.S. 364, 369 (1968)) (finding Fourth Amendment rights in shared office).

140. Brenner, *supra* note 133, at 76.

141. *See id.* at 76–80 (“We trust our ‘servant’ entities not to reveal our personal information to tabloids, disgruntled relatives, and other ‘civilians,’ and they generally live up to our expectations.”).

142. There historically have been, and no doubt will continue to be, federal and state statutory protections and state constitutional protections over and above what the Fourth Amendment provides. *See, e.g.*, GINA MARIE STEVENS & CHARLES DOYLE, CONG. RESEARCH SERV., 7-5700, PRIVACY: AN OVERVIEW OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC

confront the issue of Fourth Amendment protection in the whole range of social contexts making up the integrated online-offline world.<sup>143</sup>

Recently, some courts have begun implicitly to recognize the need for such an analysis. Apparently aware of the sweeping implications of a blunderbuss approach to surveillance of digital intermediary records, these courts are increasingly disinclined to take a simplistic and aggressive third party doctrine approach. This rethinking is most apparent in the context of e-mail, which is closely analogous to *Katz*'s telephonic communication. Thus, while courts have generally followed *Smith* and *Miller* in finding no reasonable expectation of privacy in Internet subscriber information,<sup>144</sup> the few appellate opinions to consider the issue have found that Fourth Amendment protection extends to the content of digital communication despite intermediary storage.<sup>145</sup> Most recently, the United States Court of Appeals for the Sixth Circuit held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP'" and that a warrant is required to

---

EAVESDROPPING 1 (2009), available at <http://www.fas.org/sgp/crs/intel/98-326.pdf>; Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 374 (2006) (cataloging the Fourth Amendment protections in all fifty states, since the Fourth Amendment itself "provides only a 'constitutional floor'"). In this Article, I focus on the Fourth Amendment, though the considerations raised here should certainly also inform surveillance law in these other contexts.

143. For important work by privacy theorists emphasizing the importance of social context in evaluating privacy claims see, for example, NISSENBAUM, *supra* note 132; DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 89–100 (2008) (discussing the social value of privacy); Cohen, *Cyberspace*, *supra* note 35, at 219–20 (noting the interconnectedness of cyberspace and real space); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1374 (2000) [hereinafter Cohen, *Examined Lives*] (noting increasing "public concern about networked databases of personally-identified information"); Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 921 (2005) (proposing that courts should consider to what extent a reasonable person would expect dissemination of personal information after he discloses a private detail, rather than considering whether he reasonably expected his information would remain private).

144. See, e.g., *Rehberg v. Paulk*, 611 F.3d 828, 842–47 (11th Cir. 2010) (discussing privacy expectations in e-mail and summarizing case law finding no expectation of privacy in noncontent information), *cert. granted*, 2011 WL 940891 (U.S. Mar. 21, 2011); *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (holding that an individual does not have a protectable expectation of privacy in electronic subscriber information); *United States v. Perrine*, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (explaining that there is no Fourth Amendment privacy protection in subscriber information sent to Yahoo!), *cert. denied*, 131 S. Ct. 440 (2010); *United States v. Forrester*, 512 F.3d 500, 509–11 (9th Cir. 2008) (finding, by analogy to *Smith*'s treatment of telephone numbers, no protectable privacy interest in noncontent information and declining, on qualified immunity grounds, to decide whether e-mail content receives Fourth Amendment protection).

145. See *Rehberg*, 611 F.3d at 842–47 (reviewing case law addressing the questions of reasonable expectations of privacy in e-mail content and concluding that qualified immunity was appropriate because the law is not clearly established).

obtain such communications from the intermediary.<sup>146</sup> Similarly, though the Supreme Court did not address the issue in *Quon*, the Ninth Circuit had held below that there was a reasonable expectation of privacy in the text messages stored with a provider of pager communications.<sup>147</sup> The Supreme Court has yet to rule on the applicability of the Fourth Amendment to e-mail and text messaging, but the trend of appellate court rulings, along with the Supreme Court's conspicuous failure to rely on the third party doctrine for an easy out in *Quon*, suggests that the Court will, at a minimum, eventually adopt a content/noncontent distinction in the context of two-party communications,<sup>148</sup> despite some of the rhetoric of *Miller* and *Smith*.

While the emerging consensus around a content/noncontent distinction for e-mail and text messaging may provide a means to reconcile *Smith* and *Katz* for two-way digital communications, Professor Orin Kerr's suggestion in a recent article that it can provide a "general framework for applying the Fourth Amendment to the Internet"<sup>149</sup> is overstated. Not only is there a debate about the extent to which the content/noncontent distinction can be meaningfully applied to electronic communication,<sup>150</sup> but there is also a

---

146. *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (quoting *Warshak v. United States*, 490 F.3d 455, 473 (6th Cir. 2007)). An earlier ruling on this issue was vacated on ripeness grounds. *Warshak*, 490 F.3d 455, vacated *en banc*, 532 F.3d 521 (6th Cir. 2008).

147. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 904, 910–11 (9th Cir. 2008), *rev'd and remanded sub nom. City of Ontario v. Quon*, 130 S. Ct. 2619, 2629–33 (2010). As discussed above, the Supreme Court reversed the case without deciding the privacy issue on the basis that the search was reasonable even if *Quon* had a reasonable expectation of privacy. See *supra* text accompanying notes 2–6, 9.

148. Professor Kerr suggests that the content/noncontent distinction provides a means to map the Fourth Amendment to the Internet in a "technologically neutral" way—where content/noncontent replaces a physical distinction between inside and outside. Kerr, *A General Approach*, *supra* note 25 at 1018.

149. *Id.* at 1005.

150. This distinction may work reasonably well for e-mail, where "header" information plays a role roughly analogous to the address on the outside of a postal mail envelope, but the content/noncontent distinction begins to break down rather quickly once an individual moves beyond straightforward two-way communication, such as e-mail. See, e.g., Bellia & Freiwald, *supra* note 10, at 163 (rejecting the distinction between content and noncontent information); Freiwald, *supra* note 10, at [52] (asking whether "the Fourth Amendment deprive[s] noncontent data of protection while affording protection to content data"); Susan Freiwald, *First Principles of Communications Privacy*, 2008 STAN. TECH. L. REV. 3, ¶ 49, <http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf> (noting that the content/noncontent distinction has "authorized increasingly powerful surveillance methods without meaningful judicial oversight"); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 70 (2004) (criticizing the two category distinction of communications); Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1480 (noting that no liability for noncontent monitoring is unwise); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 741 (2008) (noting that "current Fourth Amendment and statutory schemes provide only weak checks" on the government's power to search); Matthew J. Tokson, *The Content/Envelope Distinction in Internet*

dearth of case law concerning the question of how to evaluate the Fourth Amendment status of online interactions that are not directly analogous to telephone or postal mail communication.<sup>151</sup> One recent, thoughtful district court opinion, *Crispin v. Christian Audigier, Inc.*<sup>152</sup> discussed the status of stored records of the social networking sites Facebook and MySpace under the Stored Communications Act (“SCA”) in response to a motion to quash a civil subpoena for Facebook and MySpace user records.<sup>153</sup> Congress enacted the Stored Communications Act in the mid-1980s to regulate access to certain kinds of stored digital content.<sup>154</sup> Its interpretation in the context of modern Internet activities has been the subject of much discussion by commentators and, to some extent, by courts.<sup>155</sup> Because the SCA requires

---

*Law*, 50 WM. & MARY L. REV. 2105, 2105 (2009) (noting that courts “have yet to offer a means of determining the content/envelope status of unique aspects of Internet communications”).

151. *But see* Romano v. Steelcase Inc., 907 N.Y.S.2d 650 (N.Y. 2010) (permitting discovery of social network postings in tort context over Fourth Amendment objection).

152. 717 F. Supp. 2d 965 (C.D. Cal. 2010).

153. 717 F. Supp. 2d at 973–91 (holding that the plaintiff was permitted to quash the subpoena seeking his information with respect to private messages sent on MySpace and Facebook).

154. Act of Oct. 21, 1986, Pub. L. No. 99-508, sec. 201, 100 Stat. 1848, 1860–68 (codified as amended at 18 U.S.C. §§ 2701–10 (2006)); *see also* Bellia & Freiwald, *supra* note 10, at 123 (discussing the origins of support for the government’s “oddly disparate treatment” of digital information).

155. *See, e.g.*, Bellia & Freiwald, *supra* note 10, at 172–74 (discussing the limited constraints on government under the SCA and the limited remedies available to victims under the Act); Patricia L. Bellia, *Surveillance Law Through Cyberlaw’s Lens*, 72 GEO. WASH. L. REV. 1375, 1436 (2004) (explaining how some of the SCA’s ideas are outdated, including the idea of remote computing sources, while conceptions of electronic storage under the SCA are too narrow); Clifford S. Fishman, *Technology and the Internet: The Impending Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations, and the Media*, 72 GEO. WASH. L. REV. 1503, 1535–42 (2004) (examining recent cases to demonstrate that the statute protects the rights of commercial enterprises to gather information on users by installing programs on their computers); Kerr, *A General Approach*, *supra* note 25, at 1025–29 (noting the lack of case law discussing the Fourth Amendment’s application to Internet communications and how the statute has drawn attention away from possible constitutional challenges); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 871–74 (2004) (noting the ability for legislatures, in contrast to courts, to be flexible in enacting technological regulations); Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1234–42 (2004) (using case law to demonstrate that the statute is too complex in some areas and underprotective in others); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1571–76 (2004) (highlighting the gap between the actual privacy provided by the SCA and society’s basic expectations and understandings of privacy); Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 299 (2008) (discussing how the government has kept little statistics on its use in comparison to the Wiretap Act); Paul K. Ohm, *Parallel-Effect Statutes and E-Mail “Warrants”*: *Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1610–16 (2004) (noting the procedural similarities and differences between the SCA and regular warrant procedures); Solove, *Digital Dossiers*, *supra* note 10, at 1141–42 (discussing the less stringent process for government officials to gain access to stored communications than the Fourth Amendment’s warrant requirement); Solove, *Fourth Amendment*,

less than a warrant to obtain stored records, its constitutionality in the modern context has been challenged.<sup>156</sup>

Without detailing the court's analysis under the SCA (which requires the making of subtle distinctions that may have made sense in the 1980s, but make little sense today), it is of interest to note that in analyzing the SCA issues the court carefully parsed the various types of interactions occurring on the relevant social networking sites—analagizing the private messaging capability to e-mail and the profile and wall postings available only to a group of authorized “friends” to postings on a private bulletin board system.<sup>157</sup> The court remanded to the magistrate for a review of the plaintiff's privacy settings to determine whether “the general public had access to plaintiff's Facebook wall and MySpace comments, or access was limited to a few.”<sup>158</sup> Although the district court in *Crispin* recognized that Facebook and MySpace accounts meld more than one type of social interaction—and that applying legal privacy protections requires an understanding of the distinctions—the court was constrained by the SCA context to focus on analogies to earlier forms of electronic communication.<sup>159</sup> The Fourth Amendment imposes no such constraint, making a more coherent technosocial approach possible.

Courts have also begun to consider whether there should be a reasonable expectation of privacy in location tracking information because of developments in tracking devices and co-evolving social reliance on location-based technology. Earlier cases involving locational tracking distinguished tracking on the open road from tracking in an individual's

---

*supra* note 10, at 770 (highlighting areas of ambiguity in the SCA regarding e-mail that has already been read by a user but has been left on an ISP server); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1282–85 (2004) (discussing the limited scope, protective standards, and less stringent enforcement of the SCA than other legislative acts); Peter P. Swire, *Katz Is Dead. Long Live Katz*, 102 MICH. L. REV. 904, 910–12 (2004) (explaining how the SCA could be applied to allow the government to have access to telephone calls); *see also generally* SLOBOGIN, *supra* note 10.

156. *See, e.g.*, Bellia & Freiwald, *supra* note 10, at 123–24 (noting that “no court ha[s] considered what constraints, if any, the Fourth Amendment prohibition of unreasonable searches and seizures imposes”); Kerr, *A General Approach*, *supra* note 25, at 1034, 1043 (“The Supreme Court's forceful rejection of a warrant exception for telephone bugging seems to extend naturally to the Internet.”); Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 393–97 (2009) (arguing that the Fourth Amendment extends to electronic communications, meaning that some provisions of the Electronic Communications Privacy Act allowing more government access without a warrant are unconstitutional).

157. *Crispin*, 717 F. Supp. 2d at 968–70 & n.9–10.

158. *Id.* at 991.

159. *Id.* at 973–91. For example, the court compared recent types of social interaction with cases dealing with e-mail, text messaging, electronic bulletin board services, and YouTube under the SCA. *Id.*

home. *United States v. Knotts*,<sup>160</sup> for instance, involved government tracking of a beeper that a manufacturer had placed in a container of chloroform (a chemical used in the manufacture of methamphetamine) prior to its sale to the defendant.<sup>161</sup> The Court compared the use of the beeper to enhance the government's ability to track the defendant on the open highways to the automation of telephone dialing discussed in *Smith*.<sup>162</sup> Notably, the Court limited *Knotts* a year later in *United States v. Karo*,<sup>163</sup> where the court held that the warrantless monitoring of a beeper similarly placed in a container was unconstitutional when government officials monitored the beeper while the container was in the defendant's home.<sup>164</sup>

Courts are currently grappling with the increasing ease of locational tracking,<sup>165</sup> which is driven by both technical changes (the ease of surreptitiously installing and tracking with GPS devices) and social changes (the availability of extrinsic location data from cell phone and smart phone providers and other Internet location-based applications).<sup>166</sup> For example, in a recent case considering the standard for issuing a court order to produce cell site location information ("CSLI") under the SCA, a Third Circuit panel reversed a lower court ruling that the statute requires a warrant based on probable cause, but remanded for the magistrate to exercise discretion as

---

160. 460 U.S. 276 (1983).

