2011

# The Timely Demise of the Fourth Amendment Third Party Doctrine

Stephen E Henderson

# The Timely Demise of the Fourth Amendment Third Party Doctrine

*Stephen E. Henderson*[*]



In 1897, some mistakenly believed Mark Twain to be near death.[1] In characteristic fashion, Twain provided assurance that "the report of my death was an exaggeration."[2] When some ten years later it was incorrectly believed that Twain might have been lost at sea, he offered this personal assurance:

> I will make an exhaustive investigation of this report that I have been lost at sea. If there is any foundation for the report, I will at once apprise the anxious public. I sincerely hope that there is no foundation for the report, and I also hope that judgment will be suspended until I ascertain the true state of affairs.[3]

Perhaps this too is a premature obituary, but the Fourth Amendment Third Party Doctrine—which holds that a person retains no expectation of privacy in information conveyed to another—has at least taken ill, and it can

* Associate Professor, Widener University School of Law. J.D., Yale Law School, 1999; B.S., University of California at Davis, 1995. I had the pleasure of commenting on an earlier version of Matthew Tokson's paper at the 2010 Privacy Law Scholars Conference and am indebted to Joseph Thai for thoughtful comments on a previous draft of this Essay.

1. *See* SHELLEY FISHER FISHKIN, LIGHTING OUT FOR THE TERRITORY: REFLECTIONS ON MARK TWAIN AND AMERICAN CULTURE 134 (1997).

2. *Id.* It seems Twain later embellished to improve his own humor, giving us the oft-quoted "the reports of my death are greatly exaggerated." *See* MARDY GROTHE, VIVA LA REPARTEE: CLEVER COMEBACKS & WITTY RETORTS FROM HISTORY'S GREAT WITS & WORDSMITHS 124 (2005); RALPH KEYES, THE QUOTE VERIFIER: WHO SAID WHAT, WHERE, AND WHEN 42 (2006).

3. *Twain and Yacht Disappear at Sea. Mark Twain Investigating*, N.Y. TIMES, May 4–5, 1907, *reprinted in* MARK TWAIN SPEAKS FOR HIMSELF 221 (Paul Fatout ed., Purdue University Press 1997) (1978).

be hoped it is an illness from which it will never recover. In *Automation and the Fourth Amendment*,[4] Matthew Tokson adds to the Doctrine's woes by convincingly demonstrating that at least its current application fails to adequately account for automation, meaning purely machine-based processing. As Tokson notes, "[w]hile *Smith* and the Third Party Doctrine were heavily criticized even before the Internet age, the drumbeat of criticism has intensified."[5] For the last several years, I have kept my own mallet pounding.

## I. POTENTIAL FOR CHANGE

While I have always believed the Doctrine is fundamentally misguided, at first I thought that we would most likely see incremental change through a "limited third party doctrine" that recognized the distinction between intended recipients and mere conduits.[6] But then I looked closely at how unpopular the Doctrine was as a matter of state constitutional law and began to think that discord might lead to federal change.[7] So I set about crafting a replacement.[8] That replacement both relied upon and criticized the related work of Professor Christopher Slobogin,[9] and he returned the favor by pointing out that my nine-factor test—yes, *nine* factors—was somewhat lacking in administrability.[10] So, for the last three years I have had the pleasure of working with Slobogin and others to refine that proposal as the Reporter for an American Bar Association Task Force drafting Criminal Justice Standards relating to government access to third party records, and thankfully my factors are currently down to four.[11]

Tokson is quite pessimistic about the chance of outright reversal,[12] but I have become much more optimistic. Lower courts are, of course, bound by existing Supreme Court precedent, but they are noticeably skittish. In 2007, a panel of the Sixth Circuit Court of Appeals held that a sender of electronic mail retains a reasonable expectation of privacy in those messages residing

---

4. Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581 (2011).

5. *Id.* at 585 (footnote omitted).

