Speeches

Keynote Address: The Path to ECPA Reform and the Implications of *United States v. Jones*

By JAMES X. DEMPSEY*

AT THE OUTSET, I MUST SAY that there are probably twenty people at this symposium who are equally well suited to give this keynote. People like Matt Parrella, Assistant U.S. Attorney, and Andy Weissmann, FBI General Counsel, who are using the authorities provided in the Electronic Communications Privacy Act ("ECPA")[1] every day to put bad guys in jail and make us all safer. People like Stephanie Pell, Richard Salgado, Paul Ohm, Judge Ryan, and others who, at earlier stages in their careers, themselves used these tools to fight crime. People like Bryan Cunningham and others, who are daily advising companies trying to interpret this law and apply it in the context of real requests. People like Professor Susan Freiwald and Kevin Bankston, who have written amicus briefs in many of the recent key cases interpreting ECPA. And of course, Magistrate Judge Stephen Smith, who helped spark the magistrates' revolt and is writing the opinions that are helping pave the way forward on defining the relationship among ECPA, the Fourth Amendment, and new technological realities.

---

* James X. Dempsey is Vice President for Public Policy at the Center for Democracy & Technology and head of CDT West. He coordinates the Digital Due Process coalition.

1. Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). ECPA amended the federal Wiretap Act, currently codified as amended at 18 U.S.C. §§ 2510–22 (2006), to extend its rules for real-time interception to include electronic communications. Tit. I, §§ 101–110, 100 Stat. at 1848–59 (codified as amended at 18 U.S.C. §§ 2510–22 (2006)). ECPA also added new chapters setting standards for access to stored communications and transactional records, tit. II, § 201, 100 Stat. at 1860–68 (codified at 18 U.S.C. §§ 2701–11 (2006)), and for use of pen registers and trap and trace devices, which collect transactional data in real-time, tit. III, § 301, 100 Stat. at 1868–72 (codified at 18 U.S.C. §§ 3121–26 (2006)).

All of these, and others I have probably overlooked, are equally well suited to be speaking at length about the challenges of applying and updating ECPA in the digital age.

So where does that leave me? I think that my expertise, such as it is, is in the legislative arena, and that is where I am going to focus. Overall, I think there is a fascinating story here of how law reform does or does not occur. First, I am going to provide a little historical background on the legislative efforts to reform ECPA. Then, I will specifically discuss the Digital Due Process coalition and then I will spend a little bit of time talking about the future. In looking to the future, I am going to focus mainly on the non-content issues, which is where I think the real controversy now lies, post-*Warshak*.[2]

In terms of the history, we could go all the way back to 1877 when the Supreme Court held in *Ex parte Jackson*[3] that letters voluntarily disclosed to a third party—the Post Office in that case—are protected by the Constitution.[4] That case involved the same arguments about voluntary surrender that we still hear today around the third-party records doctrine.[5] However, instead of tracing the story from *Ex parte Jackson* to *Olmstead*[6] to *Katz*[7] to *Smith v. Maryland*,[8] I will go back only to the early 1990s and give a short timeline of what has happened since the enactment of ECPA.

ECPA was clearly a forward-looking statute and, in drafting it, members of Congress displayed a remarkable appreciation for the power of the then-emerging Internet and wireless technologies. At a

2. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

3. 96 U.S. 727 (1877).

4. *Id.* at 733.

5. *Id.* Briefly stated, the third-party records doctrine posits that you lose any Fourth Amendment rights in information that you voluntarily disclose to a third party, such as the information revealed or created in the course of a business transaction. *See, e.g.*, Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV 3, ¶¶ 36–49; Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

6. Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that warrantless tapping of telephone wires does not violate the Fourth Amendment, absent a physical invasion of personal property, because "one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside").

7. Katz v. United States, 389 U.S. 347, 351–52 (1967) (along with Berger v. New York, 388 U.S. 41 (1967), overturning *Olmstead* and stating, "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public . . . 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" (citations omitted)).

8. 442 U.S. 735, 741–46 (1979) (holding that the installation and use of a pen register was not a search under the Fourth Amendment because petitioner voluntarily conveyed phone numbers to the telephone company and thus lacked a reasonable expectation of privacy).

time when even the people inventing and deploying the technologies did not fully appreciate the revolution that was occurring, some members of Congress saw the need for a legal framework that would create the trust that could allow innovative services to become widely accepted.

Despite the remarkable achievement of ECPA, it was not very long before the limitations of the statute began to emerge. For example, by the early 1990s, concerns were being raised about the richness of the transactional data associated with Internet communications, which the pen register standard of ECPA allowed the government to access without any real showing of suspicion or need.[9] Also, by the early 1990s, there was growing concern about the potential of mobile phones to serve as tracking devices.[10]

In 1994, when Congress adopted the Communications Assistance for Law Enforcement Act ("CALEA"),[11] requiring telephone companies to design their networks to be wiretap friendly, it amended ECPA to strengthen the standard for § 2703(d) orders,[12] specifically to address the richness of Internet transactional data. Also, Congress added language to CALEA prohibiting the government from obtaining location data from a cell phone solely with the authority of a pen register trap and trace device.[13] (Congress did not say what the standard for location data was. It merely said what the standard was not, i.e., that it could not be a pen register standard.) However, in 1994, CALEA did not address at all the other limits in ECPA that were growing in signifi-

9. *E.g., Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and the Law of the S. Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 103d Cong. 6, 158, 160–61, 166–78 (1994) [hereinafter *Joint Hearings: Law Enforcement Access to Telecommunications Technology*], *available at* http://ia700400.us.archive.org/23/items/digitaltelephony00wash/digitaltelephony00wash.pdf (statement of Jerry Berman, including memorandum of the Electronic Frontier Foundation).

10. *Id.*

11. Communications Assistance for Law Enforcement Act, Pub. L. No. 103–414, 108 Stat. 4279 (1994) (codified as amended at 47 U.S.C. §§ 1001–10 (2006)).