161. *Id.* at 277.

162. *Id.* at 280–84. Interestingly, the Court noted the defendant's argument that technologically enhanced tracking might lead to "twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision." *Id.* at 283 (quoting Brief for Respondent at 9, *Knotts*, 460 U.S. 276 (No. 81-1802)). The Court stated, however, that "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id.* at 284. The D.C. Circuit has recently returned to this issue and held that GPS tracking of an individual for a month without a warrant constituted an impermissible search under the Fourth Amendment. *United States v. Maynard*, 615 F.3d 544, 563, 566 (D.C. Cir. 2010), *cert. denied*, 131 S. Ct. 671 (2010).

163. 468 U.S. 705 (1984).

164. *Id.* at 715–17.

165. *See, e.g.*, *United States v. Pineda-Moreno*, 591 F.3d 1212, 1214–17 (9th Cir. 2010) (holding that installation of tracking device on underside of car in driveway and monitoring defendant's movements did not constitute search), *petition for cert. filed*, No. 10-7515 (U.S. Nov. 10, 2010); *United States v. Garcia*, 474 F.3d 994, 996–99 (7th Cir. 2007) (tracking defendant's car by means of GPS device did not constitute search).

166. For discussions of the issue see, for example, Bennett L. Gershman, *Privacy Revisited: GPS Tracking as Search and Seizure*, 30 PACE L. REV. 927, 960–63 (2010) (arguing that the use of GPS tracking attached to a motor vehicle intrudes upon a reasonable expectation of privacy under the Fourth Amendment); Afsheen John Radsan, *The Case for Stewart over Harlan on 24/7 Physical Surveillance*, 88 TEX. L. REV. 1475, 1490–95 (2010) (examining both duration and intensity of governmental action under the Constitution as related to terrorism); Ian James Samuel, *Warrantless Location Tracking*, 83 N.Y.U. L. REV. 1324, 1336–51 (2008) (arguing that warrants are constitutionally necessary in the use of many tracking techniques).

to whether to require a warrant.<sup>167</sup> The court also intimated that, under *Knotts* and *Karo*, there might be a Fourth Amendment problem if the records of location information revealed an individual's presence at home.<sup>168</sup> Notably, the court rejected the government's argument, which cited *Smith* and *Miller*, that "no CSLI can implicate constitutional protections because the subscriber has shared its information with a third party, i.e., the communications provider."<sup>169</sup> The court noted that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."<sup>170</sup>

In another recent opinion, *United States v. Maynard*,<sup>171</sup> the D.C. Circuit held that law enforcement officials violated the Fourth Amendment when they installed a GPS tracking device on the defendant's car and tracked him twenty-four hours a day for four weeks.<sup>172</sup> The court read *Knotts* to have "reserved the question" of prolonged surveillance by opining that "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."<sup>173</sup> The court in *Maynard* then held that the prolonged tracking involved in the case violated the Fourth Amendment.<sup>174</sup> Analogizing prolonged tracking to the disclosure of rap sheets found to violate the privacy exception to the Freedom of Information Act in the Supreme Court decision *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*,<sup>175</sup> the D.C. Circuit invoked a "mosaic theory"<sup>176</sup>:

The whole of one's movements over the course of a month is not constructively exposed to the public because, like a rap sheet, that whole reveals far more than the individual movements it

---

167. *In re Application of the U.S. for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304 (3d Cir. 2010) [hereinafter *CSI: Third Circuit*].

168. *See id.* at 312–13 (contrasting this case with others involving tracking devices and explaining that the location information here did not intrude upon residential privacy).

169. *Id.* at 317.

170. *Id.*

171. 615 F.3d 544 (D.C. Cir. 2010), *cert. denied*, 131 S. Ct. 671 (2010).

172. *Id.* at 556–57.

173. *Id.* at 556 (quoting *United States v. Knotts*, 460 U.S. 276, 284 (1983)).

174. *Id.* at 555–68 (holding that *Knotts* was not controlling and that the police action was a search because it interfered with the victim's expectation of privacy).

175. 489 U.S. 749, 780 (1989) (holding that the disclosure of FBI rap sheets was an unwarranted invasion of privacy).

176. *See Maynard*, 615 F.3d at 561–62 (describing the "'mosaic theory' often invoked by the Government in cases involving national security information" by stating that "'[w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene'" (quoting *CIA v. Sims*, 471 U.S. 159, 178 (1985))).

comprises. The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more.<sup>177</sup>

A district court in New York recently followed *Maynard's* reasoning in holding that obtaining historical cell site location information from a service provider without a warrant violated the Fourth Amendment.<sup>178</sup> In doing so, the court explicitly rejected the aggressive version of the third party doctrine under *Smith* and *Miller* and noted the importance of technosocial change in evolving Fourth Amendment jurisprudence:

As the Supreme Court acknowledged in *Quon* when it alluded to the progression from *Olmstead* to *Katz*, the Fourth Amendment's concept of an "unreasonable" intrusion into one's personal affairs, by its very nature, is not stuck in the amber of the year 1791. That concept must instead evolve along with the myriad ways in which humans contrive to interact with one another. As the threads that connect us are increasingly entrusted into the hands of strangers who promise to make those connections broader, more intimate, more efficient, and more productive, a jurisprudence that mechanically relies on that fact to disclaim the need for meaningful oversight of the government's investigative techniques unwisely abandons the critical and continuing task of identifying the expectations of privacy our society is prepared to recognize as reasonable.<sup>179</sup>

The issue, however, is not settled. Judge Posner, writing for a Seventh Circuit panel found that monitoring the movement of a car using a tracking device installed while the car was parked on the street did not constitute a search.<sup>180</sup> In response to arguments about the potential for massive surveillance if such monitoring is not a search, Judge Posner opined, "Should government someday decide to institute programs of mass

---

177. *Id.* The distinction between occasional and ongoing surveillance is also reflected in an earlier Fifth Circuit case involving video surveillance. *United States v. Cuevas-Sanchez*, 821 F.2d 248, 249–52 (5th Cir. 1987). In *Cuevas-Sanchez*, government agents had installed a video camera on a power pole overlooking the defendant's backyard. *Id.* at 249–50. Despite the fact that the videotaped area could have been visible to observers who chose to look in from the street or from the pole itself, the court held that the ongoing recording of activity in the yard constituted a search. *Id.* at 250–52. The court also held that the government had properly authorized the surveillance with a warrant in this case. *Id.*

178. *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 736 F. Supp. 2d 578, 581–96 (E.D.N.Y.) [hereinafter *CSI: Brooklyn*], *rev'd*, Order, *CSI: Brooklyn*, 736 F. Supp. 2d 578 (E.D.N.Y. Nov. 29, 2010) (No. 10-MC-0550), ECF No. 11.

179. *Id.* at 595–96.

180. *United States v. Garcia*, 474 F.3d 994, 998–99 (7th Cir. 2007).

surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search.”<sup>181</sup> Likewise, in *United States v. Pineda-Moreno*,<sup>182</sup> the Ninth Circuit recently held that location tracking did not constitute a search.<sup>183</sup> But, in an extensive and impassioned dissent from the denial of rehearing en banc, Chief Judge Kozinski, writing for five dissenters, expressed a very different perspective from that of Judge Posner, warning ominously,

There is something creepy and un-American about such clandestine and underhanded behavior. To those of us who have lived under a totalitarian regime, there is an eerie feeling of déjà vu. This case, if any, deserves the comprehensive, mature and diverse consideration that an en banc panel can provide. We are taking a giant leap into the unknown, and the consequences for ourselves and our children may be dire and irreversible. Some day, soon, we may wake up and find we’re living in Oceania.<sup>184</sup>

While there is no settled consensus about how to interpret the Fourth Amendment’s protections in light of evolving locational technology, it is at a minimum fair to say that the evolving case law in this area by and large rejects a wooden application of the aggressive third party doctrine. In seeking to understand how constitutional protections should apply to users of social media, courts can and should do the same by employing a technosocial continuity principle which looks to the social role played by a particular technology and not primarily to the nuts and bolts of its closest technological cousins. Because of the way in which digital technology has become seamlessly integrated with social and private life in the physical world, serious protection of Fourth Amendment interests requires courts to consider how paradigmatic protected contexts play out in the intertwined networked world and whether new technologically mediated social paradigms are equally worthy of protection.

#### V. AT HOME AND AT WORK ON THE WEB

This Part focuses on the ways in which digital networked media have become intertwined with, and conceptually indistinguishable from, core Fourth Amendment concerns involving the home and the office. The social changes occasioned by the technologies of social media and cloud

---

181. *Id.* (citing *Zurcher v. Stanford Daily*, 436 U.S. 547, 566 (1978)).

182. 591 F.3d 1212 (9th Cir. 2010), *petition for cert. filed*, No. 10-7515 (U.S. Nov. 10, 2010).

183. *Id.* at 1217.

184. *United States v. Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from the denial of rehearing en banc).

computing demand a rethinking of Fourth Amendment protection of these core arenas of private life.<sup>185</sup>

*A. Fourth Amendment Protection of Home and Office*

The quintessential arena of Fourth Amendment protection is undoubtedly the home.<sup>186</sup> The importance of the home in Fourth Amendment jurisprudence can hardly be overstated.<sup>187</sup> Because of the central importance of the home to Fourth Amendment doctrine, the Court has on many occasions considered to what similar contexts the protections of the Fourth Amendment should be extended. For example, the Court distinguished the protected “curtilage” surrounding a home from unprotected “open fields.”<sup>188</sup> The Court extended the protection of the Fourth Amendment to residences that are less permanent than a house and not owned by the resident, such as rooming houses,<sup>189</sup> rental units,<sup>190</sup> hotel rooms,<sup>191</sup> state park cabins,<sup>192</sup> and mobile homes.<sup>193</sup> The Court required

---

185. See Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 532 (2005) [hereinafter Kerr, *Searches and Seizures*] (“Although obvious analogies exist between searching physical spaces and searching computers, important differences between them will force courts to rethink the key concepts of the Fourth Amendment.”).

186. See, e.g., *Silverman v. United States*, 365 U.S. 505, 511–12 (1961) (discussing the history of the Fourth Amendment and the key significance of an individual’s home); *Georgia v. Randolph*, 547 U.S. 103, 115 (2006) (same); *Kyllo v. United States*, 533 U.S. 27, 31 (2001) (same). For particularly impassioned recent defenses of the importance of Fourth Amendment protection of the home, see also *United States v. Lemus*, 596 F.3d 512, 513 (9th Cir.) (Kozinski, C.J., dissenting), *cert. denied*, 131 S. Ct. 129 (2010); *United States v. Black*, 482 F.3d 1044, 1045 (9th Cir. 2007) (Kozinski, C.J., dissenting).

187. See, e.g., *United States v. Karo*, 468 U.S. 705, 714 (1984) (“At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable.”).

188. See *Dow Chem. Co. v. United States*, 476 U.S. 227, 239 (1986) (distinguishing “open areas of an industrial plant complex” from “curtilage”); *Oliver v. United States*, 466 U.S. 170, 181, 183–84 (1984) (concluding that an individual has no reasonable expectation of privacy in “open fields”); *Hester v. United States*, 265 U.S. 57, 59 (1924) (declining to extend Fourth Amendment protections to “open fields”).

189. See *McDonald v. United States*, 335 U.S. 451, 452, 455 (1948) (concluding that the Fourth Amendment protects a defendant in a rented room), *abrogated by Warden v. Hayden*, 387 U.S. 294 (1967).

190. See *Randolph*, 547 U.S. at 112 (discussing that a tenant’s Fourth Amendment rights were violated in a search); *Chapman v. United States*, 365 U.S. 610, 610, 618 (1961) (finding a Fourth Amendment violation in a search of petitioner’s rented home).

191. See *Stoner v. California*, 376 U.S. 483, 487–88 (1964) (finding the warrantless search of a hotel room unlawful despite the fact that officials conducted the search with the consent of a hotel clerk).

192. See *Flippo v. West Virginia*, 528 U.S. 11, 12, 14 (1999) (per curiam) (applying Fourth Amendment protection to individuals staying in a cabin at a state park).

193. See *Soldal v. Cook County*, 506 U.S. 56, 61 (1992) (holding that the Soldal’s mobile home was seized in violation of the Fourth Amendment). *But see California v. Carney*, 471 U.S.

warrants for administrative searches of homes,<sup>194</sup> and has recognized Fourth Amendment rights of those who share their homes with others<sup>195</sup> and of at least some residential guests.<sup>196</sup> Although the protection of privacy in the home is certainly not absolute,<sup>197</sup> the Court routinely cabins the ability even of those law enforcement agents who have obtained legitimate access to the home to rummage around its precincts indiscriminately.<sup>198</sup> Although the issue has come up less commonly in the case law, the Court also provides expansive protection to an individual's

---

386, 394–95 (1985) (concluding that because the mobile home in this instance was readily mobile and used as a vehicle, petitioner possessed reduced expectations of privacy).

