DePaul Law Review

Volume 60
Issue 3 *Spring 2011: Symposium - Trial 2010: A Look Inside Our Nations's Courtrooms*

Article 7

Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information

Joshua J. McIntyre

BALANCING EXPECTATIONS OF ONLINE PRIVACY: WHY INTERNET PROTOCOL (IP) ADDRESSES SHOULD BE PROTECTED AS PERSONALLY IDENTIFIABLE INFORMATION

INTRODUCTION

About the time the Internet age began,[1] the Supreme Court upheld the First Amendment right to distribute anonymous political campaign handbills,[2] lauding anonymous free speech as "a shield from the tyranny of the majority."[3] Within two years, the Court had explicitly applied free speech to the new landscape of cyberspace.[4] The advent of the Internet had brought hope of a new public square for anonymous discourse,[5] a place where anyone with a computer and a phone line could speak openly to the entire world.[6]

Not two decades later, legal reality has dashed that utopian dream. Abuses of the anonymity that the Internet once afforded have required a balancing against other private rights,[7] and no longer is there a reasonable expectation of privacy in many Internet communications.[8] Instead, today's online world lulls its inhabitants into a false

1. *See* Matthew Sag, *Copyright and Copy-Reliant Technology*, 103 Nw. U. L. REV. 1607, 1607 n.1 (2009) (defining the Internet age from 1994 to present).

2. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (striking down an Ohio statute banning the distribution of anonymous handbills). The importance of anonymous speech has long been recognized, chiefly in the political context. *See* Talley v. California, 362 U.S. 60, 64 (1960) ("Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all.").

3. *McIntyre*, 514 U.S. at 357.

4. *See* Reno v. ACLU, 521 U.S. 844, 870 (1997).

5. As one scholar wrote, "[T]he Internet promises to eliminate structural and financial barriers to meaningful public discourse, thereby making public discourse more democratic and inclusive, less subject to the control of powerful speakers, and, at least potentially, richer and more nuanced." Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 894 (2000).

6. *See Reno*, 521 U.S. at 870; Doe v. Cahill, 884 A.2d 451, 456 (Del. 2005) ("Anonymous [I]nternet speech in blogs or chat rooms in some instances can become the modern equivalent of political pamphleteering.").

7. *See* Cahill v. Doe, 879 A.2d 943, 951 (Del. Super. Ct. 2005) (noting that the Internet "presents the real danger that users might abuse the medium by rapidly spreading defamatory information"), *rev'd*, 884 A.2d 451 (Del. 2005). Nevertheless, courts typically afford "greater weight to the value of free speech than to the dangers of its misuse." *McIntyre*, 514 U.S. at 357.

8. Indeed, "[t]he advent of the computer means . . . we have the ability to be more intrusive than ever before." S. REP. NO. 100-599, at 6 (1988). *See also infra* notes 325–50 and accompanying text.

sense of anonymity while secretly recording their every move for future discovery.[9]

This monitoring is made possible by the inherent structure of the Internet, the most crucial component of which is the simply named Internet Protocol (IP).[10] Every computer connected to the Internet receives a unique IP address that facilitates communications with other computers.[11] As part of the normal data exchange, these addresses are recorded, or "log[ged]," by Web servers for future network and security analysis.[12] These logs, however, can also provide a breadcrumb trail of a user's online activity.[13] When a user views a Web site, a computer server logs his IP address.[14] When a user posts on a blog,[15] a server logs his IP address.[16] When a user views a sexually explicit photograph,[17] reads a political article, or searches for "bomb placement white house,"[18] a server logs his IP address.

---

9. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1092 (2002) (noting that the Internet "gives many individuals a false sense of privacy"). This behind-the-scenes monitoring is arguably more dangerous than even the feared telescreen of George Orwell's dystopian *Nineteen Eighty-Four*; at least there, the subjects knew of their surveillance. *See* GEORGE ORWELL, NINETEEN EIGHTY-FOUR, at 3 (Signet Classics 1950) (1949) ("You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."); *see also* Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 291–92 (2001) (comparing Internet surveillance to Jeremy Bentham's Panopticon).

10. Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 549, 554 (1999) (noting the necessity of IP addresses for network functionality).

11. United States v. Steiger, 318 F.3d 1039, 1042 (11th Cir. 2003).

12. *Id.*

13. *See* State v. Reid, 194 A.2d 26, 33 (N.J. 2008) ("With a complete listing of IP addresses, one can track a person's Internet usage."); Berman & Mulligan, *supra* note 10, at 558; Solove, *supra* note 9, at 1145.