12. In its original incarnation, the ECPA standard for a court order for disclosure of transactional data and certain content required only a showing of "reason to believe the . . . information sought, [was] relevant to a legitimate law enforcement inquiry." Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, tit. II, §201(a), 100 Stat. 1848, 1861 (codified at 18 U.S.C. § 2703(d) (1988)). Currently, post-CALEA, the government must present specific and articulable facts showing that there are reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation. *See* 18 U.S.C. § 2703(d) (2006).

13. § 103, 108 Stat. at 4281 (codified as amended at 47 U.S.C. § 1002(a)(2)(B) (2006)).

cance, such as the 180-day rule for stored e-mail,[14] which even then no longer made sense given the way services were evolving.

In 1998, Senator John Ashcroft introduced the first significant ECPA reform bill, the E-Privacy Act,[15] cosponsored by the author of ECPA, Senator Patrick Leahy, and by a number of Republican senators, including current Senator Kay Bailey Hutchison of Texas. The Ashcroft bill would have required a court order based on probable cause for cell phone tracking,[16] a warrant for accessing content from a service provider (or a subpoena served on the subscriber to compel him to disclose his communications),[17] and true judicial review of both pen register and trap and trace applications, requiring the judge to make a finding of relevance.[18] The bill did not move, however, and expired at the end of the congressional session.[19]

In 1999, Senator Leahy reintroduced a nearly identical bill.[20] Then, in September of 2000, the Republican-controlled House Judiciary Committee, by a vote of twenty to one, reported legislation that would have required probable cause for access to cell phone location information[21] and, for pen-traps, a judicial finding of specific and articulable facts giving reason to believe the information sought was relevant to an ongoing investigation.[22] The bill also would have extended the 180-day rule to one year.[23] Remarkably, it also would have extended the statutory suppression rule in Title III (a rule that currently applies to interceptions only, and only wire and oral, but not electronic, communications)[24] to all electronic communications,[25] and to stored, as well as real time, access.[26]

14. 18 U.S.C. § 2703(a)–(b) (stating that the government can use a subpoena to compel a service provider to disclose e-mail that has been in electronic storage for more than 180 days).

15. Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY) Act, S. 2067, 105th Cong. (1998).

16. *Id.* § 104(a).

17. *Id.* § 103.

18. *Id.* § 105.

19. *See Overview: S. 2067 (105th): Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY) Act, 105th Cong.*, GOVTRACK.US, http://www.govtrack.us/congress/bills/105/s2067#overview (last visited Jan. 18, 2013).

20. The Electronic Rights for the 21st Century Act, S. 854, 106th Cong. (1999).

21. H.R. 5018, 106th Cong. § 7(h)(1) (2000); H.R. REP. NO. 106–932, at 17 (2000).

22. H.R. REP. NO. 106–932, at 15.

23. H.R. 5018 § 12.

24. *See* 18 U.S.C. § 2515 (2006).

25. *Id.* § 2.

26. H.R. 5018 § 2(a)(2).

That was and remains a high-water mark of ECPA reform legislation. The year 2000 was an election year. By the time the Judiciary Committee filed its report on the legislation, it was October, and the ECPA reform legislation died. In January 2001, a new administration took office, and then, of course, the attacks of September 11th, 2001 occurred. At that point, rational discussion of these issues became impossible.

In the Patriot Act,[27] in my view, there were expansions of government power that made sense. It was appropriate, for example, for Congress to establish authority for roving taps in intelligence investigations.[28] After all, ECPA had authorized roving taps on the law enforcement side in 1986.[29] Similarly, it was appropriate to tear down the wall that had separated law enforcement and intelligence. The wall had become totally perverted and was not serving either civil liberties or national security interests.

However, in my view, when addressing these legitimate concerns, and removing some of the unjustified constraints on the government that were inhibiting our ability to prevent future terrorist attacks, Congress should also have looked at the other side of the ledger. It should have taken up some of the ECPA reforms that the House Judiciary Committee had approved only a year earlier, so as to counterbalance the expansions of government power with the enhanced protections that it also acknowledged were needed. However, in October 2001, pleas for such balance were drowned out and, in subsequent years, ECPA reform disappeared from the legislative agenda.

In precincts less susceptible to the fear that dominated our political discourse after 9/11, ECPA reform was not totally forgotten. In 2003, George Washington University held a symposium entitled "The Future of Internet Surveillance Law," which produced a number of articles, including Orin Kerr's *A User's Guide to the Stored Communications Act and a Legislator's Guide to Amending It*,[30] Deirdre Mulligan's

27. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. 107–56, 115 Stat. 272 (2001) (codified in scattered sections of the U.S.C.).

28. § 206, 115 Stat. at 282.

29. Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, tit. I, §106(d), 100 Stat. 1848, 1856–57 (codified as amended at 18 U.S.C. § 2518(11)).

30. 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, 1208–09 (2004) (explaining the basic structure and text of the Stored Communications Act, which was enacted as a part of ECPA, and suggesting four categories of potential reforms including bolstering privacy protections, simplifying the statute, repealing provisions that have caused more harm than good, and restructuring the remedies scheme for violations).

article, *A Critical Perspective on ECPA*,[31] and Patricia Bellia's article, *Surveillance Law through Cyberlaw's Lens*,[32] all of which had basically the same premise: that ECPA, in various ways, was outdated and needed to be amended.