194. See *Michigan v. Clifford*, 464 U.S. 287, 298 (1984) (demonstrating “the importance of prior judicial review of proposed administrative searches”); *Camara v. Municipal Court*, 387 U.S. 523, 534 (1967) (holding that “administrative searches . . . are significant intrusions upon the interests protected by the Fourth Amendment”).

195. See *Randolph*, 547 U.S. at 106 (“We hold that . . . a physically present co-occupant’s stated refusal to permit entry prevails, rendering the warrantless search unreasonable and invalid as to him.”); *Bumper v. North Carolina*, 391 U.S. 543, 546 (1968) (finding a Fourth Amendment violation where petitioner’s grandmother consented to search); *Amos v. United States* 255 U.S. 313, 317 (1921) (“The contention that the constitutional rights of defendant were waived when his wife admitted to his home the government officers, who came, without warrant, demanding admission to make search of it under government authority, cannot be entertained.”).

196. See *Minnesota v. Olson*, 495 U.S. 91, 93 (1990) (holding that police violated petitioner’s Fourth Amendment rights by searching a house where he was an overnight guest). *But see Minnesota v. Carter*, 525 U.S. 83, 89–91 (1998) (holding that the Fourth Amendment rights of nonovernight guests of an apartment, who were simply present for a business, rather than a personal, transaction, were not violated when a police officer looked through a window and saw respondents bagging cocaine).

197. See, e.g., *Brigham City v. Stuart*, 547 U.S. 398, 400, 406–07 (2006) (discussing the scope of the exigency exception to the warrant requirement); *Florida v. Riley*, 488 U.S. 445, 447–48, 452 (1989) (finding that the Fourth Amendment was not violated in surveillance of a partially covered greenhouse in a residential backyard); *California v. Ciraolo*, 476 U.S. 207, 210, 215 (1986) (holding that there was no reasonable expectation of privacy in garden viewable from navigable airspace); *United States v. Santana*, 427 U.S. 38, 42–43 (1976) (discussing the hot pursuit exception).

198. See *Maryland v. Buie*, 494 U.S. 325, 327–28 (1990) (requiring that an officer have articulable facts and reasonable inferences from those facts leading to a reasonable belief that a space (in this case, a basement) contained a dangerous thing or individual before making an unwarranted “protective sweep”); *Steagald v. United States*, 451 U.S. 204, 205–06, 222 (1981) (finding that the Fourth Amendment requires a search warrant to make a legal search of a third party’s home when law enforcement execute a warranted arrest in the third party’s home); *Mincey v. Arizona*, 437 U.S. 385, 387, 395 (1978) (finding a search impermissible even though a homicide had recently occurred in the apartment); *Chimel v. California*, 395 U.S. 752, 753–54, 768 (1969) (finding a violation of the Fourth Amendment where police officers obtained an arrest warrant, but not a search warrant, and had the occupants of the house open drawers and move items around to facilitate a search); *Gouled v. United States*, 255 U.S. 298, 304–06 (1921) (finding a violation of the Fourth Amendment where the searchers came under the guise of a personal visit), *abrogated by Warden v. Hayden*, 387 U.S. 294 (1967).

office, even if that office is shared with other workers or accessible by an employer.<sup>199</sup>

The primary exception to the solicitousness with which the Court treats the home and office arises in cases involving informants and undercover agents. The Court has routinely refused to grant Fourth Amendment protection against deception by informers and government agents.<sup>200</sup> The government's agents are free to gain consensual access to an individual's home or office (or, more generally, to her confidence) by deceit or to induce betrayal by his or her friends or associates.<sup>201</sup> No court has

---

199. *See, e.g.*, *O'Connor v. Ortega*, 480 U.S. 709, 718–19 (1987) (plurality opinion) (finding that a reasonable expectation of privacy in an office desk and cabinets); *See v. City of Seattle*, 387 U.S. 541, 545–46 (1967) (finding a warrant was needed when searching commercial property not open to the public). Moreover, no one has ever suggested that the government violates an individual's Fourth Amendment rights by the fact that various people are invited into an individual's home or office. Family, friends, neighbors, repair people, babysitters, housecleaners, and co-workers come and go, some may even be given keys and allowed access when the primary resident is not on the premises, yet the suggestion that this access leaves an individual's home open to warrantless search or surveillance by the police would be absurd. *See, e.g.*, *United States v. Hardin*, 539 F.3d 404, 407–08, 424–26 (6th Cir. 2008) (finding that a landlord, who at the time was acting as a government agent, did not obtain proper consent to enter by calling out “[m]aintenance” upon entering apartment).

200. *See, e.g.*, *United States v. White*, 401 U.S. 745, 751 (1971) (plurality opinion) (explaining that recording a conversation does not violate the Fourth Amendment where the conversation itself would not be protected); *Hoffa v. United States*, 385 U.S. 293, 302–03 (1966) (finding that the Fourth Amendment does not protect a wrongdoer's misplaced confidence); *Lewis v. United States*, 385 U.S. 206, 206–07, 212 (1966) (determining that the Fourth Amendment was not violated when a police officer misrepresented his identity and was invited into the petitioner's home under the pretense of a drug transaction); *Lopez v. United States*, 373 U.S. 427, 438 (1963) (finding that an illegitimate offer of a bribe to an IRS official who is in the defendant's home is not a constitutionally protected communication).

201. This doctrine is also sometimes called the third party doctrine. *See, e.g.*, Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 518–521 (2005) (discussing the development of the third party doctrine in Supreme Court case law); Kerr, *Case for the Third-Party Doctrine*, *supra* note 10 (advocating for the third party doctrine); Kerr, *Defending the Third Party Doctrine*, *supra* note 10 (same); Kate Vershov, *US v. Miller and “Voluntary” Data Handover, c. 2009*, COLUM. SCI. & TECH. L. REV. (Apr. 20, 2009), <http://www.stlr.org/2009/04/us-v-miller-and-voluntary-data-handover-c-2009> (discussing what the term “voluntary” means with respect to the third party doctrine). This is a bit of a misnomer since the informants and undercover officers involved are really second parties to the conversations that they report or permit to be monitored. The suggestion that the government can monitor conversations with the permission of one of the participants has not been taken to mean that privacy has been so vitiated by sharing information with another person that government can monitor the conversation directly without the permission of a party to the conversation. *See* Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What Katz Is Made Of?*, 41 U.C. DAVIS L. REV. 781, 813–15 (discussing how courts' holdings that conversations are unprotected when “there is a potential that an anonymous conversant may breach confidences” are “pav[ing] the way for holding that private chat room or instant message conversations may be monitored by the police, even when none of the participants has consented to interception”); Lawless, *supra* note 10, at 2–4 (explaining the current status of the third party doctrine and how it will need to be “retool[ed]” as technology continues to advance). This second party doctrine has itself been frequently criticized by commentators who emphasize its failure to

held that the Constitution protects against misplaced trust.<sup>202</sup> While this doctrine has held strong over the years (meaning that in the United States, unlike in Europe, for example, the regulation of undercover policing is almost entirely a matter for the executive<sup>203</sup>), a number of related issues have generated controversy.

For example, the Supreme Court narrowly held in *United States v. White*<sup>204</sup> that a government informant could permissibly wear a wire to transmit conversations to police agents.<sup>205</sup> This was the case even when the conversations took place in the defendant's home.<sup>206</sup> This controversial outcome led a number of states to take more protective positions (especially with regard to conversations in an individual's home) under their state constitutional provisions, requiring a warrant for electronic monitoring of conversations with an informant or undercover agent.<sup>207</sup>

Under Supreme Court precedent, although an informant or undercover agent can wear a wire, the scope of what she can do while in a suspect's home is circumscribed by the scope of that individual's consent to the informant's presence. For example, an early Supreme Court case held that an informant who is invited into a suspect's home or office cannot constitutionally seize documents she finds there.<sup>208</sup> Moreover, an

---

recognize the importance of shared privacy. See, e.g., Crocker, *supra* note 30, at 53–56 (2009); Coombs, *supra* note 133, at 1593–1600; Epstein, *supra* note 10, at 1202; see also generally Donald L. Doernberg, “Can You Hear Me Now?”: *Expectations of Privacy, False Friends, and the Perils of Speaking Under the Supreme Court's Fourth Amendment Jurisprudence*, 39 IND. L. REV. 253 (2006).

202. See *Hoffa*, 385 U.S. at 302 (“Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.”).

203. See, e.g., Jacqueline E. Ross, *Impediments to Transnational Cooperation in Undercover Policing: A Comparative Study of the United States and Italy*, 52 AM. J. COMP. L. 569, 586–91 (2004) [hereinafter Ross, *Impediments*]; Jacqueline E. Ross, *The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany*, 55 AM. J. COMP. L. 493, 512 (2007) [hereinafter Ross, *Covert Surveillance*].

204. 401 U.S. 745.

205. *Id.* at 752–53.

206. *Id.* at 747.

207. See, e.g., *Commonwealth v. Blood*, 507 N.E.2d 1029, 1034, 1037 (Mass. 1987) (finding it was “objectively reasonable to expect that conversational interchange in a private home will not be invaded” without a warrant); *State v. Goetz*, 191 P.3d 489, 504 (Mont. 2008) (finding warrantless recording and monitoring of conversations constituted a search and was prohibited under the state constitution); *Commonwealth v. Brion*, 652 A.2d 287, 287 (Pa. 1994) (prohibiting a confidential informant from recording and disclosing to police a conversation recorded within a suspect's home); *State v. Geraw*, 795 A.2d 1219, 1220 (Vt. 2002) (holding that the state constitution prohibits secret recordings of police interviews within a home); *State v. Mullens*, 650 S.E.2d 169, 190 (W. Va. 2007) (holding that failure to obtain a warrant for recording information conversations was a violation of the state constitution).

208. *Gouled v. United States*, 255 U.S. 298, 305–06 (1921), *abrogated by* *Warden v. Hayden*, 387 U.S. 294 (1967). *Warden v. Hayden*, overruled the “mere evidence” rule associated with that

informant cannot constitutionally plant an electronic “bug” in a suspect’s home (or even in a container that the suspect will herself bring into the home)<sup>209</sup> in order to monitor conversations occurring in the informant’s absence. Permissible electronic monitoring is limited to that which would confirm what the agent or informant would be able to report firsthand.<sup>210</sup>

*B. The Social Significance of New Social Media and Cloud Computing: Technosocial Extension of the Home and Office*

As illustrated by the hypothetical that began this Article, social media and cloud computing have affected the social space of the home and office profoundly, and the effects promise to become even more significant as these technologies evolve. Not long ago, the home and office were the primary storage areas for personal documents of all kinds.<sup>211</sup> In the case of the home, these documents often included financial records (including check books, personal cash account records, telephone and electrical bills), health records, personal correspondence, diaries, appointment books, photographs and other “keepsake” documents, perhaps attempts at “creative writing,” newspaper and magazine clippings, brochures for entertainment options, and more. Now, many of these records have moved to the personal computer or laptop.<sup>212</sup> The advent of cloud computing and

---

case, 387 U.S. at 309–10, but the limitation on informants’ constitutional ability to search and seize remains, *see, e.g.*, *Ferguson v. City of Charleston*, 532 U.S. 67, 84–85 (2001) (finding a warrantless informant-recorded conversation approach inconsistent with the Fourth Amendment); *Club Retro, L.L.C. v. Hilton*, 568 F.3d 181, 197, 201 (5th Cir. 2009) (listing three specific criteria required for a permissible warrantless search of a business).

209. *United States v. Karo*, 468 U.S. 705, 713, 716–18 (1984).

210. *See White*, 401 U.S. at 751 (“If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant’s constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others . . . to whom the defendant is talking and whose trustworthiness the defendant necessarily risks.”); *see also Karo*, 468 U.S. at 715 (noting that it is a violation of the Fourth Amendment when, “without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house”).

211. *See, e.g.*, Liz Szabo, *High-Tech “Scribes” Help Transfer Medical Records into Electronic Form*, USA TODAY (Oct. 7, 2009, 1:54 PM), [http://www.usatoday.com/news/health/2009-10-06-electronic-medical-records\\_N.htm](http://www.usatoday.com/news/health/2009-10-06-electronic-medical-records_N.htm) (confirming that “[w]hile most other businesses scrapped their paper files decades ago, hospitals have lagged” and are still transitioning their files from paper to digital).