6. *See* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV 507, 524–28 (2005).

7. *See* 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, 373–76 (2006).

8. *See generally* 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 (2007) (exploring alternatives to the Third Party Doctrine and setting forth nine factors relevant to a decision whether to restrict law-enforcement access).

9. *See id.* at 1000, 1011, 1019–24.

10. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 181–82 (2007).

11. *See infra* pp. 50–51.

12. *See* Tokson, *supra* note 4, at 585–86.

with a service provider,[13] the first decision to so hold. Although service-provider computers scan e-mail content, the court was persuaded that such an automated search does not diminish a sender's reasonable expectation of privacy,[14] thus providing a foundation upon which Tokson would ably build. Although that opinion was vacated based on the case's odd procedural posture,[15] in December of 2010 a second panel agreed, holding that a warrant is necessary to access stored e-mail.[16] A panel of the Eleventh Circuit Court of Appeals briefly held to the contrary,[17] but it quickly reversed course and punted on the substantive question.[18] I like to think that about-face was influenced by a terrific amicus brief written by Professor Paul Ohm, to which I was a signatory,[19] but in its opinion the court understandably relied primarily upon an intervening decision by the U.S. Supreme Court in *City of Ontario v. Quon*.[20]

The question in *Quon* was whether the user of a government-issued pager retains a reasonable expectation of privacy in messages stored by the service provider.[21] But a unanimous Court set aside that question, instead holding the particular government conduct reasonable even assuming the user retained such an expectation.[22] Eight members of the Court called for caution and prudence in determining constitutional protections for electronic communications, a far cry from the knee-jerk reaction of a monolithic Third Party Doctrine:

> Th[is] Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment . . . . The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. . . . 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. . . . At present, it is

13. Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007), *vacated*, 532 F.3d 521 (6th Cir. 2008) (en banc).

14. *See Warshak*, 490 F.3d at 474.

15. Warshak had requested and received a preliminary injunction restricting future government access to e-mail, a constitutional claim the en banc court held was not ripe for review. *See Warshak*, 532 F.3d at 523.

16. United States v. Warshak, 2010 WL 5071766, at *14 (6th Cir. Dec. 14, 2010).

17. *See* Rehberg v. Paulk, 598 F.3d 1268, 1281–82 (11th Cir.), *vacated*, 611 F.3d 828 (11th Cir. 2010).

18. *See Rehberg*, 611 F.3d at 846–47 (granting qualified immunity).

19. Brief for Law Professors and Instructors as Amici Curiae Supporting Appellee, *Rehberg*, 598 F.3d 1268 (No. 09-11897-G), *available at* http://www.jdsupra.com/post/documentViewer.aspx?fid=b2381ce7-bdfo-498f-8416-cfo405f4ccaf.

20. 130 S. Ct. 2619 (2010).

21. *Id.* at 2626.

22. *Id.* at 2628–29, 2632–33.

> uncertain how workplace norms, and the law's treatment of them, will evolve. . . . 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.[23]

As noted by the Eleventh Circuit, despite briefing by the parties and ten amicus curiae, the Supreme Court was so cautious that it did not even articulate "the governing principles [necessary] to answer" the Fourth Amendment question, let alone answer it.[24]

Even before *Quon*, I realized that the Third Party Doctrine had less firm a foundation than it might seem. It seems so ingrained in part because of this oft-quoted language from *United States v. Miller*, in which the Court refused Fourth Amendment protection for bank records:

> [We] ha[ve] held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [the third party] 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.[25]

However, while the Court did so hold in a string of cases extending from the 1960s to the 1980s, it has yet to do so in the modern era in which social norms and technologies dictate that vastly more personal information resides with third parties.[26]

---

23. *Id.* at 2629–30. Only Justice Scalia took issue with this portion of the *Quon* opinion, and although he felt the majority was exaggerating the difficulty in unnecessary dicta, he acknowledged that "[a]pplying the Fourth Amendment to new technologies may sometimes be difficult." *Id.* at 2635 (Scalia, J., concurring in part and concurring in the judgment).