Despite the widespread recognition that ECPA was outdated, throughout the first decade of the new millennium there was no congressional interest in ECPA reform. Instead, the Foreign Intelligence Surveillance Act ("FISA")[33] dominated the agenda. In December of 2005, *The New York Times* broke the story about the National Security Agency's warrantless wiretapping program,[34] which led to a three-year battle that resulted ultimately in amending FISA to ratify and somewhat expand what the administration had been doing in the warrantless program.[35]

In the absence of congressional attention, but driven by ongoing, dramatic changes in the technology and the way people were using it, the action shifted to the courts. In 2003, in *Theofel v. Farey-Jones*,[36] the Ninth Circuit rejected the Justice Department's distinction between opened and unopened e-mail.[37] In June 2004, the First Circuit issued its *Councilman* decision,[38] in which the three-judge panel misinterpreted a key definition under the statute.[39] Both privacy advocates and the Justice Department agreed that the judges had gotten it

31. Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1559 (2004) (concluding that ECPA "has failed to keep pace with changes in and on the Internet and therefore no longer provides appropriate privacy protections").

32. Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1458 (2004) ("[I]n 1986, when Congress sought largely to align treatment of electronic communications with treatment of wire communications, it could not have anticipated that technological developments would place so many electronic communications in the hands of third parties.").

33. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95–511, 92 Stat. 1783 (codified as amended in 50 U.S.C. 1801–1871 (2006)) (defining rules for the collection of foreign intelligence information by electronic surveillance and other means).

34. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

35. *See* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110–261, 122 Stat. 2436 (2008).

36. 341 F.3d 978 (9th Cir. 2003), *reh'g denied and opinion superseded*, 359 F.3d 1066 (9th Cir. 2004).

37. Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004) (holding that "prior access is irrelevant to whether the messages at issue were in electronic storage").

38. United States v. Councilman, 373 F.3d 197 (1st Cir. 2004).

39. The panel held that an electronic communication that is in electronic storage, however temporary, is not covered by the Wiretap Act. *Id.* at 203–04.

wrong,[40] and an en banc decision[41] mitigated most of the confusion.[42] That case proved most significant for illustrating how hard it was for judges to interpret and apply the Act's non-intuitive categories.

Then, in August of 2005, Magistrate Judge James Orenstein in New York ruled that the government needed a warrant to track a cell phone in real time,[43] rejecting the so-called "hybrid theory" developed by the Justice Department to work its way around CALEA's prohibition on the use of a pen register to acquire location information.[44] A month or so later, Magistrate Judge Smith in Texas ruled the same,[45] and the magistrates' revolt was underway. As of today, we have had at least thirty magistrates' opinions going in both directions on the question of what is the standard for location information. All grappling with the fact that it is not clear under ECPA what that standard is.[46]

In July of 2006, a district court in Ohio enjoined the government from using an order under § 2703(d) to obtain stored e-mail.[47] That ruling ultimately led to the Sixth Circuit's December 2010 decision in

40. *See* Petition of the United States for Rehearing and for Rehearing En Banc at 1, United States v. Councilman, 385 F.3d 793 (1st Cir. 2004) (No. 03-1383); Brief for Center for Democracy & Technology, Electronic Frontier Foundation, Electronic Privacy Information Center, & American Library Association as Amici Curiae Supporting Appellant's Petition for Rehearing & Rehearing En Banc at 2, United States v. Councilman, 385 F.3d 793 (1st Cir. 2004) (No. 03-1383).

41. United States v. Councilman, 418 F.3d 67 (1st Cir. 2005).

42. *Id.* at 79–80 (concluding that the term "electronic communication" includes transient electronic storage that is intrinsic to the communication process for such communication).

43. *In re* Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 384 F. Supp. 2d 562, 564 (E.D.N.Y. 2005) (holding "the information the government seeks . . . is *not* information [it] may lawfully obtain absent a showing of probable cause").

44. *Id.* at 565. Under the hybrid theory, the Department of Justice claims that it can acquire real-time location information using the combined authority of a pen register order and an order issued under § 2703(d). *See, e.g.*, *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth. ("*In re Application for Cell Site Location Auth.*"), 396 F. Supp. 2d 747, 761 (S.D. Tex. 2005).

45. *In re Application for Cell Site Location Auth.*, 396 F. Supp. 2d at 765 ("The government's hybrid theory, while undeniably creative, amounts to little more than a retrospective assemblage of disparate statutory parts to achieve a desired result.").

46. For a description of the courts' conflicting responses to the government's arguments and a compilation of decisions through June 1, 2010, see *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 83–85, 93 (2010) [hereinafter *Hearing: Revolution in Location Based Technologies*] (statement of Magistrate Judge Stephen Wm. Smith).

47. Warshak v. United States, No. 1:06-cv-357, 2006 WL 5230332, at *8 (S.D. Ohio July 21, 2006).

United States v. Warshak,[48] which held ECPA unconstitutional to the extent that it allows access to stored e-mail with less than a warrant.[49]

Also in 2006, a district court in California decided a civil case, *Quon v. Arch Wireless*,[50] which held that there is a reasonable expectation of privacy in stored text messages[51]—a ruling that was upheld by the Ninth Circuit,[52] and which was left untouched by the Supreme Court when it considered the case under the name of *City of Ontario v. Quon*.[53]

With these cases, we may be seeing a shift in the attitude of the judiciary, away from merely complaining about how hard it is to interpret ECPA—a theme that pervaded the earlier cases—towards a recognition that the statute's rules, whatever they are, are inadequate as a constitutional matter, requiring courts to hold that a warrant is required in circumstances where the statute did not require one.

While the courts were grappling with ECPA's limitations, I began perceiving a shift in the attitude of the communications and Internet companies that are on the receiving end of government requests. As Al Gidari said in his famous remarks, these companies are caught in the middle between their recognition of the legitimate needs of the government, their desire to respect the privacy of their customers, and their business interest in providing a trusted service.[54] These companies want to cooperate with and recognize the legitimate interests of the government, but they also want to be able to provide better, clearer assurances of privacy to their customers.

The Center for Democracy and Technology ("CDT") coordinates the Digital Privacy and Security Working Group ("DPSWG"), a forum for companies, trade associations, and public interest groups from across the political spectrum. DPSWG actually predates CDT, having been established at the ACLU by Jerry Berman. Jerry moved management of DPSWG to the Electronic Frontier Foundation ("EFF") when he headed the EFF office in Washington for a while, then brought it

48. 631 F.3d 266 (6th Cir. 2010).