212. The search and seizure of personal computers raise thorny Fourth Amendment issues. *See, e.g.*, Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 39–43 (2002), <http://www.mtlr.org/voleight/Brenner.pdf>; Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700 (2010); Kerr, *Searches and Seizures*, *supra* note 185, at 531–35; Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 STAN. TECH. L. REV. 2, <http://stlr.stanford.edu/pdf/ohm-olmsteadian-seizure-clause.pdf>.

the demands of a mobile society for easy remote access to all of these records make it likely that in the future many, if not most, personal records of this type will be stored online “in the cloud.”<sup>213</sup> It will barely be evident to users where the bits and bytes representing the documents are physically stored.<sup>214</sup> Although books, CDs, and DVDs are unlikely to disappear completely any time soon, more and more individuals will maintain large fractions of their personal libraries electronically.<sup>215</sup> These items, too, often will be stored in the cloud.<sup>216</sup>

Social media promise to change the face of social relationships at least as drastically.<sup>217</sup> While nothing may ever replace a dinner at home with family and friends, social media provide other ways to converse, to play games, to pursue hobbies, to share entertainment and to meet for purposes ranging from political activism to business planning to romantic intimacy.<sup>218</sup> Often these social media supplement interactions in the physical world or permit them to continue even when families, friends, and associates are physically separated.<sup>219</sup> Akin to earlier pen pal relationships,

213. See Memorandum from John B. Horrigan, Assoc. Dir. for Research, Pew Internet & Am. Life Project on Use of Cloud Computing Applications and Servs. 1 (Sept. 2008), available at [http://www.pewinternet.org/~media/Files/Reports/2008/PIP\\_Cloud.Memo.pdf.pdf](http://www.pewinternet.org/~media/Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf) (indicating that of September 2008, sixty-nine percent of American Internet users already used at least one form of cloud computing).

214. Cf. Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83, 85 (2006), [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=916046](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=916046) (discussing the increasing use of computers as “workstations” and noting that most individuals will have a “first-order reasonable expectation of privacy for e-mail stored on their behalf” by third parties).

215. See, e.g., Joel Selvin, *MP3 Music—It’s Better than It Sounds*, SFGATE.COM (Aug. 8, 2007), [http://articles.sfgate.com/2007-08-08/entertainment/17255506\\_1\\_audio-quality-recording-studios-mp3](http://articles.sfgate.com/2007-08-08/entertainment/17255506_1_audio-quality-recording-studios-mp3) (explaining how CDs are “on [their] way out [as] . . . computer files tak[e] over as the primary means of hearing recorded music”).

216. See Memorandum, Horrigan, *supra* note 213.

217. Joe Thomas, *Social Networking Sites’ Effect on Relationships Among College Students*, ASSOCIATED CONTENT (Oct. 1, 2007), [http://www.associatedcontent.com/article/393599/social\\_networking\\_sites\\_effect\\_on\\_relationship\\_s.html?singlepage=true&cat=41](http://www.associatedcontent.com/article/393599/social_networking_sites_effect_on_relationship_s.html?singlepage=true&cat=41) (confirming that “[t]echnology is slowly taking over people’s lives and beginning to effect [sic] their personal relationships”).

218. See, e.g., EHARMONY, <http://www.eharmony.com> (last visited Mar. 5, 2011) (dating); FACEBOOK, <http://www.facebook.com> (last visited Mar. 5, 2011) (introducing friends); HUFFINGTON POST, <http://www.huffingtonpost.com> (last visited Mar. 5, 2011) (political activism); REDSTATE, <http://www.redstate.com> (last visited Mar. 5, 2011) (political activism); SECOND LIFE, <http://secondlife.com> (last visited Mar. 5, 2011) (games, hobbies, and entertainment); SKYPE, <http://www.skype.com> (last visited Mar. 5, 2011) (business planning); TWITTER, <http://www.twitter.com> (last visited Mar. 5, 2011) (different means of conversation within a social group); YOUTUBE, <http://www.youtube.com> (last visited Mar. 5, 2011) (photo and video sharing).

219. See, e.g., Facebook, FACEBOOK, <http://www.facebook.com/facebook?sk=info> (last visited Mar. 5, 2011) (describing how Facebook gives “people the power to share and make the world more open and connected”); *Skype Ushers in New Era in Face-to-Face Online Video Communication*, SKYPE (Jan. 5, 2011),

these media permit social relationships that cross barriers of distance and culture.<sup>220</sup> Social media also provide means for people with similar interests and concerns to find one another.<sup>221</sup> Sometimes these uses are very personal, involving medical problems, sexual concerns, or exploration of unpopular political perspectives.<sup>222</sup> New varieties of social media seem to crop up almost daily and there is no telling which will become inextricable pieces of daily life for a sizable number of citizens.<sup>223</sup>

Social media can be very important enablers of social relationships not only for people who are physically separated from their friends but also for those, like our hypothetical friend Moira, who are unable to avail themselves of “real space” privacy, often because financial circumstances dictate that they live in close quarters with others.<sup>224</sup> Thus, social media provide the potential to redress some of the inequitable effects of the focus on the home and office as loci of private life.<sup>225</sup>

None of this is to suggest that the physical home and office do not continue to play central roles in social and private life. The point is that those traditional roles are becoming intertwined with the digital world and

---

[http://about.skype.com/press/2010/01/new\\_era\\_in\\_face\\_to\\_face.html](http://about.skype.com/press/2010/01/new_era_in_face_to_face.html) (describing how “Skype is software that enables the world’s conversations”).

220. See, e.g., *supra* note 219.

221. Of course, there is no denying that social media can also facilitate undesirable—and criminal—social behavior. See, e.g., Kerr, *Case for the Third-Party Doctrine*, *supra* note 10; see also, e.g., THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION (Saul Levmore & Martha C. Nussbaum eds., 2010).

222. See, e.g., *About*, THE RED PHOENIX, <http://theredphoenix.wordpress.com/about> (last visited Mar. 6, 2011) (American Party of Labor blog); *Be a Part of the WebMD Community*, WEBMD, <http://exchanges.webmd.com/default.htm> (last visited Mar. 6, 2011) (public discussion forum available about medical problems); *WebMD Sexual Health Community*, WEBMD, <http://exchanges.webmd.com/sex-and-relationships-exchange> (last visited Mar. 6, 2011) (public discussion forum available about sexual concerns).

223. See *List of Social Networking Websites*, WIKIPEDIA, [http://en.wikipedia.org/wiki/List\\_of\\_social\\_networking\\_websites](http://en.wikipedia.org/wiki/List_of_social_networking_websites) (last visited Mar. 6, 2011) (providing a nonexhaustive, but extensive, list of “notable, well-known sites,” excluding online dating websites).

224. See danah boyd, *Why Youth [Heart] Social Network Sites: The Role of Networked Publics in Teenage Social Life*, in YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 137–38 (David Buckingham ed., 2008) (describing teens’ use of online social network profiles to harness mediated publics and develop their social identities).

225. See Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 404–05 (1974) (discussing the disparate impact of Fourth Amendment protections for individuals who live in single houses or well-insulated apartments in comparison to tenements); Stephanie M. Stern, *The Inviolable Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 923 (2010) (noting that the judicial preference for protecting the home over other spaces unfairly affects low income individuals who spend more time in public, as well as residents of mobile motor homes); William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1265–66 (1999) (asserting that protections under the Fourth Amendment unfairly benefit wealthy, white criminals by only applying to certain kinds of spaces).

that this development is the result of a complicated evolution of culture, transportation technology, digital storage technology, communication technology, social norms, and more. The time is fast approaching—and is probably already here—when it will be impossible to understand what happens in the home or office without understanding the way in which these environments are intertwined with the digital world and hence with third party servers.<sup>226</sup>

To determine to what degree this affects the values traditionally guarded by the Fourth Amendment's solicitude toward the home and the office, it is important to tease out what this solicitude is protecting. What is it about the home and the office that make them the historical bastions of Fourth Amendment protection? Unfortunately, on this point one gets little help from either the case law or the scholarly literature.<sup>227</sup> The cases may wax poetic about the importance and even the "sanctity" of the home and its privacies (and emphasize, though perhaps with less poetry, the importance of the office), but the importance of privacy at home and in the office are largely unexplained, being deemed, no doubt, self-evident.<sup>228</sup> Legal scholarship delving into the connection between privacy (or other Fourth Amendment values) and the home is scant, though some scholars recently have begun the inquiry.<sup>229</sup> Professor Benjamin Barros, for example, has recently argued for a more thorough examination of the psychology of the home as it relates to a number of legal concepts, but concludes that the necessary psychological studies are for the most part yet to be done.<sup>230</sup>

Professor Stephanie Stern has argued that the privileging of the home in Fourth Amendment jurisprudence has distorted the law, led to underprotection of privacy away from the home, and is inconsistent with

---

226. There is some potential for this to change once again so as to put more or less of the stored data physically within the premises of the owner of the data or of dispersed peers. See *The Project*, DIASPORA, <https://joindiaspora.com/> (last visited Mar. 6, 2011) (presenting the opportunity for Diaspora users to share and control data dispersed throughout the Internet); Audio & Video: Eben Moglen, *Freedom in the Cloud: Software Freedom, Privacy and Security for Web 2.0 and Cloud Computing*, Address Before the Internet Society, New York Chapter (Feb. 5, 2010), <http://www.isoc-ny.org/?p=1338> (discussing alternatives to centralized servers for social media and cloud computing). The technosocial continuity principal would continue to apply when and if these possibilities are realized.

227. See *supra* notes 10–15 and accompanying text (discussing the judiciary's reluctance to account for advancements in technology).

228. See *Kyllo v. United States*, 533 U.S. 27, 37 (2001) (discussing the Fourth Amendment sanctity of the home and the protections of all intimate details in the home); *Payton v. New York*, 445 U.S. 573, 601 (1980) ("[R]espect for the sanctity of the home . . . has been embedded in our traditions since the origins of the Republic.").

229. See, e.g., D. Benjamin Barros, *Home As a Legal Concept*, 46 SANTA CLARA L. REV. 255, 255–56 (2006) (discussing the privacy implications of a physical home and "the psychology of [a] home").

230. *Id.* at 276–300.

psychological evidence demonstrating that “[h]igh-quality relationships, not the physical home or residential privacy, are what is essential to self and psychosocial functioning.”<sup>231</sup> She rightly points out that an overly rigid adherence to the goal of protecting the physical home could lead to a neglect of precisely the types of digital information discussed in this Article.<sup>232</sup> She throws the baby out with the bathwater, however, when she proposes “replacing the expansive and formalistic protection of the physical home, and the rhetoric surrounding residential privacy, with a doctrinal focus on substantive privacy and intimate association.”<sup>233</sup> The idea that the home is deserving of particular protection against government intrusion is deeply embedded in jurisprudence, culture, and popular and legal intuition. Rather than root it out, we should build upon it in a technosocially continuous manner.

While undertheorized, the special solicitude for the home and office appears to have its roots in a number of social functions these places perform that enhance substantive privacy and intimate association. The home has been protected as a place for solitude and intellectual activity, a locus of family and other private relationships,<sup>234</sup> and a realm of individual autonomy and choice.<sup>235</sup> For these reasons, government intrusion is particularly offensive because the home aggregates so many of the pieces of an individual’s life into a complete picture which an individual may not

---

231. Stern, *supra* note 225, at 928–29; *see also* Stephanie M. Stern, *Residential Protectionism and the Legal Mythology of Home*, 107 MICH. L. REV. 1093, 1097 (2009) (“The central claim of this Article is that the psychological and social benefits of remaining in a particular home do not warrant the vast apparatus of categorical protections that pervade American property law.”).

232. Stern, *supra* note 225, at 918.

233. *Id.* at 938; *see also* Coombs, *supra* note 133, at 1593–96 (arguing that relational privacy should have a place at the center of Fourth Amendment jurisprudence in light of current neglect of how “chosen sharing” embodies privacy).

234. I say private here rather than intimate because I believe that some of the relationships protected by the jurisprudence of the home and office are private, but not necessarily intimate. Relationships with business partners, or with fellow members of political, religious, or cultural groups (which often meet in homes), are important private relationships but might not accurately be characterized as intimate.

235. Here, I am well aware of the gendered nature of this assertion. While a man’s house may be his castle, a woman’s home has frequently been her prison. Nonetheless, it is important to recognize that these values are associated with the home and office and intended to be protected by Fourth Amendment protection of those places. Indeed, those who live partly on the web may be able to introduce these values into their lives through the homes they make for themselves online more effectively than they may introduce them into their physical residences. This is an argument for extension of the treatment of home to certain online contexts rather than an argument against viewing the Fourth Amendment’s protection of the home as promoting autonomy values. For discussions of issues of gender, domestic abuse, and privacy, *see, for example*, ANITA L. ALLEN, *UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY* 58–81 (1988); Ruth Gavison, *Feminism and the Public/Private Distinction*, 45 STAN. L. REV. 1, 1 (1992); Reva B. Siegel, “*The Rule of Love*”: *Wife Beating as Prerogative and Privacy*, 105 YALE L.J. 2117, 2150–70 (1996).

wish to share with just anyone.<sup>236</sup> The office shares many of these attributes although, of course, the relationships it fosters are less personal.