24. Rehberg v. Paulk, 611 F.3d 828, 845 (11th Cir. 2010).

25. 425 U.S. 435, 443 (1976).

26. It should also be noted that courts sometimes look to other law as creating a reasonable expectation of privacy ("REP") despite the Third Party Doctrine. One source is the constitutional protection of medical privacy. *See, e.g.*, Doe v. Broderick, 225 F.3d 440 (4th Cir. 2000) (requiring a warrant to access medical/prescription records); State v. Skinner, 10 So. 3d 1212 (La. 2009) (same); Commonwealth v. Riedel, 539 Pa. 172 (1994) (finding a REP in medical records and requiring probable cause but no warrant); *cf.* People v. Perlos, 462 N.W.2d 310 (Mich. 1990) (finding no REP). Another source is the First Amendment. *See, e.g.*, Amazon.com v. Lay, 2010 WL 4262266, at *10–12 (W.D. Wash. Oct. 25, 2010) (rejecting government subpoena of expressive records); *In re* Grand Jury Investigation of Possible Violation of 18 U.S.C. Section 1461, 706 F. Supp. 2d 11, 16–23 (D.D.C. 2009) (same); *In re* Grand Jury Subpoena to Amazon.com Dated August 7, 2006, 246 F.R.D. 570, 572–74 (W.D. Wis. 2007) (same). Another source is statutory or common law. *See, e.g.*, Warshak v. United States, 490 F.3d 455, 474–75 (6th Cir. 2007) (looking to federal statute in requiring warrant for e-mail), *vacated on other grounds by* 532 F.3d 521 (6th Cir. 2008); Doe v. Broderick, 225 F.3d 440, 450 (4th Cir. 2000) (looking to federal statute in requiring warrant for medical records); DeMassa v. Nunez, 770 F.2d 1505, 1506–07 (9th Cir. 1985) (looking to other constitutional

Instead, in the last decade the Court has four times rejected the argument of dissenting colleagues that cases should be decided according to the Doctrine, thereby restricting government tactile probing of carry-on luggage,[27] the drug testing of pregnant women,[28] the thermal scanning of homes,[29] and the entering of homes upon contested consent.[30] The District of Columbia Circuit seemed responsive to this changing tide when it recently distinguished two Supreme Court third-party cases concerning automobile tracking.[31] In *United States v. Maynard*, the District of Columbia Circuit Court held that continuous warrantless electronic tracking of a vehicle constitutes an unreasonable search.[32] The issue is not a straightforward application of the Third Party Doctrine, in that the location information is not actually held by another,[33] and the court was able to expand upon concessionary language in a previous Supreme Court opinion.[34] But the court's very thoughtful decision is nonetheless one more chink in a monolithic Third Party Doctrine.[35]

The Third Circuit also recently took a skeptical view. Professor Susan Freiwald and the Electronic Frontier Foundation convinced the court that a magistrate has the statutory option of requiring probable cause before the government can obtain historic cell site location information.[36] On the constitutional issue, the court rejected the government's assertion of the Third Party Doctrine on the basis that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."[37] Given that knowledge of location is necessary to provide the service, this is more a rejection of the Supreme Court's doctrine than

---

provisions, federal and state statutes, caselaw, and codes of professional responsibilities in requiring warrant for attorney files); People v. Gutierrez, 222 P.3d 925, 932–36 (Colo. 2009) (looking to federal and state statutes and case law in requiring warrant for tax-preparer records).

27. *See* Bond v. United States, 529 U.S. 334, 338–39 (2000).

28. *See* Ferguson v. City of Charleston, 532 U.S. 67, 86 (2001).

29. *See* Kyllo v. United States, 533 U.S. 27, 40–41 (2001).