49. *Id.* at 288 ("[T]o the extent that the SCA purports to permit the government to obtain . . . emails warrantlessly, the SCA is unconstitutional.").

50. 445 F. Supp. 2d 1116 (C.D. Cal. 2006).

51. *Id.* at 1140–43.

52. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 903–08 (9th Cir. 2008).

53. 130 S. Ct. 2619, 2629–30 (2010) (avoiding the constitutional question of whether there exists a reasonable expectation of privacy in stored text messages, on prudential grounds).

54. Albert Gidari, Jr., *Companies Caught in the Middle*, 41 U.S.F. L. Rev. 535, 558 (2007).

with him in 1994 when he founded CDT.[55] CDT has managed DPSWG ever since. DPSWG served as a focus for the dialogue that led to the enactment of ECPA in 1986.[56] It also served as a forum for discussion and consensus building around the encryption debates of the 1990s.[57]

So when I began to sense around 2005 or 2006 that communications and Internet companies were becoming increasingly uncomfortable with the application of ECPA and with the disconnect between what they perceived their customers expected and what the statute allowed, DPSWG was the best forum in which to begin a dialogue around updating ECPA.

Convening DPSWG, CDT chaired a series of discussions through 2007, 2008, and 2009. First, we met every two to four months, exploring the issues. We started with a list of over a dozen issues. Gradually we pared these down and built consensus around a set of incremental reforms. As concerns coalesced, the pace of our meetings picked up. We began to meet face-to-face and by conference call on a monthly, and then ultimately a weekly basis,[58] bringing together companies, public interest groups, and other experts. Among others playing key roles were former prosecutors,[59] such as Richard Salgado and Mark Zwillinger, who brought to the discussion their practical experience about the government's needs.

During this process, several key points emerged that I believe are critical to the success of ECPA reform. First of all, it is critical to have the participation and support of the companies that are developing

55. *See Joint Hearings: Law Enforcement Access to Telecommunications Technology*, *supra* note 9, at 65–67; *Electronic Communications Privacy Act: Hearings on H.R. 3378 before the Subcomm. on Courts, Civil Liberties and the Administration of Justice of the Comm. on the Judiciary*, 99th Cong. 469 (1985) [hereinafter *House ECPA Hearings*], *available at* http://www.justice.gov/jmd/ls/legislative_histories/pl99-508/hear-50-1985.pdf (memorandum summarizing a consultation convened by what later became DPSWG regarding the privacy issues posed by electronic mail).

56. *See Electronic Communication Privacy: Hearing on S. 1667 Before the Subcomm. on Patents, Copyrights and Trademarks of the S. Comm. on the Judiciary*, 99th Cong. 124–25 (1985) [hereinafter *Senate ECPA Hearing*], *available at* http://www.justice.gov/jmd/ls/legislative_histories/pl99-508/hear-j-99-72-1985.pdf (statement of Jerry Berman describing industry-privacy consultations on electronic communications privacy).

57. *See* ELEC. SURVEILLANCE TASK FORCE OF THE DIGITAL PRIVACY & SEC. WORKING GRP., INTERIM REPORT: COMMUNICATIONS PRIVACY IN THE DIGITAL AGE 23–26 (1997), *available at* https://www.cdt.org/wiretap/9706rpt.html (last visited Jan. 25, 2013).

58. *Electronic Communications Privacy Act Reform, Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 5 (2010) [hereinafter *Hearing: Privacy Act Reform*] (statement of James X. Dempsey), *available at* http://judiciary.house.gov/hearings/printers/111th/111-98_56271.PDF.

59. *Id.*

innovative technologies and offering the communications services that have become so central to our daily lives. Particularly post-9/11, civil liberties interests have to be combined with the interests of the corporate sector in innovation, certainty, clarity, and customer trust as essential components of the business model. Indeed, it was industry and civil liberties groups working together that promoted passage of ECPA in the first place.[60] Key corporate supporters in 1986 included AT&T and IBM.[61] It is crucial that they be actively engaged today as well.

Second, ECPA reform must be bi-partisan. It must not be pigeonholed according to the left-right, liberal-versus-conservative dynamics that infect so many policy debates. The Fourth Amendment is just as dear to conservatives and libertarians as it is to liberals. Limits on government power are at the core of the conservative and libertarian philosophies. I am very proud that the ECPA reform effort includes Americans for Tax Reform, the Competitive Enterprise Institute, and other leading conservative and libertarian voices.[62]

Third, ECPA reform must preserve the building blocks of the investigative process: the subpoena for subscriber identifying information and other basic information, the court order issued under § 2703(d) on less than probable cause for Internet transactional information, and the warrant for communications content and other highly sensitive information. It is important that investigators have the ability to work their way up that ladder of authority, gaining access to more sensitive data as the standard increases.

Fourth, ECPA reform does not have to take on the whole third-party doctrine. The concurring opinions in *Jones* may prompt a reconsideration of the third-party doctrine,[63] but ECPA reform need focus only on communications data and communications service providers.

60. S. REP. NO. 99-541, at 5–6 (1986) (listing corporate supporters of the legislation); H. REP. NO. 99-647, at 29–30 (1986) (same).

61. *House ECPA Hearings*, *supra* note 55, at 108–10 (transcript of AT&T testimony in support of the Act); *Senate ECPA Hearing*, *supra* note 56, at 155 (listing ECPA's supporters, including corporate sponsors AT&T and IBM).

62. *See Who We Are*, DIGITAL DUE PROCESS, http://digitalddueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163 (last visited Nov. 9, 2012) (alphabetically listing all Digital Due Process coalition members).