Just like hotel and guest rooms, cloud computing arrangements and social media of various kinds share many (but not all) of the attributes that motivate strong Fourth Amendment protection of the home and office. These technologies are potentially the technosocial extensions of our homes and offices and, like hotel rooms and curtilages, need Fourth Amendment protection.<sup>237</sup>

Whether a particular arrangement is or is not a technosocial extension of the home or office may depend on two types of contextual factors: (1) those relating to the structure of the particular technology (Facebook, for example, has a very different structure than Twitter), and (2) those relating to the particular uses to which an individual puts the technology (some people are selective about Facebook friends and careful with their privacy settings while others are not, for instance). Implementing the principle that cloud computing and social media may be technosocially equivalent to the home and office will mean selecting a particular level of granularity at which to determine whether Fourth Amendment protection applies. The current implementation of protection for the home is at a high level of abstraction, as is evident in *Kyllo*'s application of Fourth Amendment protection to thermal imaging.<sup>238</sup> Some people may not use their homes (and certainly not their hotel rooms) for particularly private activities. Nonetheless, the Court takes a categorical approach. It is the fact that the home provides the *potential* base for a fulfilling private and social life that makes it worthy of strong Fourth Amendment protection.<sup>239</sup> As the Court pointed out in *Kyllo*, that potential would be disrupted if the government could peer in without notice to see whether the occupants were using the home to its full privacy potential.<sup>240</sup>

A similarly categorical approach would be appropriate to applying the Fourth Amendment in the context of cloud computing and social media.

---

236. See, e.g., ALAN F. WESTIN, *PRIVACY AND FREEDOM* (1967); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002).

237. See *supra* note 10 (citing articles criticizing the lack of Fourth Amendment protection for some digital information).

238. Compare *Kyllo v. United States*, 533 U.S. 27, 40 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore the details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."), with *Stern*, *supra* note 225, at 908 ("[P]rivileging the physical home has adulterated Fourth Amendment doctrine by extending the home's expansive 'umbrella' of Fourth Amendment protection beyond the relational and domestic core of residential spaces.").

239. See *Barros*, *supra* note 229.

240. See *Kyllo*, 533 U.S. at 37–40 ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.").

Storing files in a password-protected portion of the cloud accessible only to a limited number of people should be the equivalent of storing them in a file cabinet in an individual's office or home (or putting them in a locked storage container).<sup>241</sup> The government should need a warrant to look at them. Moreover, this common situation illustrates that the content/noncontent distinction, advocated by some as a way to handle information privacy, is unhelpful outside of the communication context.

Noncontent information, such as the number or types of files an individual has, should be protected from warrantless government scrutiny just as it would if the files were stored in a home or office. The importance of this point is evident when one thinks of one form of cloud storage that many individuals are likely to use: archives of e-books. Prior to the advent of e-book readers, the government would need a warrant to look at one's personal library—even if only to count the books.<sup>242</sup> Certainly, the government would need a warrant to look at the titles. Even more personal, of course, is information about where a person has placed her bookmark and which books she is currently actively reading. None of this is communication content in any ordinary sense of the term, but surely it should be protected under a principle of technosocial continuity.<sup>243</sup>

A content/noncontent distinction will not draw the appropriate line in these cases, and is unnecessarily complicated in these contexts. Storage in the cloud is a fairly straightforward extension of Fourth Amendment protection if one acknowledges its social equivalence to storage at home or in the office, rather than struggling to determine whether book titles and page numbers are content. Cloud computing, which includes not just data storage but also data processing, may raise somewhat more difficult issues. Technosocial continuity demands at the very least that a mere relocation of calculations from an account book to a personal computer and then to the cloud not undermine Fourth Amendment protections.

The question of how to deal with the growing variety of social media is more difficult. Nonetheless, it may still be possible to determine

---

241. For discussions of privacy issues relevant to cloud computing, see, for example, Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. REV. COLLOQUY 1 (2008), <http://www.law.northwestern.edu/lawreview/colloquy/2008/25/LRColl2008n25Picker.pdf>; Sarah Salter, *Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages*, 32 HASTINGS COMM. & ENT. L.J. 365 (2010); Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. ON TELECOMM. & HIGH TECH. L. 359 (2010); Zittrain, *supra* note 214; David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205 (2009).

242. See generally *supra* notes 186–199 and accompanying text (discussing Fourth Amendment protections for the individual home and its contents).

243. For critiques of the content/noncontent distinction, see *supra* note 150.

categorically, from the structure of a given social media platform, whether it is acting as an extension of the home or office. Generally, if the “occupant” of the site controls access, and does not make it accessible to the public at large, requiring that law enforcement officials obtain a warrant in order to search the activity records of the site seems reasonable.<sup>244</sup> The fact that the occupant of the site is not the owner of the servers that maintain the data may be no more relevant than the fact that the resident of a rented apartment or hotel room is not the owner of that property.<sup>245</sup>

Nor should it be decisive that the provider of a social media platform has access to the site for certain purposes, such as maintenance or automated parsing of the site to provide personalized advertising.<sup>246</sup> Though no direct analog to personalized advertising existed in earlier contexts involving privacy of the home or office, it is nonetheless entirely consistent with earlier treatment of the home to note that private arrangements allow entrance of property “management” for various purposes related to the terms under which access to the property is permitted. Those private arrangements do not undercut the constitutional treatment of a particular location as a home, office, or hotel room, and that access is not understood to give the landlord or hotel owner carte blanche to permit law enforcement officials to rummage through a residence or office. Nor do most cases considering the Fourth Amendment status of various places spend time carefully reading the leases and private contracts that control the arrangements between those who reside or work in a rented space and the “platform providers.”<sup>247</sup>

---

244. See, e.g., cases cited *supra* note 199 (noting two cases, *O'Connor v. Ortega*, 480 U.S. 709 (1987), and *See v. City of Seattle*, 387 U.S. 541 (1967), where sequestering an area away from the public created a reasonable expectation of privacy under the Fourth Amendment).

245. See *supra* note 199 (citing *O'Connor* where the building and cabinets were owned by the state employer, but where the expectation of privacy was reasonable under the Fourth Amendment).

246. This point may require rethinking of the dictum in *Smith* that the phone company’s automation of telephone dialing was irrelevant to the determination that there is no reasonable expectation of privacy in phone numbers. That point, awkwardly made in the opinion, is better understood as supporting a distinction between addressing information and content for communications. See Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581 (2011) (arguing that courts should interpret the Fourth Amendment as drawing a line with regard to third party exposure between automated processing and exposure to humans). While there are problems with automated data processing, see, e.g., Danielle Keats Citron, *Fulfilling Government 2.0’s Promise with Robust Privacy Protection*, 78 GEO. WASH. L. REV. 822 (2010) [hereinafter Citron, *Fulfilling Government 2.0’s Promise*]; Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008), individuals adapt their social behavior and expectations of privacy in response to whether they believe an automated system or a human being is monitoring them.

247. When determining the validity of *consent* to a government search, courts do concern themselves with details of the access permitted to those, such as family, roommates, co-workers, and employers, who have some rights to co-occupy a particular home or office. Social network

For this reason, whether to treat a particular social media platform as an extension of the home or office should depend primarily on whether the platform generally is set up for the kinds of social interactions typical of a home—conversation, sharing of photos and other items of interest, playing games and so forth—and whether the individual “residing” at the site has granted access to the public at large or maintained control over who can enter. The district court in *Crispin v. Christian Audigier, Inc.* asked the appropriate question in its SCA analysis: whether, “assuming privacy settings are optional, [the ‘resident’] chose privacy settings that would support a finding that his [social media sites are] sufficiently restricted that they are not readily available to the general public.”<sup>248</sup> Just as in determining whether to treat a physical space as a residence, the Supreme Court should not inquire too closely into the specific uses an individual chooses to make of an online social space; an individual does not have a lesser basic expectation of privacy against the government in her home simply because she gives frequent parties or has a large number of guests.<sup>249</sup>

Similarly, the detailed privacy settings an individual has chosen—as long as they are restrictive against the general public—should not necessarily determine whether she resides at her social media site.<sup>250</sup> As the *Crispin* court said in the related context of the SCA:

---

providers, however, are more appropriately analogized to landlords than to roommates or employers. On the other side, when courts have been inclined to find no Fourth Amendment protection—as in *United States v. Miller*, in particular—they have not been persuaded by arguments that the parties had entered into confidentiality arrangements. 425 U.S. 435, 440–41 (1976). *Miller* may have been wrong in analyzing bank records as “business records of the banks” and “negotiable instruments to be used in commercial transactions” and comparing them to information imparted in conversation rather than the analog of private papers. *Id.* at 440–42. A similar analysis in today’s world of ATMs and online banking might weigh even more heavily in favor of treatment of bank records as the technosocial equivalents of private “papers.” Ohm, *supra* note 150, at 1421–47 (“calling for a ban on at least the most invasive forms of ISP monitoring”). Whatever the outcome of such an analysis would or should be, the point remains that the result is not dictated entirely by the details of the parties’ “terms of service.”

248. 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

249. The Court does, however, consider whether a person has essentially turned his home into a commercial venue for illegal activities. See, e.g., *Minnesota v. Carter*, 525 U.S. 83, 90–91 (1998) (“Respondents . . . were obviously not overnight guests, but were essentially present for a business transaction and were only in the home a matter of hours.”); *Lewis v. United States*, 385 U.S. 206, 211 (1966) (“But when, as here, the home is converted into a commercial center to which outsiders are invited for purposes of transacting unlawful business, that business is entitled to no greater sanctity than if it were carried on in a store, a garage, a car, or on the street.”). This distinction seems to have influenced the Court’s approach to the informant cases. See, e.g., *United States v. White*, 401 U.S. 745, 752 (1971) (“Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his.”).

250. Note that available privacy settings may be subject to frequent change and may permit more or less granular determinations of who is given access to what pieces of an individual’s

Although here a large number of users, i.e., all of plaintiff's Facebook friends, might access the storage and attendant retrieval/display mechanism, the number of users who can view the stored message has no legal significance. Indeed, basing a rule on the number of users who can access information would result in arbitrary line-drawing and likely in the anomalous result that businesses such as law firms, which may have thousands of employees who can access documents in storage, would be excluded from the statute.<sup>251</sup>

A categorical approach based on the type of platform and whether the account owner has closed it off from public view is the best starting point for determining whether a cloud computing or social media account generally warrants treatment as a technosocial extension of the home or office.

*C. Beyond the Third Party Doctrine: Plain View and Undercover Cops on Social Media and in the Cloud*

Determining that a social media site is the technosocial extension of a home or office, and therefore concluding that the Fourth Amendment would generally require a government agent to obtain a warrant in order to gain access to the site through the platform providers, is only the very beginning of the inquiry. Once the overly aggressive interpretation of the third party doctrine is jettisoned, we are left to confront the same kinds of questions that have occupied courts for years with regard to privacy in the home or office. There are many such questions: issues of exigency, particularity of warrants and scope of search, third party consent, the plain view doctrine, and the activities of undercover police or informants. Full treatment of these issues is well beyond the ambitions of this Article, but in this Section, I will briefly tackle two of them: the plain view doctrine and undercover policing.

*1. Plain View Online*

The plain view doctrine draws the sensible conclusion that the Fourth Amendment does not require law enforcement to close its eyes against things in the line of public view (or in the line of view of someone with legitimate access) even if the items or activities in view are within a

---

social network site. See, e.g., Riva Richmond, *A Guide to Facebook's New Privacy Settings*, N.Y. TIMES: GADGETWISE (May 27, 2010, 4:41 PM), <http://gadgetwise.blogs.nytimes.com/2010/05/27/5-steps-to-reset-your-facebook-privacy-settings/> (noting that "[w]ith the changes it announced Wednesday in its privacy settings, Facebook will soon be giving users significantly more control over their information").

251. *Crispin*, 717 F. Supp. 2d at 990.

home.<sup>252</sup> This means, for example, that if a member of the public could legitimately see into a home from any vantage point outside of the curtilage, including an overflying airplane, government agents are permitted to do the same. The plain view doctrine permits government agents to use generally available aids to perception, such as flashlights,<sup>253</sup> binoculars,<sup>254</sup> and cameras,<sup>255</sup> to enhance their ability to see what is in plain view without treading on Fourth Amendment rights. At some point, however, the government's use of technological aids in observing a home crosses over into a Fourth Amendment search for which a warrant is required.<sup>256</sup> The Supreme Court recently elaborated on the question of "how much technological enhancement of ordinary perception from [a plain view] vantage point, if any, is too much."<sup>257</sup> In *Kyllo*, the Court held that the use of a thermal imaging device to "view" heat patterns within a home was a Fourth Amendment search, opining that "[w]here, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."<sup>258</sup> How should courts translate the plain view doctrine—along with the limits established by *Kyllo* and other precedent—to the context of social media and cloud computing?

---

252. See, e.g., *Florida v. Riley*, 488 U.S. 445, 450 (1989) ("Because the sides and roof of his greenhouse were left partially open, however, what was growing in the greenhouse was subject to viewing from the air."); *California v. Ciraolo*, 476 U.S. 207, 211–12 (1986) ("Yet a 10-foot fence might not shield these plants from the eyes of a citizen or a policeman perched on the top of a truck or a two-level bus."); *Washington v. Chrisman*, 455 U.S. 1, 5–6 (1982) ("The 'plain view' exception to the Fourth Amendment warrant requirement permits a law enforcement officer to seize what clearly is incriminating evidence or contraband when it is discovered in a place where the officer has a right to be."). But see *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (limiting the plain view doctrine to technology in general public use).

253. See, e.g., *United States v. Dunn*, 480 U.S. 294, 305 (1987) (noting that it is "'beyond dispute' that the action of a police officer in shining his flashlight to illuminate the interior of a car, without probable cause to search the car, 'trenched upon no right secured . . . by the Fourth Amendment'" (alteration in original) (quoting *Texas v. Brown*, 460 U.S. 730, 739–40 (1983) (plurality opinion))).