30. *See* Georgia v. Randolph, 547 U.S. 103, 106 (2006).

31. *See* United States v. Karo, 468 U.S. 705 (1984); United States v. Knotts, 460 U.S. 276 (1983).

32. 615 F.3d 544, 555–58 (D.C. Cir. 2010).

33. *See id.* at 558–63.

34. *See id.* at 556–58; *Knotts*, 460 U.S. at 283–84 ("[T]he fact is that the reality hardly suggests abuse; 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." (citation omitted) (internal quotation marks omitted)).

35. The Ninth Circuit declined to follow suit but over vigorous dissents by Judges Kozinski and Reinhardt. *See* United States v. Pineda-Moreno, 617 F.3d 1120 (9th Cir. 2010) (dissenting from denial of rehearing en banc).

36. *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 319 (3d Cir. 2010).

37. *Id.* at 317.

the Third Circuit cared to admit. Two federal magistrates have taken the next logical step, recently holding that the Fourth Amendment requires a warrant before law enforcement can access historic cell site location information.[38]

This is not to say, however, that the Third Party Doctrine is without its champions, or at least without its champion. Professor Orin Kerr has defended the Doctrine for its ex ante clarity and for maintaining technological neutrality.[39] I do not think any of the many critics of the Doctrine fail to recognize that it is a wonderfully bright-line rule. But then it is always easy to craft an arbitrary bright line: Police can stop a person with black hair without suspicion, but require a warrant to stop anyone else. Of course there would still be some quibbles—what to do if the person is bald, or has on a hat that completely covers the hair—but for the most part the rule would be as wonderfully clear as it would be unjust. An even clearer rule would be akin to the Third Party Doctrine: Police can stop every person without suspicion. If two rules are equally wise, prudence dictates that we select the rule that is more clear. But when it is a rule's very arbitrary nature that allows avoidance of all hard questions, which is the case with the Third Party Doctrine, that clarity does little to commend it.

Nor would it be less clear to have the opposite default: Police cannot access any record information without probable cause. Such a rule would be devastating to the legitimate needs of law enforcement, but it would be plenty clear. So, the options are (1) having a clear rule that devastates privacy, (2) having a clear rule that devastates law enforcement, or (3) working out a rule that respects both. I should add that the difficult work is for the courts. Once courts decide, say, that medical records are protected by a warrant requirement like phone conversations[40] and the home,[41] while bank records are protected by a probable-cause requirement like an arrest,[42] and transactional information regarding communications requires reasonable suspicion like *Terry* stops[43] and *Gant* searches incident to arrest,[44] police will find it straightforward to comply.[45]

---

38. *In re* Application of the U.S. for an Order Authorizing Release of Historical Cell-Site Info., 2010 WL 3463132 (E.D.N.Y. Aug. 20, 2010); *In re* Application of the U.S. for Historical Cell Site Data, 2010 WL 4286365 (S.D. Tex. Oct. 29, 2010).

39. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 561 (2009). On the opposite side, a very interesting novel attack upon the Doctrine is contained within Professor Jed Rubenfeld's thesis that the mistake has been to consider the Fourth Amendment to be about protecting privacy, when it is instead textually about protecting "security." Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 104 (2008).

40. *See* Berger v. New York, 388 U.S. 41 (1967).

41. *See* Payton v. New York, 445 U.S. 573 (1980).

42. *See* United States v. Watson, 423 U.S. 411 (1976).

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

44. *See* Arizona v. Gant, 129 S. Ct. 1710 (2009). Admittedly, *Gant*'s holding is far from a model of clarity, but that self-inflicted confusion was completely unnecessary. The Court could

As for technological neutrality, it is true that any protective doctrine permits "savvy wrongdoers" to hide portions of their crime from public observation.[46] My criminal-procedure students rather quickly recognize that perhaps the best protection against traditional government investigation is money. Money can buy a detached single-family home, which comes with protected curtilage,[47] a backyard awning that protects against surveillance from the air,[48] a screen door that protects against police entry,[49] and a crosscut shredder to protect against snooping from the trash.[50] But it is in fact technology and associated changes in social norms that have *caused* far more information to reside with third persons than has ever been the case.