63. *See* United States v. Jones, 132 S. Ct. 945, 954–57 (2012) (Sotomayor, J., concurring) (finding that even short term GPS monitoring violates society's reasonable expectation of privacy and suggesting that, in the digital age, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"); *id.* at 957–64 (Alito, J., concurring) (finding that the

Fifth, it is best to leave in place the parallel system of authorities that exist for national security investigations and not to try to harmonize standards under ECPA with those under FISA. FISA is probably more confusing and less coherent than ECPA, but rational debate over FISA standards is impossible given the fear of terrorism and the secrecy that surrounds the interpretation and application of FISA.

Sixth, in reforming ECPA, it is not necessary to change—and may be best to leave unchanged—the rules surrounding the use of subpoenas served on individuals or corporations that demand disclosure of the communications or other records created by and pertaining to those individuals or corporations. Traditionally, when the government seeks records from a corporation, it serves a subpoena on the corporation itself, compelling the corporation to turn over all responsive records, including copies of communications to or from the corporation that are stored by or accessible to the corporation.[64] Even though such a subpoena is not based on probable cause, it is "reasonable" as a matter of Fourth Amendment law, provided it satisfies certain requirements.[65] The recipient of the subpoena can resist it on the grounds that it is overbroad or burdensome.[66] ECPA reform will not require the government to obtain a warrant in order to compel a corporation to disclose its own communications (as both sender and recipient). In the case of individuals, the Fourth Amendment allows the government to use a subpoena to demand that the individual turn over relevant records that are in the individual's possession or otherwise available to

long-term surveillance of defendant's movements, enabled by modern technology, violated society's reasonable expectation of privacy).

64. *See, e.g.*, U.S. DEP'T OF JUSTICE, GRAND JURY MANUAL § III.A.2(c) (1991) ("Subpoenas duces tecum may be served on any natural person, legal entity, or corporation. . . . Documents or other tangible items may be obtained by subpoena duces tecum from any person who is either in physical or constructive possession or control of them."). The same rule applies to civil investigations, where the Federal Rules of Civil Procedure specify that a subpoena extends to electronically stored information in a person's "possession, custody, or control." FED. R. CIV. P. 45(a)(1)(A)(iii). Control under this rule has been construed "as the legal right, authority or *practical ability* to obtain the materials sought upon demand." SEC v. Credit Bancorp, Ltd., 194 F.R.D. 469, 471 (S.D.N.Y. 2000) (emphasis added). *See also* SEC. & EXCH. COMM'N DIV. OF ENFORCEMENT, ENFORCEMENT MANUAL § 3.2.6.2 (2012) ("The subpoenaed entity or individual is required to produce all subpoenaed items that are in its possession, custody or control. This includes items under the subpoenaed entity or individual's control or custody, but that are not in its immediate possession.").

65. Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 208–09 (1946).

66. *Id.*; *see also* Joshua Gruenspecht, *"Reasonable" Grand Jury Subpoenas: Asking for Information in the Age of Big Data*, 24 HARV. J.L. & TECH. 543, 545–47 (2011) (noting that the reasonableness of a subpoena turns on its "relevance, particularity, and . . . temporal scope").

him,[67] but the Fifth Amendment may limit the ability of the government to compel an individual to disclose any such records.[68] The Fifth Amendment does not protect corporations in this context.[69] ECPA reform need not affect current practice under these rules; ECPA reform instead is focused on compelled disclosure from service providers. To the extent that the Constitution allows use of subpoenas to require a party to disclose its own communications, that rule would remain unaffected by ECPA reform.

Guided by these principles, and after some remarkable meetings that built trust among the participants, a DPSWG spin-off coalition calling itself Digital Due Process ("DDP") was launched in March 2010.[70] At the time, the coalition consisted of nine companies and twelve trade associations, think tanks, and advocacy groups.[71] As of March 2012, the coalition has tripled in size, growing to twenty-seven companies and thirty-one associations and groups.[72]

The goal of DDP is to "simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public."[73] Within this framework, DDP adopted four principles. First,

> A governmental entity may require an entity covered by ECPA (a provider of wire or electronic communication service or a provider of remote computing service) to disclose communications that are

67. *In re* Grand Jury Subpoena (Rich & Co. v. United States), 707 F.2d 663, 667 (2d Cir. 1983) ("The test for the production of documents is control, not location."); Schwimmer v. United States, 232 F.2d 855, 860 (8th Cir. 1956) ("The law recognizes no distinction between constructive possession, with control, and physical possession, as a basis for a subpoena to compel production . . . ."); *see also* FED. R. CIV. P. 45(a)(1)(A)(iii) (a subpoena commands the person to whom it is directed to produce documents in that person's possession, custody, or control); Cooper Indus. v. British Aerospace, 102 F.R.D. 918, 919 (S.D.N.Y. 1984) (to be subject to subpoena "[d]ocuments need not be in the possession of a party to be discoverable, they need only be in its custody or control."). For a general discussion of the position of subpoenas under the Fourth Amendment, see *In re* Subpoena Duces Tecum (United States v. Bailey), 228 F.3d 341 (4th Cir. 2000).

68. *See* United States v. Hubbell, 530 U.S. 27, 43–46 (2000).

69. Braswell v. United States, 487 U.S. 99, 104–05 (1988).

70. Miguel Helft, *A Wide Call to Improve Web Privacy*, N.Y. TIMES, Mar. 31, 2010, at B1.

71. Press Release, Digital Due Process, Advocacy Groups, Companies Call for an Update of the Privacy Framework for Law Enforcement Access to Digital Info. (Mar. 30, 2010), *available at* http://digitaldueprocess.org/index.cfm?objectid=3CD858A0-ABFA-11E0-817A000C296BA163.

72. *See Who We Are*, *supra* note 62 (alphabetically listing members of DDP).