254. See, e.g., *United States v. Grimes*, 426 F.2d 706, 708 (5th Cir. 1970) (explaining that an investigator's observation of appellant placing cardboard boxes in a car through binoculars "did not constitute an illegal search").

255. See, e.g., *Dow Chem. Co. v. United States*, 476 U.S. 227, 239 (1986) ("We hold that the taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment.").

256. Another limit on the plain view doctrine is that the information obtained must really be in plain view. A law enforcement officer legitimately within a residence, but without a warrant of sufficient scope, may not open drawers to look for documents or even turn over a piece of stereo equipment to look at an identification number. *Arizona v. Hicks*, 480 U.S. 321, 323–26 (1987).

257. *Kyllo*, 533 U.S. at 33.

258. *Id.* at 40.

Generally, a sensible extension of the doctrine would be that documents stored in the cloud or items posted on social media sites that have no limitations as to who can view them are in plain view.<sup>259</sup> Questions will certainly arise as to what types of data mining technologies can be applied to sweep the Internet in search of suspicious activities, photos, or statements on publicly accessible portions of social media and cloud computing sites. *Kyllo* should be understood as establishing that new means of analyzing available data can change the constitutional balance.<sup>260</sup> As I have argued elsewhere, “Like the thermal imager in *Kyllo*, data mining takes data that is already accessible to law enforcement (the heat radiating from the house was in ‘plain view’) and transforms it into new knowledge that would not otherwise be available by constitutional means.”<sup>261</sup> In the present context, information that can be found by standard search technology in general public use (such as Google) should be considered open to the plain view of law enforcement officials.<sup>262</sup> More sophisticated data mining might be sufficiently intrusive to constitute a Fourth

---

259. See *supra* note 252 and accompanying text.

260. See, e.g., Strandburg, *supra* note 150, at 748 (“The main contention of this Article is that First Amendment freedom of association guarantees must provide an additional check, distinct from the Fourth Amendment’s protections from unreasonable search and seizure, on overreaching relational surveillance potential.”).

261. *Id.* at 799–800.

262. Criminal prosecutions have resulted from law enforcement access to publicly available social media sites. See, e.g., Edward M. Marsico, Jr., *Social Networking Websites: Are MySpace and Facebook the Fingerprints of the Twenty-First Century?*, 19 WIDENER L.J. 967 (2010); Daniel Findlay, Recent Development, *Tag! Now You’re Really “It” What Photographs on Social Networking Sites Mean for the Fourth Amendment*, 10 N.C. J.L. & TECH. 171 (2008). There has been criticism and consternation about the intrusiveness of the use of Google and social media sites in situations such as employment or by schools in monitoring their students. See, e.g., DANIEL J. SOLOVE, *THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET* (2007); Ian Byrnside, *Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants*, 10 VAND. J. ENT. & TECH. L. 445, 453–54 (2008); Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES MAG. (July 21, 2010), [http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=1&\\_r=1](http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=1&_r=1); Dave Marcus & Patricia Kitchen, *Employers Scour Web for Details on Applicants*, NEWSDAY.COM (July 23, 2010, 2:17 PM), <http://www.newsday.com/classifieds/jobs/employers-scour-web-for-details-on-applicants-1.2133284>. Some countries have regulated the extent to which employers can use Google and social media sites in evaluation applicants. See, e.g., Frank Pasquale, *Internet Nondiscrimination Principles: Commercial Ethics for Carriers and Search Engines*, 2008 U. CHI. LEGAL F. 263, 285 (discussing Finland’s regulations); Verena Schmitt-Roschmann, *Germany May Prevent Employer Facebook Checks*, NEWSDAY.COM (Aug. 25, 2010, 8:06 PM), <http://www.newsday.com/business/germany-may-prevent-employer-facebook-checks-1.2235726> (discussing a draft German law). It may be that social norms even in this country will evolve to discourage such methods of assessing candidates. More likely, and preferably, people will become more aware of what parts of their social media sites are available for public viewing and more careful both about posting and privacy settings. In any event, I can see no plausible argument for requiring law enforcement to forego simple access to publicly accessible media or use of commonly available search technology, unless an individual advocates a radically reconceptualized Fourth Amendment.

Amendment search, just as some courts have held with respect to sufficiently extensive aggregation of locational data.<sup>263</sup> Supreme Court opinions have repeatedly recognized the danger that technological advances might turn plain view observation into constitutionally troubling dragnet searches.<sup>264</sup> Under *Kyllo*, it is an open question whether some data mining techniques, applied to publicly accessible parts of social media or cloud computing sites, might similarly cross the line of Fourth Amendment reasonableness.<sup>265</sup>

Moreover, there will also be complex questions related to the scope of searches in the cloud even when they are appropriately authorized. These issues should be similar to those encountered when searching personal computers. Indeed, Professor Kerr has argued that elimination or radical curtailment of the plain view doctrine in such circumstances might be necessary to avoid the issuance of what amount to general warrants.<sup>266</sup> As the Ninth Circuit opined in one of the few cases to deal with these issues:

We recognize the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.<sup>267</sup>

---

263. See *supra* text accompanying notes 152–184.

264. For discussion of this issue, see, for example, Christopher Slobogin, *Government Dragnets*, LAW & CONTEMP. PROBS., Summer 2010, at 107. For an argument for a reconceptualizing of the Fourth Amendment focused on a right of security and a prohibition of general warrants, see also, for example, Rubinfeld, *supra* note 30.

265. See *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (examining the plain view doctrine).

266. See Kerr, *A General Approach*, *supra* note 25, at 1047–48 (suggesting that “[b]ecause searches of computer data are so comprehensive, courts should not admit evidence of crimes found in a search pursuant to an Internet warrant unless the evidence under consideration falls within the scope of the warrant”); Kerr, *Searches and Seizures*, *supra* note 185, at 576–84 (“Narrowing or even eliminating the plain view exception may eventually be needed to ensure that warrants to search computers do not become the functional equivalent of general warrants.”).

267. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1175–77 (9th Cir. 2010) (per curiam) (cabining the plain view doctrine in the context of computer searches and noting the complexities of searching files stored remotely).

## 2. *Undercover Surveillance and Informants on Social Media*

The strong Fourth Amendment protection for the home has never been extended to the use of undercover law enforcement officials or confidential informants.<sup>268</sup> Thus, the walls of the home may be breached by an undercover agent or informant who deceives the resident as to her trustworthiness and good intentions.<sup>269</sup> Moreover, under the Federal Constitution and many state constitutions, an informant or undercover police officer can use electronic technology to broadcast or record any conversations to which she is privy once inside.<sup>270</sup> Curbs on undercover investigation come almost entirely from the executive branch.<sup>271</sup> United States law differs from the law of other Western democracies in its permissive approach to undercover policing<sup>272</sup> despite the fact that excessive and inappropriate use of informants and undercover operatives was a major concern of the Church Committee investigation into FBI

---

268. See *supra* note 200 and accompanying text.

269. See *Hoffa v. United States*, 385 U.S. 293, 302–03 (1966) (finding no Fourth Amendment violation when a defendant misplaces his trust in another individual, whom the defendant invited into his office); *Lewis v. United States*, 385 U.S. 206, 211 (1966) (“A government agent, in the same manner as a private person, may accept an invitation to do business and may enter upon the premises for the very purposes contemplated by the occupant.”); *Lopez v. United States*, 373 U.S. 427, 439 (1963) (explaining that a government agent is entitled to disclose a conversation in an individual’s home in which he was a participant).

270. See, e.g., *United States v. White*, 401 U.S. 745, 751 (1971) (finding no constitutional violation when police agents use recording technology as a way to obtain evidence). For a discussion on how the Court in *White* could have found a Fourth Amendment requirement of a warrant for electronic surveillance, see Catherine Hancock, *Warrants for Wearing a Wire: Fourth Amendment Privacy and Justice Harlan’s Dissent* in *United States v. White*, 79 MISS. L.J. 35, 40–48 (2009).

271. Katherine Goldwasser, *After Abscam: An Examination of Congressional Proposals to Limit Targeting Discretion in Federal Undercover Investigations*, 36 EMORY L.J. 75, 81–90 (1987).

272. See Tracey Maclin, *Informants and the Fourth Amendment: A Reconsideration*, 74 WASH. U. L.Q. 573, 575 (1996) (“[T]he Supreme Court has interpreted the Constitution to impose few, if any, restraints on the government’s authority to plant or send covert informants and spies into our lives.”); see also Amsterdam, *supra* note 225, at 406–09 (expressing reservations as to whether an administrable Fourth Amendment line can be drawn when police spies and informants are utilized); Epstein, *supra* note 10, at 1215–24 (examining Fourth Amendment implications in the use of undercover pen registers and recorded oral evidence); Elizabeth E. Joh, *Breaking the Law to Enforce It: Undercover Police Participation in Crime*, 62 STAN. L. REV. 155, 159–60 (2009) (characterizing undercover operations as “authorized criminality” and calling for strengthened regulation and guidelines); Ross, *Impediments*, *supra* note **Error! Bookmark not defined.** (comparing the principles and norms surrounding the legitimacy of undercover operations between the United States and Italy); Ross, *Covert Surveillance*, *supra* note **Error! Bookmark not defined.** (comparing the same in the United States and Germany); Rubinfeld, *supra* note 30, at 133–35 (suggesting that Fourth Amendment standards to restrict undercover operations may differ depending on the context and severity of the intrusion into an individual’s personal life).

activity that instigated wide-ranging legislative regulation of electronic monitoring.<sup>273</sup>

The theory behind the acceptance of deceptive undercover work seems to be a combination of law enforcement's need and reliance on the autonomy of individuals to choose, whether wisely or not, the company they keep. The underlying intuition, as is suggested by the assumption of risk language in several cases,<sup>274</sup> may be that this type of government deception is more likely to ensnare those engaged in illegal activity than the rest of us. Lawbreakers will be forced to consort with untrustworthy individuals, thus putting themselves at risk of betrayal even before law enforcement becomes involved.<sup>275</sup> This argument is not entirely satisfactory, however, since it assumes what the warrant requirement is intended to determine—that surveillance is directed at those likely to be engaged in criminal behavior. When the informant or officer is posing as someone engaged in or seeking to engage in illegal activity—a drug buyer or seller, pedophile, or prostitute—or even as an attractive potential victim, this assumption makes sense. The interaction with the undercover officer or informant takes place within the context of a criminal act. In fact, one way to view the lenient approach that Fourth Amendment jurisprudence has taken to undercover police and confidential informants is as something of a mitigation of the categorical Fourth Amendment protection provided to residences, offices, and their equivalents. As the Supreme Court noted in *Lewis v. United States*,<sup>276</sup> if an individual turns her home into the site of an

---

273. The investigation culminated in a Final Report of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, which compiled information on American intelligence activities, as well as congressional interest in pursuing certain intelligence actions. S. REP. NO. 94-755 (1976). For a discussion of the political decision not to regulate undercover policing, see Ross, *Covert Surveillance*, *supra* note **Error! Bookmark not defined.**, at 533–538, and Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups*, 46 ARIZ. L. REV. 621, 628–35 (2004) (discussing instances of executive orders and congressional acts expanding and restricting surveillance).

274. See, e.g., *White*, 401 U.S. at 752 (“Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his.”).

275. See Thomas J. Miceli, *Criminal Solicitation, Entrapment, and the Enforcement of Law 1* (Univ. of Conn., Dep’t of Econ., Working Paper No. 2006-24, Sept. 2006), available at [http://digitalcommons.uconn.edu/econ\\_wpapers/200624](http://digitalcommons.uconn.edu/econ_wpapers/200624) (“The presumption underlying the use of this strategy is that the target of the solicitation has a predisposition to commit the crime in question and therefore will likely commit an actual crime if not first apprehended by the police sting.”).

276. 385 U.S. 206 (1966).

illegal business, she should not be heard to complain if law enforcement uses the ruse of being a customer of that business in order to enter.<sup>277</sup>

Use of undercover agents and informants in more ambiguous contexts is more disturbing. The Fourth Amendment, as currently interpreted, appears to pose no barrier to undercover surveillance of political and religious organizations or of those simply deemed by law enforcement, by virtue of their ethnicity or where they live, likely to engage in crimes.<sup>278</sup> Current barriers to such surveillance, to the extent they exist, are a result of law enforcement guidelines and policies,<sup>279</sup> which are unavoidably motivated in significant part by the substantial resources that would be required to place officers into these contexts.<sup>280</sup> For purposes of this Article, I will nonetheless accept the doctrine as it has been applied by the Court in the context of the physical home and office. This Subsection will ask how existing doctrines should extend to social media when they are technosocial extensions of the home or office.

Technosocial extension from the context of the physical home and office suggests that there would be no blanket constitutional barrier to investigations in which police officers use deception in online social contexts.<sup>281</sup> Undercover investigations online are familiar to most of us from news reports involving the policing of child pornography and pedophilia. A common scenario involves an undercover officer posing as an underage boy or girl and visiting a chat room or other online locale where child predators are suspected or known to lurk.<sup>282</sup> This scenario demonstrates one way in which online undercover work differs from similar law enforcement approaches in the real world. As the old comic says, “On the Internet, Nobody knows [if] You’re a Dog”<sup>283</sup>—or a forty-year-old police officer. If the justification for permitting unregulated use of

---

277. See *id.* at 211 (“[W]hen, as here, the home is converted into a commercial center to which outsiders are invited for purposes of transacting unlawful business, that business is entitled to no greater sanctity than if it were carried on in a store, a garage, a car, or on the street.”).