For example, whole categories of data are stored that never were before. If I wanted to purchase a book in a time not so distant, I would enter a bookstore, browse in a practically anonymous fashion, and make my purchase with cash. The bookstore made no record of my identity other than the fleeting and casual memory of the store clerk. But today if I want to purchase a book I am likely to do so online, where not only the bookstore, but also my Internet service provider and payment provider will make personal records. Indeed, the bookstore might not only record what books I ultimately purchase, but every book I peruse. And these records are stored in a digital format that permits, once an architecture has been established, essentially costless searching and distribution.

Nothing in the Fourth Amendment prohibits such a bookstore, or any other third party, from conveying information to law enforcement on its own initiative. Thus, even if there is some constitutional restraint on government-initiated access, it is not clear that sharing is a boon for criminals. More generally, it is dubious to justify the Third Party Doctrine on the grounds of technological neutrality when technology causes ever more personal information to be subject to its vacuum.

---

have used, and I presume it will ultimately use, the familiar "reasonable suspicion" in place of the ambiguous "reasonable to believe." *See id.* at 1719.

45. Much of the reason Kerr thinks we need a binary Third Party Doctrine is because he believes in a binary Fourth Amendment: "If any observation of any part of the target's conduct violates his reasonable expectation of privacy, then the police would need a warrant to observe any aspect of his behavior." Kerr, *supra* note 39, at 576. Although the Supreme Court has sometimes hemmed and hawed, that monolithic view simply is not necessary post-*Terry*. Indeed, there is an irony in justifying a regime of no protection on the grounds that were we to give any protection it would have to be the highest known to constitutional law.

46. *See* Kerr, *supra* note 39, at 564.

47. *See* United States v. Dunn, 480 U.S. 294, 300 (1987) (protecting as curtilage that area intimately tied to a home).

48. *See* Florida v. Riley, 488 U.S. 445, 450–51 (1989) (refusing protection from an aircraft flyover); California v. Ciraolo, 476 U.S. 207, 215 (1986) (same).

49. *See* United States v. Arellano-Ochoa, 461 F.3d 1142, 1145 (9th Cir. 2006) (prohibiting opening of screen door without warrant or other justification).

50. *See* California v. Greenwood, 486 U.S. 35, 37 (1988) (refusing protection for garbage left for collection).

In a nutshell, I remain as skeptical as ever of the Third Party Doctrine, but more hopeful regarding its fate.

## II. CONSIDERING AUTOMATION

What Tokson adds to this mix is the careful consideration of another technological development: automation. What would have at one time required a human can now be done by machine. Hence, while at one time human operators connected telephone calls, today this is handled entirely by artificial means. In one of the key third-party cases, *Smith v. Maryland*, the Supreme Court deemed that automation irrelevant: "We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate."[51] But the Supreme Court has also repeatedly held that whether government conduct constitutes a search depends upon whether it invades a "reasonable expectation of privacy,"[52] and Tokson marshals evidence that people consider information private if it is reviewed solely by computer.[53] Thus, by accessing that information the government infringes upon that expectation. Although the Court might assert that the disclosing party "assumed that risk," that merely begs the question. It is the law that defines what risks we do and do not assume.[54]

Therefore, Tokson argues—and I agree—that one can retain a reasonable expectation of privacy in information provided to an automated third party. He also gives courts reason to depart from the content/non-content distinction that reigns in the traditional telephone context. But Tokson's data does not demonstrate that people are unconcerned with automated use of their information, but rather only that people are even more concerned with human use. Thus, he cites surveys in which between fifty and sixty percent of respondents are uncomfortable with automated use of their data for purposes of targeted advertising.[55] Although he discounts a survey in which a much higher eighty-seven percent of respondents report that they would likely deny permission for such automated use,[56] the results of his own empirical work demonstrate that people believe automated use of their data is invasive, albeit less invasive than human use.[57]

---

51. 442 U.S. 735, 744–45 (1979).

52. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 33 (2001).

53. *See* Tokson, *supra* note 4, at 617–25.

54. In this Essay, I unfortunately lack the space needed to cover click-through agreements that bury generalized "consents" to government access, but there are serious questions of knowledge and voluntariness.

55. Tokson, *supra* note 4, at 617–20.

56. *Id.* at 619–20.

57. *See id.* at 620–21 (ranking automated uses of web surfing data from between 6.1 to 6.9 on a 10 point intrusiveness scale).

Tokson and I disagree as to whether automated use can infringe upon privacy.[58] In my view, at information privacy's core is the ability to control what information about you is conveyed to others, and for what purposes. If, without my permission or even expressly contrary to my permission, a third party runs my data through a human-programmed algorithm that reacts to its contents, that is an infringement of my right to control, and thus my right to privacy.[59] It would be an even more significant infringement if the third party were to turn over my data to another for this purpose, such as the government. Being human programmed, any such algorithm is human guided, even if only to give credence to believed statistical correlations. If, to use Tokson's example, the content of advertising is based upon searches of my data, upon receipt I would rightly wonder *why* the provider believes I am interested in those certain things, and indeed depending upon its content, I might be offended that it has made this assumption.

Umbrage is not the only potential harm. Imagine an Internet service provider's algorithm sending advertisements for "how to commit suicide" books to those who search for particular terms or visit particular pages, perhaps including those concerning obesity or bullying. When a recipient goes forward and kills him- or herself, one could try to categorize this as a harm other than a privacy harm. But since it all began with a breach of the right to control what information about oneself is used by others and for what purposes, certainly the harm includes, if it not is limited to, an infringement of informational privacy.

Tokson's survey results support my view. Respondents were relatively unconcerned with automated screening of e-mail content for spam,[60] but considered it more invasive if that automated software made another decision based on the content, in this case for purposes of targeted advertising.[61] Similarly, respondents deemed automated collection and use of web-surfing data for purposes of targeted advertising quite invasive.[62] If automated use could not invade privacy, its precise nature would seem unimportant. In short, I am unwilling to accept the proposition that nothing but a human being can invade privacy. Not only does computing capability regularly advance, but what is at stake is the privacy of the information, and thus control over the information. Absent specific consent, any response to that information, automated or not, infringes upon that privacy.

My disagreement with Tokson is thus also a disagreement with Judge Richard Posner, who has argued that "machine collection and processing of

58. *See id.* at 622–23 (arguing automated use cannot infringe privacy).

59. For a differently reasoned privacy argument reaching the same conclusion and providing more examples, see Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. (forthcoming 2011).

60. *See* Tokson, *supra* note 4, at 621 (reporting an invasiveness of 3.4 out of 10).

61. *See id.* (reporting an invasiveness of 5.5 out of 10).

62. *See id.* (reporting an invasiveness range of 6.1 to 6.9).

data cannot . . . invade privacy,"[63] and therefore that the government can run computer searches of data without constitutional restraint.[64] If Tokson is correct that we retain privacy when we give information to third parties *because* computers do not—indeed, cannot—invade privacy, then it would seem the government could run machine searches of data without justification. Perhaps there would be an ultimate human reader, but it would occur only after the necessary justification, or perhaps in a future system the computer would inform officers to focus on a certain threat or a certain geographic area without revealing any of the searched data.