73. *Id.*

> not readily accessible to the public only with a search warrant issued based on a showing of probable cause, regardless of the age of the communications, the means or status of their storage or the provider's access to or use of the communications in its normal business operations.[74]

This reform would mean that the government, except in emergency circumstances or pursuant to one of ECPA's other exceptions, would need a warrant to compel a service provider to disclose stored communications content—whether opened or unopened and whether more than 180 days old or not. Basically, this change would eliminate for this purpose the significance of the difference between an electronic communication service ("ECS")[75] and a remote computing service ("RCS").[76] As an e-mail moved from ECS to RCS status, its legal protection would not change. All e-mail—messages in the spam folder, the read messages, the unread messages—regardless of age, would be covered by the same standard.

The second principle adopted by DDP states, "[a] governmental entity may access, or may require a covered entity to provide, prospectively or retrospectively, location information regarding a mobile communications device only with a warrant issued based on a showing of probable cause."[77] This reform would establish the probable cause standard for location tracking information, including information identifying cell towers, which is becoming increasingly more detailed and revealing.

The third adopted principle says,

> A governmental entity may access, or may require a covered entity to provide, prospectively or in real time, dialed number information, email to and from information or other data currently covered by the authority for pen registers and trap and trace devices only after judicial review and a court finding that the governmental entity has made a showing at least as strong as the showing under 2703(d).[78]

This principle would reform the pen-trap statute, which currently says that the court, whenever presented with an application by the

74. *Our Principles*, DIGITAL DUE PROCESS, http://digitalddueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163 (last visited Jan. 14, 2012).

75. Electronic Communications Privacy Act, 18 U.S.C. § 2510(15) (2006) (defining "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications").

76. 18 U.S.C. § 2711(2) (defining "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system").

77. *See Our Principles*, *supra* note 74.

78. *Id.*

government, "shall" issue the order if it finds that the government has said that the information sought is relevant to an ongoing investigation.[79] Ironically, current law states that when the government seeks Internet transactional data from storage, it must obtain a court order under § 2703(d) based on a showing of "specific and articulable facts."[80] The proposed reform would establish the § 2703(d) standard as the uniform rule for both real-time interception and access to stored transactional data.

Fourth and finally, "[w]here the Stored Communications Act authorizes a subpoena to acquire information, a governmental entity may use such subpoenas only for information related to a specified account(s) or individual(s). All non-particularized requests must be subject to judicial approval."[81] This principle would prevent the government from using subpoenas for bulk disclosure of transactional data. It responds to cases, such as the Indymedia investigation, where the government has tried to use a subpoena to obtain all of the information on all of the subscribers who have accessed a certain page or certain content.[82] Under the DDP proposal, such bulk information would not be available without a warrant under the § 2703(d) standard.

In response to the launch of DDP's recommendations, the Judiciary Committees of both the House and the Senate held hearings on ECPA reform. The House Committee held three hearings starting in May 2010.[83] The Senate Committee held a hearing in September of the same year.[84] In May of 2011, Senator Leahy, chairman of the Senate Judiciary Committee and the original author of ECPA, introduced

79. 18 U.S.C. § 3123(a)(1) (2006).

80. *Id.* § 2703(d).

81. *See Our Principles*, *supra* note 74.

82. *See How the Government Secretly Demanded the IP Address of Every Visitor to Political News Site Indymedia.us*, ELECTRONIC FRONTIER FOUNDATION (Nov. 9, 2009), https://www.eff.org/wp/eff-s-secret-files-anatomy-bogus-subpoena; Declan McCullagh, *Justice Dept. Asked for News Site's Visitor Lists*, CNET (Nov. 10, 2009, 9:10 PM), http://news.cnet.com/8301-13578_3-10394026-38.html.

83. *Hearing: Privacy Act Reform*, *supra* note 58; *ECPA Reform and the Revolution in Cloud Computing, Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. (2010), *available at* http://judiciary.house.gov/hearings/printers/111th/111-149_58409.PDF; *Hearing: Revolution in Location Based Technologies*, *supra* note 46.

84. *See The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age, Hearing Before the S. Comm. on the Judiciary*, 111th Cong. (2010), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-111shrg66875/pdf/CHRG-111shrg66875.pdf.

ECPA reform legislation,[85] adopting several of the recommendations of our coalition, notably a warrant for access to content[86] and a warrant for real time tracking of location information.[87]

The following month, in June 2011, Senator Ron Wyden in the Senate, and Representatives Jason Chaffetz and Bob Goodlatte in the House, introduced the Geolocational Privacy and Surveillance Act[88] ("GPS Act"), requiring a warrant for access to both real time and stored location information.[89] In October 2011, on the twenty-fifth anniversary of the enactment of ECPA, Republican Senator Kirk cosponsored the Wyden legislation.[90] On November 29, 2012, the Senate Judiciary Committee reported legislation that would have amended ECPA to require a warrant for the government to compel a service provider to disclose the content of communications.[91] The legislation expired at the end of the congressional session without further action, but the bi-partisan vote signaled the start of a new phase in ECPA reform.

Meanwhile, the pace of the judicial process has accelerated, with some dramatic results. In August 2010, the D.C. Circuit held that the planting of a GPS device was a search requiring a warrant.[92] In September 2010, the Third Circuit ruled that magistrates could require the government to obtain a warrant in order to compel a service provider to disclose stored cell site information.[93] In December of the same year, the Sixth Circuit ruled in the *Warshak* case that stored e-mail was constitutionally protected and that ECPA was unconstitutional to the extent that it allowed access to e-mail content without a

85. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011).

86. *Id.* § 3.

87. *Id.* § 5.

88. *See* Geolocational Privacy and Surveillance Act, S. 1212, 112th Cong. (2011); Geolocational Privacy and Surveillance Act, H.R. 2168, 112th Cong. (2011).

89. *See* S. 1212 § 2602(h); H.R. 2168 § 2602(h).

90. Press Release, Mark Kirk, U.S. Sen. for Illinois, Kirk Joins Wyden as Cosponser of Digital Surveillance Legislation (Oct. 18, 2011), *available at* http://www.kirk.senate.gov/?p=press_release&id=337.