278. Fisher, *supra* note 273, at 643–44.

279. See, e.g., MICHAEL B. MUKASEY, THE ATTORNEY GENERAL’S GUIDELINES FOR DOMESTIC FBI OPERATIONS 31–33 (2008), available at [www.justice.gov/ag/readingroom/guidelines.pdf](http://www.justice.gov/ag/readingroom/guidelines.pdf).

280. See John Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991, 1001 (1984) (“The limited resources of law enforcement usually make it impracticable to conduct dragnet investigations.”).

281. See Grimmelmann, *supra* note 27, at 1197 (describing online interactions using current reasonable expectation analysis and third-party doctrine).

282. E.g., *To Catch a Predator* (NBC television series).

283. Peter Steiner, *On the Internet, Nobody Knows You’re a Dog*, NEW YORKER, July 5, 1993, at 61 (cartoon).

informants and undercover agents is essentially consent,<sup>284</sup> and an understanding that individuals are generally responsible for exercising judgment in the choice of their companions, then taking away some of the clues one might use in exercising that judgment might seem to weaken that justification. This perhaps undermines the force of the consent analysis even in these chat room contexts. Although somewhat appealing, such an argument should be rejected. Caution in dealing with strangers is normal and reasonable social behavior, which most of us are taught from childhood.<sup>285</sup> Similarly, anyone who lives part of her life online knows that spoofing of identities is common in some contexts—indeed, the ability to try on new identities and speak anonymously is an often-celebrated aspect of some types of online activity.<sup>286</sup> Unless we are willing to turn the Internet into a very different place in which real world identities are tightly tied to online identities, those who form relationships with strangers online in chat rooms must be aware of the possibility that things are not what they seem.

An online chat room is analogous to a bar or other social club, but is not the online extension of a home or office and thus is not the focus of this Subsection.<sup>287</sup> The more difficult issues concerning undercover surveillance of social media arise in much more controlled environments such as Facebook, which purport to require the use of true identities and are

---

284. See *Hoffa v. United States*, 385 U.S. 293, 302 (1966) (“Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer’s misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.”).

285. See ROB MCKENNA, U.S. DEP’T OF JUSTICE, CASE MANAGEMENT FOR MISSING CHILDREN HOMICIDE INVESTIGATION 83–84 (May 2006), [http://www.missingkids.com/en\\_US/documents/homicide\\_missing.pdf](http://www.missingkids.com/en_US/documents/homicide_missing.pdf) (“‘Stranger Danger’ has become a common warning issued by American parents to children.”).

286. See, e.g., Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1642 (1995) (pointing to psychological and sociological research supporting beneficial effects of assuming a different “personae”); Cohen, *Examined Lives*, *supra* note 143, at 1425 (recognizing that “anonymity shelters constitutionally-protected decisions about speech, belief, and political and intellectual association” and emphasizing the importance of “experiment[ing] with preferences [as] a vital part of the process of learning, and learning to choose”); Lee Tien, *Who’s Afraid of Anonymous Speech? McIntyre and the Internet*, 75 OR. L. REV. 117, 173 (1996) (noting the interest in limiting interactions with others and selectively revealing oneself); cf. Solove, *Digital Dossiers*, *supra* note 10, at 1102–04 (recognizing the importance of not only traditional affirmative anonymity in speech and association but also of freedom to read information anonymously).

287. Some lower courts are in accordance with this view. See, e.g., *United States v. Charbonneau*, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997) (finding that the Fourth Amendment protection covered evidence gathered from defendant’s home but did not extend to conversations in an AOL chatroom because the “[d]efendant could not have a reasonable expectation of privacy in the chat rooms”).

not intended to be fora for anonymous interactions.<sup>288</sup> In such an environment, undercover work will require a law enforcement agent to seek to become a “friend” of the individual whose site is to be infiltrated or to turn one of the individual’s own friends into a government informant. The infiltration could take a number of distinct forms. For example, a law enforcement officer could seek to “friend” the target of the surveillance using: (1) her own true identity; (2) a fictitious identity; or (3) the identity of someone the target knows personally. Alternatively, the law enforcement officer could encourage an informant known to the target to become an online “friend,” arrange to “look over the shoulder” of one of the target’s current online friends, or take over the account of a current friend. Should any of these scenarios raise Fourth Amendment concerns?

At first blush, the first two scenarios seem easily to fall within the rubric of the permissive approach taken in the physical world. It seems reasonable to conclude that, by inviting an unknown individual (either the law enforcement officer or her fictitious doppelganger) into one’s social network, one assumes the risk that this unknown individual could be virtually anyone—from law enforcement officer to identity thief.<sup>289</sup> Such a lax approach may also indicate that, though the site is of the type generally

---

288. For example, the privacy policies of Facebook and MySpace require users to submit personally identifiable information, such as name, e-mail address, and birthdate. *Facebook’s Privacy Policy*, FACEBOOK (rev. Dec. 22, 2010), <http://www.facebook.com/policy.php>; *Privacy Policy*, MYSPACE (Feb. 28, 2008), <http://www.myspace.com/index.cfm?fuseaction=misc.privacy>.

289. It may well be that this is a good way to gain entrance to the social networks of many people. Famously, in an experiment, a large number of people were willing to accept the social network friendship of a plastic frog. Grimmelmann, *supra* note 27, at 1185–86. In fact, open government initiatives have now put government entities directly on social network sites where individuals may “friend” them in order to enhance their democratic participation. Unless people are careful, however, they may end up exposing their private information to government at the same time. Citron, *Fulfilling Government 2.0’s Promise*, *supra* note 246, at 829–34. Interestingly, a document produced by the Department of Homeland Security in response to a Freedom of Information Act request by the Electronic Frontier Foundation suggested using exactly this approach as a means to obtain “an excellent vantage point for [Fraud Detection and National Security] to observe the daily life of beneficiaries and petitioners who are suspected of fraudulent activities.” U.S. DEP’T OF HOMELAND SEC., SOCIAL NETWORKING SITES AND THEIR IMPORTANCE TO FDNS 1 (2010), *available at* [http://www.eff.org/files/filenode/social\\_network/DHS\\_CustomsImmigration\\_SocialNetworking.pdf](http://www.eff.org/files/filenode/social_network/DHS_CustomsImmigration_SocialNetworking.pdf). According to the document, “In essence, using MySpace and other like sites is akin to doing an unannounced cyber ‘site-visit’ on a [sic] petitioners and beneficiaries.” *Id.* One wonders whether this kind of wide-eyed innocent approach to social networks is likely to last, however, especially in light of reported incidents of use of social network information in identity theft and phishing scams. Indeed, there is evidence of increasing and more sophisticated use of privacy settings on social media. *See, e.g.*, Jacqui Cheng, *Students Finally Wake Up to Facebook Privacy Issues*, ARS TECHNICA, <http://arstechnica.com/web/news/2010/07/students-finally-wake-up-to-facebook-privacy-issues.ars> (last visited Mar. 6, 2011) (concluding that the number of students who use Facebook’s privacy settings has increased); Ki Mae Heussner, *Google Buzz Draws Class-Action Suit from Harvard Student*, ABCNEWS (Feb. 18, 2010), <http://abcnews.go.com/Technology/google-buzz-draws-class-action-suit-harvard-student/story?id=9875095>.

deemed to be a technosocial extension of the home or office, a particular individual is not actually “living” there in any of the senses deemed important to private life. Even at this level, however, it is worth noting that features of the online social network environment, at least as reflected in a platform such as Facebook, make any “friendship” with an undercover officer more intrusive than a casual friendship in the physical world. At least with the current default structure of Facebook, any online “friend”—even one who simply lurks in the background and does not participate—has twenty-four hour access to everything on the site, including photos, conversations with other friends, and in some cases parts of the social network sites of other friends.<sup>290</sup> Because an online friend does not take up physical space, it may be very easy for the “resident” of a social network site to forget that the online friend is there.

Furthermore, infiltration of social networks using fictitious friends is extremely cheap, easy, and safe for government agents to do, distinguishing it from undercover work in the physical world.<sup>291</sup> Government agents could easily send out mass friend requests to classes of people based on information found in their public profiles, such as ethnicity (perhaps based on names) or political or religious affiliation, without any specific reason to suspect those individuals of criminal behavior.<sup>292</sup> Those who carelessly

---

290. This description exaggerates the availability of information to Facebook friends to some extent. Facebook allows quite a bit of customizing of what information is available to which people using “Friend Lists.” *Help Center*, FACEBOOK, [http://www.facebook.com/help/?faq=12074&ref\\_query=friend+list](http://www.facebook.com/help/?faq=12074&ref_query=friend+list) (last visited Mar. 6, 2011). The available structure of privacy settings on Facebook changes relatively frequently in both privacy-enhancing and privacy-destroying ways. The increasing use of more nuanced social structures than the blanket tiers of “friends,” “friends of friends,” and “everyone” seems nearly inevitable, whether on Facebook itself or on some new social networking platform. Norms and practices are far from settled, and it is clear that people are sensitive to nuances in how they are connected to others online despite studies and anecdotes demonstrating profligate posting of personal information for wide consumption. Two recent “scandals” illustrate the point. In one case, Facebook began to use its users’ online purchases as the basis for advertisements to their friends in which they were identified as having purchased particular items. *See* William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105, 1119–20. After an outraged response, the program was discontinued. *Id.* at 1120. In another case, Google, in attempting to launch its own social network platform “Google Buzz,” automatically peopled the social networks of those who signed up for the service with everyone with whom they exchanged electronic mail using Google’s G-mail program. Thomas Claburn, *Google Buzz Stung by Lawsuit*, INFORMATIONWEEK (Mar. 8, 2010, 2:25 PM), <http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=223200135>. Again, people were outraged at this exposure of their two-way communication connections, and Google beat a hasty retreat. *Id.*

291. Kerr, *A General Approach*, *supra* note 25, at 1032.

292. The idea that the government might conduct such mass infiltration of social networking sites is not as far-fetched as it might sound in light of past domestic surveillance. *See, e.g.*, S. REP. NO. 94-755 (1976) (documenting specific instances of past U.S. domestic surveillance); Fisher, *supra* note 273, at 622–23, 628–35 (same); *see also* Amsterdam, *supra* note 225, at 407 (rather presciently voicing concern about the day when “science produces robots in the likenesses of men,

accept the requests need not be actively monitored. Rather, the fictitious friends can idle, ready to be activated if the government takes an interest in someone. If enough people are sloppy about whose online friendship they accept, the fictitious individual may also pick up credibility through the friend suggestion tools that many social network sites use to identify individuals with common acquaintances.<sup>293</sup>

The extent of undercover surveillance possible in the online world is drastically greater than the possibilities for similar surveillance in the physical world. Online undercover activity is simply much cheaper and safer and the deception much easier.<sup>294</sup> These aspects are socially positive where surveillance is warranted (given that the online environment also facilitates certain types of criminal activity).<sup>295</sup> Nonetheless, the ease of such surveillance undercuts the implicit assumption of the case law that undercover surveillance will be limited to those who are conducting illegal transactions. This raises additional concerns about pervasive surveillance similar to those raised in recent cases about locational tracking and about the potential for over-reaching government infiltration of political, religious, and other expressive associations.<sup>296</sup>

Is all of this enough to avoid the rationale of cases like *United States v. White*, which held that there is no Fourth Amendment violation if an informant's report of a consensual interaction within someone's home is enhanced by electronic recording or transmission? On an individual level, probably not, though fictitious identities would violate the terms of service of many social media sites.<sup>297</sup> Social network denizens are aware of the degree of access they are providing when they "accept" a friend request<sup>298</sup> and the rationale of cases such as *White* would seem to apply. The specter of widespread insertion of government agents wherever individuals are

---

and government sends them down on us in droves"); Calo, *supra* note 28 (discussing technological advancements in anthropomorphic designs and their impact on privacy).

293. For example, Facebook utilizes users' networks, mutual friends, and other personal information to suggest friends. *Help Center*, FACEBOOK, <http://www.facebook.com/help/?page=925> (last visited Mar. 6, 2011). Moreover, this tool may uncover people the user does not even know. *Id.*

294. Kerr, *A General Approach*, *supra* note 25, at 1032.

295. *Id.* at 1014, 1033, 1044–48.

296. See, e.g., S. REP. NO. 94–165 (1975) (detailing the results of the investigation by the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities); Fisher, *supra* note 273, 622–28 (noting renewed interest in surveillance and proposing such techniques targeting religious groups and other types of affiliations should not be permitted unless there is a reasonable suspicion of criminal activity).

297. See, e.g., *Statement of Rights and Responsibilities*, FACEBOOK (rev. Oct. 4, 2010), <http://www.facebook.com/terms.php> (stating that users may not provide any false personal information or create an account for someone else).