Like Judge Posner, I am not necessarily opposed to such suspicionless government computer searches of data.[65] The goal of data mining is to determine previously unknown information, and one can imagine instances in which the government has legitimate cause for running an algorithm upon a broad data set precisely because it might reveal previously unknown suspicions, even though the government does not now suspect any person whose information is contained therein. And as in the offline context of an automobile roadblock or regime of mandatory drug testing, each of us takes solace in knowing that we are not individually targeted for suspicion. But this of course means the government is not only reviewing data of the "usual suspects," meaning persons who would otherwise come to the attention of law enforcement, but instead is reviewing the data of very large numbers of persons who would otherwise never come under law enforcement suspicion. Hence, if we are to permit these suspicionless searches, we should rely upon other protections, such as broad or uniform applicability to gain the protections of the political process, advanced notice, use controls, and perhaps selective revelation which only permits individualized results upon a demonstration that the algorithm is sufficiently predictive.[66] I am not ready to concede that none of these restraints are required by the Fourth Amendment. In other words, although I am open to broadly considering the universe of possible constitutional constraints, I am not ready to concede—as I think Tokson might—that government computer searches of data are unrestricted by the Fourth Amendment.

Tokson and I do agree that courts need to understand the technology at issue before making a Fourth Amendment decision, and he ably demonstrates that in the context of the Internet there is evidence that they

---

63. Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, at A31.

64. *See* Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 254 (2008). According to Posner, "[c]omputer searches do not invade privacy because search programs are not sentient beings. Only [a] human search should raise constitutional or other legal issues." *Id.*

65. *See id.* at 252–53.

66. *See* Henderson, *supra* note 6, at 554–62; Christopher Slobogin, *Government Dragnets*, 73 LAW & CONTEMP. PROBS. (forthcoming 2011).

do not.[67] I also agree that the mere act of conveying information to a third party does not necessarily defeat a reasonable expectation of privacy.

What I do not accept is the inverse of Tokson's proposition.[68] Tokson argues that if a third party is automated, one retains a reasonable expectation of privacy. The inverse is therefore that if a third party is *not* automated, one does *not* retain a reasonable expectation of privacy. I realize that not every reader fondly recalls learning of inverse, converse, contrapositive, and contradiction, but it is rather easy to see that the inverse of a proposition is not necessarily true. For example, it is true that if a shape is a triangle, it is a polygon, but it is *not* true that if a shape is not a triangle, it is not a polygon. Therefore, I am not necessarily disagreeing with Tokson in making this claim. But the claim is critical. If the inverse of his hypothesis were true, it would lead to odd results that would seem difficult for the government to navigate.

Consider bank records. In the traditional system, which is still quite common, I would transfer money between accounts by physically presenting myself to a teller and providing the necessary authorization. In the computerized system, which is now also quite common, I can transfer money between accounts online in an automated transaction that a human might never witness. Not only would it be counterintuitive if one were treated as private and the other were not, but it would be a nightmare for officers wanting bank records: how are they to know which was the case, and therefore what, if any, authorization is required? And by every sensible measure the two transactions seem identically private. Just like I trust the bank's computer algorithm to preserve my privacy, meaning it will not e-mail information on my transfer to another, post it on the World Wide Web for all to see, or, absent a law specifically requiring it, send it to the government, I trust the teller to abide by both contract and positive law forbidding disclosure. Hence, one can retain a reasonable expectation of privacy regardless of automation.

## III. THE IDEAL STANDARD

So, how should courts determine when a person retains a reasonable expectation of privacy in information given to a third party? Unfortunately, by hard work. Smart people have been thinking about this for some time, and I have seen no persuasive easy answer. This is unfortunate, because courts interpreting a constitutional provision—even one as explicitly vague as protecting against "unreasonable searches and seizures"—are not legislating, and I have always been wary of my proposals seeming to out-do even *Miranda* in terms of generating a complicated set of specific rules from a brief constitutional provision. I do not even take much solace from

67. *See* Tokson, *supra* note 4, at 627–29.