91. Press Release, Patrick Leahy, U.S. Sen. for Vermont, Senate Judiciary Committee Approves Leahy-Authored Legislation to Update Video Privacy Protection Act, Electronic Communications Privacy Act (Nov. 29, 2012), *available at* http://www.leahy.senate.gov/press/senate-judiciary-committee-approves-leahy-authored-legislation-to-update-video-privacy-protection-act-electronic-communications-privacy-act.

92. United States v. Maynard, 615 F.3d 544, 566 (D.C. Cir. 2010).

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

warrant.[94] And then, of course, most remarkably, in January 2012, the Supreme Court handed down its decision in the *Jones* case, holding that the government's installation and use of a GPS device to track a person for twenty-eight days was a search under the Fourth Amendment.[95]

Looking to the future, I think the debate on e-mail is essentially over. The Sixth Circuit requires a warrant.[96] The Ninth Circuit would almost certainly hold the same, based on its finding in the *Quon* case that there is a reasonable expectation of privacy in stored texts.[97] The leading providers of cloud-based e-mail services have said that they insist on a warrant for disclosure of content[98] and, in practice, the government seems to be using a warrant in most cases. Perhaps the government is getting stored content without a warrant in some cases in some jurisdictions, but I think it is unlikely that the government would ever seek a straight ruling that there is no expectation of privacy in stored e-mail. Instead, it is more likely to try to cite specific terms of service as eliminating the reasonable expectation of privacy for that particular service. For reasons beyond our scope here, I believe that effort should fail in most if not all cases.[99]

94. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

95. United States v. Jones, 132 S. Ct. 945, 949 (2012).

96. *See Warshak*, 631 F.3d at 288.

97. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904–08 (9th Cir. 2008).

98. *Dropbox Law Enforcement Handbook*, DROPBOX, https://dl.dropbox.com/s/77fr4t57t9g8tbo/law_enforcement_handbook.html (last visited Jan. 14, 2013) ("Dropbox will not provide user content, whether in files or otherwise, without a search warrant (or an equivalent legal obligation) that requires the content to be disclosed."); *Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/safety/groups/law/guidelines/ (last visited Jan. 14, 2013) ("A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, wall posts, and location information."); *Guidelines for Law Enforcement*, TWITTER, http://support.twitter.com/groups/33-report-a-violation/topics/148-policy-information/articles/41949-guidelines-for-law-enforcement#section5 (last visited Jan. 14, 2013) ("[R]equests for contents of communication require a U.S. search warrant"); *see* Chris Soghoian, *Google's Pro-Privacy Legal Position Re: DOJ Could Assist Class Action Lawyers in Search Referrer Privacy Lawsuit,* SLIGHT PARANOIA, (Apr. 4, 2012) http://paranoia.dubfire.net/2012/04/googles-pro-privacy-legal-position-re.html (quoting remarks by Richard Salgado at this symposium stating that "Google and I think a lot of providers are taking this position, [seeing] the 4th amendment particularly as it has been applied in the Warshak cases, as establishing that there is a reasonable expectation of privacy such that disclosure of the contents held with the third party is protected by the 4th Amendment. And not limited to email, but other material that is uploaded to the service provider to be handled by the service provider.").

99. *See* Jim X. Dempsey, *Privacy Policies Don't Trump Expectation of Privacy,* CENTER FOR DEMOCRACY & TECH. (Apr. 21, 2011), https://www.cdt.org/blogs/jim-dempsey/privacy-policies-dont-trump-expectation-privacy.

Despite what seems to be a clear trend suggesting that privacy advocates have already won on the standard for stored communications, I—being a little bit of a legislative purist—think it would still be useful to correct the statute. Not only has a major statute protecting the privacy rights of Americans now been held unconstitutional in part, but, as a major investigative tool for law enforcement agencies at the state and federal level, it deserves to be made consistent with the Constitution. To some degree, I understand the Justice Department's willingness to continue operating under an unconstitutional statute. Regardless, I think it would be logical to eliminate the unconstitutional language from ECPA, which can be easily done.

The real battle now is over transactional data. In this regard, *Jones* is momentous. In that case, not a single member of the Supreme Court accepted the Justice Department's argument that a person has zero privacy interest in information voluntarily disclosed to a third party (in that case, one's location on the public street). In other words, not a single Justice in *Jones* was swayed by the vision of privacy that underpins the third-party doctrine.

In retrospect, after reading *Jones*, it is remarkable how much scope the lower courts accorded the third-party doctrine in the years since it was first laid down. First of all, as Professor Freiwald has explained in her articles, when you actually read *Smith v. Maryland*, you see how narrow that opinion was.[100] The Supreme Court noted there that pen-trap information does not reveal whether the call was completed or not.[101] Today, in contrast, transactional data collected by a pen-trap can reveal the websites you visit, what port number is being used (which can indicate the application or process that is being used), the time, date and duration of each communication, the size of each communication, the existence and size of any attachments to an e-mail, the IP addresses and "to" and "from" addresses of the parties

100. *See, e.g.*, Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 733 (2011) ("Finally, far from establishing a broad 'non-contents' rule, *Smith* covered only the telephone numbers the target dialed and limited its reasoning to that data."); Susan Freiwald & Patricia L. Bellia, *Fourth Amendment Protection for Stored E-Mail*, U. CHI. LEGAL F. 121, 163 (2008) ("*Smith* did not address the vastly richer information available about modern communications, such as the identities of the parties, the duration of their communications, and all of the information associated with web-based communications and use.").