298. See Cheng, *supra* note 289 (explaining that "young people are very engaged with the privacy settings on Facebook").

careless about accepting friend requests is disconcerting, however, and might change the analysis, just as the extensiveness of locational tracking has been deemed to change the constitutional balance.<sup>299</sup> In any event, state courts that read their own constitutional provisions more broadly than the Federal Constitution and reject the analysis of *White*<sup>300</sup> may decide that their state constitutions require authorization for law enforcement infiltration of social networks as well.

The potential for a law enforcement agent to take on the identity of someone an individual knows raises additional concerns. This issue does not arise in the physical world. Outside of detective fiction, individuals generally do not have to worry that someone purporting to be a known friend or acquaintance is actually a law enforcement agent in disguise. In the physical world this is next to impossible to pull off. In the online world, however, it may not be so difficult (though this approach is obviously less subject to the concerns about dragnets raised above), particularly if the individual is chosen cleverly so that it is unlikely that interactions in the physical world will blow the agent's cover. (An old classmate might be the perfect choice, for example.)

At this point, our Fourth Amendment hackles should be raised. Although it may be reasonable to have to worry that strangers one invites into one's confidence may be government agents or even that friends or associates may decide to turn informant, as a society we should find it unreasonable that someone purporting to *be* a citizen's old friend Flo from high school is actually a government agent. Such a ruse would certainly be highly unacceptable (and potentially fraudulent) if perpetrated by a private individual.<sup>301</sup>

---

299. *E.g.*, *United States v. Maynard*, 615 F.3d 544, 555–56 (D.C. Cir. 2010) (holding that locational tracking violated defendant's reasonable expectation of privacy), *cert. denied*, 131 S. Ct. 671 (2010).

300. *See, e.g.*, *Commonwealth v. Blood*, 507 N.E.2d 1029, 1034, 1037 (Mass. 1987) (requiring a warrant for electronic surveillance of spoken conversations); *State v. Goetz*, 191 P.3d 489, 500 (Mont. 2008) (electronic monitoring of defendant's conversations was a search that violated privacy provisions in the state constitution); *Commonwealth v. Brion*, 652 A.2d 287, 289 (Pa. 1994) (same); *State v. Geraw*, 795 A.2d 1219, 1220, 1225 (Vt. 2002) (adopting Justice Harlan's dissent in *White* that the burden rests with the government to justify the need to eavesdrop by obtaining a warrant); *State v. Mullens*, 650 S.E.2d 169, 190 (W. Va. 2007) (requiring a warrant for electronic surveillance of conversations).

301. *See, e.g.*, Sarah Perez, *Fake Social Network Profiles: A New Form of Identity Theft in 2009*, READWRITEWEB (Feb. 3, 2009, 5:36 AM), [http://www.readwriteweb.com/archives/fake\\_social\\_network\\_profiles\\_a.php](http://www.readwriteweb.com/archives/fake_social_network_profiles_a.php) (noting the relative ease in creating fake online personas in social networking sites). As Professor Kerr notes, the Supreme Court sometimes acts as if the dictates of "positive law" matter for the Fourth Amendment analysis and sometimes do not. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 517–19 (2007). A more complete analysis of the potential implications of legal restrictions on acceptable behavior on the Internet for Fourth Amendment analysis would be worthwhile, but I do not undertake it here.

Of course, the well-known circularity problem of the Fourth Amendment is evident in this discussion. If we know that government agents might pose as old friends, we can take measures to vet our online friends to verify their identities. But that is the point of the technosocial perspective. Social behavior is contingent on available technology and on expectations of surveillance. In the end, the determination must be a normative one, as it was in *Katz*. Given the important role that these online extensions of our homes are beginning to play in maintaining and enhancing our private lives, is this level of intrusiveness something that a free people should accept from its government?

The informant examples also raise close questions. What kind of access to an individual's social network site may an informant provide to the government without triggering Fourth Amendment scrutiny? There are two distinct ways to analyze this issue in analogy to physical world case law and they lead to contradictory results. On the one hand, one might view the informant social network friend as analogous to the informant wearing a wire and hence outside of Fourth Amendment protection under *White*. From that perspective, an informant who permits a government agent to look over her shoulder as she navigates a friend's social network site is doing nothing more than providing the government with a more accurate record of what she could report from her own visits to her friend's social network home, and thus no Fourth Amendment interests are implicated. On the other hand, however, an informant who permits a government agent to look over her shoulder as she roams about a friend's social network "home" is essentially providing third party consent to allow the agent to enter. In most circumstances where an individual has set protective privacy settings, it will be entirely evident to the agent that the informant does not have authorization to consent to the agent's entrance into the site. This is even more the case if the agent does not merely peer over the informant's shoulder but directs the informant's activities on the site, essentially "becoming" the informant. Moreover, if the site's resident has set privacy preferences to allow certain information to be visible to friends only, that would seem to be the social equivalent of standing at the threshold and denying entry, as in *Georgia v. Randolph*.<sup>302</sup>

Present Fourth Amendment case law deals with the distinction between an informant wearing a wire and a government agent performing a search of a home by delineating the conversations and activities in which the informant actually participates as the authorized scope of observation. For example, courts have held that law enforcement officers may set up video surveillance cameras in a hotel room where an informant will interact with a suspect, but the cameras must be turned off when the informant is

---

302. 547 U.S. 103, 113–15 (2006).

not in the room.<sup>303</sup> Similarly, the controversial doctrine of “consent-once-removed” permits law enforcement officers to enter a home based on consent given to an informant or undercover officer, but, even in jurisdictions that accept the doctrine, it is limited to periods immediately after the informant establishes probable cause and the scope of the consent is limited essentially to providing back-up to an arrest.<sup>304</sup> Moreover, the doctrine has been called into question by the Supreme Court’s holding in *Georgia v. Randolph*, limiting the scope of third party consent in the presence of an objecting occupant of a home.<sup>305</sup>

Lines delineating the circumstances in which an informant can provide law enforcement access to a home are much more difficult to draw in the context of a “home-like” social media site, since the site keeps a record of all activity, and at least in many cases, essentially the entire record is accessible to a friend whenever that friend signs on.<sup>306</sup> The bottom line is that the assumption of risk analysis that justified placing the informant wearing a wire outside of the Fourth Amendment’s purview is more problematic in the context of a social networking site, where access to the

---

303. See, e.g., *United States v. Lee*, 359 F.3d 194, 203 (3d Cir. 2004) (determining that no constitutional violation occurred because defendant was present during the entire surveillance); *United States v. Nerber*, 222 F.3d 597, 600 (9th Cir. 2000) (holding that defendants had a reasonable expectation that once the informants left the room, electronic surveillance of their conversation was no longer permitted).

304. See, e.g., *United States v. Bramble*, 103 F.3d 1475, 1478 (9th Cir. 1996) (concluding that warrantless entry did not violate the Fourth Amendment when undercover agent was invited into the home, established probable cause, and summoned help from other officers); *United States v. Jachimko*, 19 F.3d 296, 299 (7th Cir. 1994) (holding that consent was not vitiated merely because confidante turned out to be an informant and not a police officer); *United States v. Diaz*, 814 F.2d 454, 459 (7th Cir. 1987) (finding that consent was not vitiated merely because the agent had momentarily left the room to obtain backup); *United States v. Janik*, 723 F.2d 537, 547–48 (7th Cir. 1983) (concluding that the fact that arresting officer received help from backup officers does not matter for consent purposes, particularly since evidence seized was in plain view); *United States v. Schuster*, 684 F.2d 744, 749 (11th Cir. 1982) (determining that consent may carry over to backup officer but is limited to original consent given); see also *United States v. Romero*, 452 F.3d 610, 613 (6th Cir. 2006) (holding that the “consent once removed” doctrine justified backup officers’ entry into a hotel room); *United States v. Yoon*, 398 F.3d 802, 807 (6th Cir. 2005) (finding that the “consent once removed” doctrine applies when agent is invited to residence of defendant and establishes probable cause); *United States v. Pollard*, 215 F.3d 643, 649 (6th Cir. 2000) (adopting the “consent once removed” doctrine because probable cause was established and backup officers acted within constitutional limits); *United States v. Akinsanya*, 53 F.3d 852, 856 (7th Cir. 1995) (identifying the three factors of “consent once removed” to include: (1) entry by express invitation, (2) existence of probable cause, and (3) immediate summoning for backup from other officers).

305. See *Callahan v. Millard County*, 494 F.3d 891, 896–98 (10th Cir. 2007) (declining to extend consent once removed doctrine to include informants), *rev’d on other grounds sub nom. Pearson v. Callahan*, 555 U.S. 223 (2009).

306. See, e.g., *Facebook’s Privacy Policy*, *supra* note 288 (detailing exactly what information is collected from the site and how Facebook uses that information).

site is equivalent to law enforcement entry against the express wishes of the site's "occupant." When social network sites function as extensions of the home, it may be normatively reasonable for occupants to expect privacy at those sites against intrusions by government officials essentially hiding in their friends' pockets. The close balance of *White* may be tipped in the other direction by the inability to limit the scope of the government agent's intrusion the way it can be limited when an informant is electronically monitored in a physical home. Certainly those states that have not adopted *White*'s reasoning in their state constitutional analyses should be troubled by the use of informants on protected social networking sites.

Moreover, the need to obtain court authorization before monitoring an individual's social networking account through access provided by an informant should not be overly burdensome for law enforcement. The informant is undoubtedly free to report any illegal activity (or reports of illegal activity) she observes on the site to a law enforcement officer, who may use the information as the basis of a request for a warrant. The need for an informant to wear a wire in the physical world is based at least in part on the ephemeral nature of the activities under observation in the usual informant context.<sup>307</sup> Although postings can in principle be removed from social networking sites, they generally remain on an individual's page, meaning that the urgency to get things "on tape," which is present in most physical informant situations, is absent. These features of informant-provided access to a social networking site, along with the important role such sites may play in social relationships, suggest that we should read the Fourth Amendment to require a warrant for monitoring of an individual's site through access provided by an informant.<sup>308</sup>

## VI. CONCLUSION

The rapidly changing social role of the Internet and other digital media requires a rethinking of the scope of Fourth Amendment protection. To adapt to changing technology, courts must focus not only on the potential

---

307. See Evan Haglund, Note, *Impeaching the Underworld Informant*, 63 S. CAL. L. REV. 1405, 1411 (1990) (identifying "narcotics, gambling, prostitution, and tax-evasion" as typical crimes involving informants); *Informants, What's Wrong with the Drug War?*, DRUG POL'Y ALLIANCE, <http://www.drugpolicy.org/drugwar/informants/> (last visited Mar. 6, 2011) (explaining that police use informants in "the vast majority of drug arrests in the United States . . . [which are] for simple possession—often marking the first time a person encounters the criminal justice system").

308. It is also possible that some lesser standard than a probable cause warrant might be workable. I do not intend here to take a side in the debate about whether a sliding scale approach to the Fourth Amendment would be more appropriate in general. See Rubinfeld, *supra* note 30, at 134–35 (arguing that a security-based conception of the Fourth Amendment might require reasonable suspicion for some government undercover activities within a home and probable cause for the most extensive intrusions).

for increasing intrusion into time-honored private realms, as in *Kyllo*, but also on the privacy implications of technology-mediated social change. This is the message of *Katz* and the question with which the Court grappled, but declined to confront, in *Quon*. The social role of the Internet and related technologies goes far beyond serving as an additional, and parallel, means of communication, analogous to the telephone and postal mail.

While courts are still grappling with text messaging and e-mail, society has moved on, integrating the web more and more seamlessly into the social realm and providing virtual extensions of the home, the office, and other core loci of private life. The Fourth Amendment must respond to these changes if its values are to be preserved for coming generations. First, as courts are already recognizing, we must abandon any aggressive form of third party doctrine that suggests that any and all exposure of private data or communications to an intermediary or platform provider destroys a reasonable expectation of privacy (if, indeed, it ever really existed) as inconsistent with precedent dealing with social life in the physical world. Second, courts should adopt an approach of technosocial continuity, acknowledging both the increasing intrusiveness technology makes possible and the intertwined and changing social structure of the physical and online worlds.

Viewed from a technosocial perspective, much cloud computing and storage is an extension of the home or office and should be afforded comparable Fourth Amendment protection. Similarly, certain types of social networking platforms provide extensions of the social function of the home, connecting people with their friends, families, and intimates and aggregating the varied pieces of an individual's private life. These sites should be protected from government intrusion much as homes are. In applying the Fourth Amendment's protections to these interwoven virtual and physical private spaces, some Fourth Amendment doctrines will translate relatively easily and lines may be drawn analogously to the way they have been drawn in physical world contexts. Other cases will raise more difficult line-drawing questions. Courts have already begun to recognize this in the arena of locational tracking, and some have determined that the potential for ubiquitous tracking changes the balance in favor of finding Fourth Amendment protection even though limited physical tracking is not deemed a search. This Article briefly explores undercover policing and the use of informants in the social network context as another example of how technosocial change may require rethinking the Fourth Amendment's application.

The goal of this Article is not to construct a distinct Fourth Amendment regime for the Internet, but to argue that we must zoom out from the focus on translating the Fourth Amendment's protections to cyberspace and see digitally mediated social behavior for what it is—an

2011]

HOME, HOME ON THE WEB

165

inextricable part of social interaction more generally. If we are to maintain a space for private life away from government scrutiny, the Fourth Amendment's protections must adapt to the broadened context in which citizens live their private lives.