68. Using the implication "if P, then Q," the inverse is "if not P, then not Q."

*Miranda* now having a completely non-textual "two week" rule,[69] because I am genuinely more comfortable crafting a complicated set of factors to be used by legislators than by courts. But at least until comprehensive legislation exists, I cannot see any way out of it. In the words of Professor Daniel Solove:

> In an ideal world, government information gathering would be regulated by a comprehensive statutory regime. Courts would analyze whether the rules in this statutory regime met basic Fourth Amendment principles rather than craft the rules themselves. A pronouncement as short and vague as the Fourth Amendment best serves as a guidepost to evaluate rules, rather than as a source of those rules.
>
> But a comprehensive statutory regime to regulate government information gathering does not yet exist. Statutes regulate government information gathering in isolated areas, but there is no all-inclusive regime. For better or worse, the Fourth Amendment has been thrust into the role of the primary regulatory system of government information gathering. Until there is a substitute, we should treat the Fourth Amendment as the regulatory system it has been tasked with being. If legislatures respond with rules of their own, courts should shift from crafting the rules to evaluating the rules made by legislatures.[70]

Thus, I still propose something like the factors I have previously published, but culled to a more administrable format. Via my work as Reporter for the American Bar Association ("ABA") Task Force on Government Access to Third Party Records, my nine factors have been streamlined into four. A transferor's expectation of privacy should depend on the extent to which:

(1) The initial transfer of the information from the person to a third party is reasonably necessary to participate meaningfully in society or is socially beneficial, including to freedom of speech and association;
(2) The information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma if disclosed, and whether outside of the initial transfer to a third party it is typically disclosed only within one's close social network, if at all;

---

69. *See* Maryland v. Shatzer, 130 S. Ct. 1213, 1227 (2010) ("Because Shatzer experienced a break in *Miranda* custody lasting more than two weeks between the first and second attempts at interrogation, *Edwards* does not mandate suppression of his March 2006 statements.").

70. Daniel Solove, Essay, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1515 (2010) (footnote omitted).

(3) The information is accessible to and accessed by non-government persons outside the institution; and
(4) Existing law restricts or allows access to and dissemination of the information or similar information.

Although this intermediate stage of work does not reflect the position of the ABA, it reflects my current best thinking. It will have to await other publications to do the factors descriptive justice, but one thing is immediately apparent: My third factor considers only the accessibility of the information *outside* the third party, thus not relying upon Tokson's automation distinction. Again, this is not so much because I disagree with Tokson's hypothesis, but because I disagree with its inverse and thus would not limit protection to automated third parties.

Perhaps ironically, since I am hoping for the bigger change, I do not think the future is as bleak as Tokson suggests if courts do not buy into his automation rationale. But that is because I think his important article is only one act—albeit a very useful one—in this complicated third-party drama. The story of the Third Party Doctrine now spans some forty years, and because none of the difficult cases have reached the Supreme Court in the last decade, the most critical chapter remains untold. In predicting that result, I am mindful of Mark Twain's alleged cautionary words that "[t]he art of prophecy is very difficult, especially with respect to the future."[71] But I do not think the Third Party Doctrine can withstand the pressures which technology and social norms are placing upon it, and I most definitely do not think it should.

71. These words, or something very much like them, are often attributed to Twain. *See, e.g.*, Robert Samuelson, *The Burden of Global Aging*, CHI. TRIB., Mar. 2, 2001, at 19; *see also* Nicholas D. Kristof, *Be Careful What You Ask for*, N.Y. TIMES, Nov. 8, 2002, at A31. It seems, however, that they might be more accurately attributed to physicist Niels Bohr. *See* THE YALE BOOK OF QUOTATIONS 92 (Fred R. Shapiro ed., 2006) (quoting Niels Bohr as saying "it is difficult to predict, especially the future"). But the uncertainty—a concept that Bohr would very much appreciate even if it cost him a citation—permits the rhetorical benefit of beginning and ending with Twain.