101. Smith v. Maryland, 422 U.S. 735, 741–42 (1979) (quoting United States v. N.Y. Tel. Co., 434 US. 159, 167 (1977)).

on both ends of the communication, and approximate physical location, among other details.[102]

Moreover, looking back over the Supreme Court's jurisprudence in light of *Jones*, one finds other indications that the Supreme Court has never held as narrow a view of privacy as the lower courts. Instead, as Stephen Henderson wrote last year,[103] the Supreme Court has in fact rejected in several cases the argument that a voluntary disclosure wipes out all privacy interests against the government. For example, *Bond v. United States*[104] was the Supreme Court case in which a majority held that it was a search under the Fourth Amendment for the police to squeeze a person's bag in the overhead rack on a bus.[105] The dissent explicitly cited *Smith v. Maryland* for the proposition that there is no privacy interest in your luggage on the bus because, the dissent said, you have knowingly exposed it to the public.[106] In *Kyllo v. United States*,[107] the government essentially argued that the heat coming from your house was something that you not only exposed to the public, but also discarded as waste.[108] Yet, the Court found in *Kyllo* that monitoring the heat radiating from the house was a search.[109]

I recently looked again at a 1989 case that seems very relevant now: *United States Department of Justice v. Reporters Committee for Freedom of the Press*.[110] It is a Freedom of Information Act ("FOIA") case. A reporter was seeking criminal records from the FBI rap sheet database

102. United States v. Forrester, 512 F.3d 500, 504 (9th Cir. 2008) (pen register collected IP addresses of websites visited and to/from information on e-mails); U.S. DEPT. OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING EVIDENCE IN CRIMINAL INVESTIGATIONS 227–32 (2009) (sample pen-trap application specifying that surveillance is expected to acquire e-mail address information identifying the parties to each communication, the date, time, and duration of each message, the size of each message, and the number and size of any attachments); U.S. DEPT. OF JUSTICE ELECTRONIC SURVEILLANCE MANUAL 39 (2005) (explaining that pen registers can collect IP addresses, port numbers, and e-mail "to" and "from" information); Thomas Lowenthal, *IP Address Can Now Pin Down Your Location to Within a Half Mile*, ARS TECHNICA (Apr. 22, 2011), http://arstechnica.com/tech-policy/2011/04/getting-warmer-an-ip-address-can-map-you-within-half-a-mile/.

103. Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 41–43 (2011).

104. 529 U.S. 334 (2000).

105. *Id.* at 339.

106. *Id.* at 341–43 (Breyer, J., dissenting).

107. 533 U.S. 27 (2001).

108. *Id.* at 35 ("The Government maintains . . . that the thermal imaging must be upheld because it detected 'only heat radiating from the external surface of the house.'" (quoting Brief for the United States at 26, Kyllo v. United States, 533 U.S. 27 (2001) (No. 99-8508), 2000 WL 1890949, at *26)).

109. *Id.* at 40.

110. 489 U.S. 749 (1989).

about a man named Charles Medico, who was suspected of having ties to organized crime. The FBI denied the request under FOIA's privacy exemption.[111] The reporter argued that privacy could not be invoked to deny his request because all arrest records are public.[112] If they are available one by one on the blotter sheets at police stations and in the records of the courts, the reporter argued, then they cannot become private when compiled into one comprehensive record at the FBI.[113]

The Supreme Court rejected the reporter's claim and upheld the government's argument that there is in fact a privacy interest in the compiled records.[114] The Court's language is essentially a rejection of the rationale behind the third-party records doctrine:

> Because events summarized in a rap sheet have been previously disclosed to the public, respondents contend that Medico's privacy interest in avoiding disclosure of a federal compilation of these events approaches zero. We reject respondents' cramped notion of personal privacy.
>
> To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person. In an organized society, there are few facts that are not at one time or another divulged to another. Thus the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private. According to Webster's initial definition, information may be classified as "private" if it is "intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public." Recognition of this attribute of a privacy interest supports the distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole.[115]

There it was, a total refutation of the theory that if you give information to one party for one purpose, you've lost all control over it for any other purpose. Stevens wrote the opinion, which Justices Rehnquist, White, Marshall, O'Connor, Scalia, and Kennedy all joined. Blackmun and Brennan concurred.[116]

So all the time that the lower courts were broadly applying the third-party doctrine and assuming that the privacy interest in a partic-

111. *Id.* at 757.
112. *Id.*
113. *Id.*
114. *Id.* at 762–71.
115. *Id.* at 762–64 (citations omitted).
116. U.S. Dept. of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 750 (1989).

ular piece of information was a binary right that could be lost with a single disclosure to a third party, there was actually a fundamentally different vision of privacy at the Supreme Court, one that was more consistent with the information-based society we live in. Then *Jones* reached the Court, and not a single Justice agreed with the government's claim that there is no privacy interest in information voluntarily disclosed to another.

Personally, what's interesting about this is that in the dialogue leading up to the creation of the DDP coalition, I was the one arguing against taking on the third-party records doctrine. I assumed the doctrine was unassailable. I argued that we should accord transactional data a higher degree of protection only one category at a time, based on the category's unique sensitivity. Following that approach, DDP in effect identified only one category of data entitled to higher protection: location data. In the future, I assumed, there might develop consensus that other categories of data also deserved higher protection, as their significance became apparent.

However, the Justice Department, by resisting legislative reform, and by going all in on the third-party doctrine in *Jones*, has ended up with a decision that fundamentally questions the third-party doctrine—at the very least, for large quantities of transactional data that reveal a person's activities or associations. Suddenly, five Justices seem open to the "mosaic theory," which posits that disparate items of data, each relatively insignificant on its own, become more sensitive as they are compiled in larger quantities to create a picture of a person's life.[117]

Over the coming years, the courts are going to zig and zag over the meaning of the *Jones* decision, but to me *Jones* shows just how modest the DDP proposals are. I see *Jones* as opening up a new era of Fourth Amendment law, in particular, requiring us to go back and look again at the third-party record doctrine. In the meantime, while we explore the implications of *Jones*, I will continue to urge the Justice Department to come to the table and correct the unconstitutionality of ECPA. I urge companies who are not yet members of DDP to join this effort. After *Jones*, it is clear that the issue of government access to electronically generated data, which seemed to be gridlocked by the fear of terrorism and the partisanship in Washington, has suddenly taken on new life.

117. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).