14. *See* Oscar H. Gandy, Jr., *Exploring Identity and Identification in Cyberspace*, 14 NOTRE DAME J.L. ETHICS & PUB. POL'Y 1085, 1093 (2000).

15. Short for weblog, a blog is a Web site to which users post comments, hyperlinks, and other general discussion. *Blog*, MERRIAM WEBSTER ONLINE, http://www.merriam-webster.com/dictionary/Blog (last visited Jan. 14, 2011). Blogs have been at the forefront of the Web 2.0 movement in which online users become active participants rather than passive consumers of online material. *See generally* Tim O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, O'REILLY.COM (Sept. 30, 2005), http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=3. Blogs can reveal a wealth of private information and are, therefore, a tremendous privacy concern.

16. *See, e.g.*, Doe v. Cahill, 884 A.2d 451, 454 (Del. 2005) (involving a blog operator who maintained a log of commentators' IP addresses).

17. *See, e.g.*, Gonzales v. Google, Inc., 234 F.R.D. 674, 687 (N.D. Cal. 2006) (expressing concern for the privacy of searches for sexually explicit material).

18. *See id.* (noting that the government may be forced to investigate such a query); *see also* Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV. 1433, 1442 ("Google records all search queries linked to a specific Internet Protocol (IP) address.").

Although these logs are scattered across the vast reaches of the Internet,[19] there are important middlemen with access to it all: Internet Service Providers (ISPs).[20] ISPs assign IP addresses to their subscribers, logging who is using what address at any given time.[21] ISPs are the gatekeepers of access to not only the Internet but also to the identification of any particular user.[22] By comparing its own IP address logs to those maintained by the Internet's Web servers,[23] an ISP can readily link online activity to a specific subscriber account and, potentially,[24] to an individual.[25] This means that ISPs "have the power to obliterate privacy online. Everything we say, hear, read, or do on the Internet first passes through ISP computers."[26]

Herein lies the concern for privacy. Although data logs maintained by Web site operators typically correlate online activity only to an IP address, that address may be traced backwards to expose the individual behind the computer.[27] While various federal statutes protect similar data such as telephone numbers and mailing addresses as Personally Identifiable Information (PII), federal privacy law does not generally regard IP addresses as information worthy of protection.[28] It has, therefore, become commonplace for litigants to subpoena ISPs

19. *See* Gandy, *supra* note 14, at 1093; Helms, *supra* note 9, at 296.

20. *See* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1420.

21. United States v. Steiger, 318 F.3d 1039, 1042 (11th Cir. 2003); *see also In re* Charter Commc'ns, Inc., 393 F.3d 771, 774 (8th Cir. 2005) (noting that only an ISP can link an IP to an individual).

22. *See* Solove, *supra* note 9, at 1143 (stating that the ISP "holds the key" to user anonymity); *see also* Cahill v. Doe, 879 A.2d 943, 955 (Del. Super. Ct. 2005) ("[T]he ISP can readily provide the identity of its subscriber(s). But this does not mean in all instances that it should be compelled to do so."), *rev'd*, 884 A.2d 451 (Del. 2005).

23. Because ISPs also have the ability to record what Web sites their subscribers visit, such comparison may not be necessary in all circumstances. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1233 (1998). If the ISP chooses to maintain IP address logs, it can link a user to his traffic without the aid of the Web site operators or other data aggregators. *See, e.g.*, Klimas v. Comcast Cable Commc'ns, Inc., 465 F.3d 271, 273 (6th Cir. 2006) (involving an ISP that temporarily stored data listing its subscribers' Web site visits).

24. If multiple users access the Internet via the same subscriber account, the IP address will likely identify all of their Internet traffic and will not, therefore, be perfectly linked to any individual user. Frederick Lah, *Are IP Addresses "Personally Identifiable Information"?*, 4 I/S J. L. & POL'Y FOR THE INFO. SOC'Y 681, 700–01 (2008). There may be enough of a link, however, to provide probable cause for a criminal investigation of the account owner. *See infra* notes 205–24 and accompanying text.

25. *See* Helms, *supra* note 9, at 296.

26. Ohm, *supra* note 20, at 1420.

27. *See* Tene, *supra* note 18, at 1450 ("[S]earch-query logs . . . become privacy threatening if they can be traced back to a specific user.").

28. *See* Paige Norian, *The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress Should Respond*, 52 CATH. U. L. REV. 803, 811 (2003) (noting that the "patchwork" nature of federal privacy law left "significant gaps in online privacy").

to unmask online speakers.[29] Many ISPs have no reason to fight these subpoenas[30] and readily give up their subscribers' names, addresses, telephone numbers, and other identifying data without demanding any court oversight or providing any notice to the subscriber.[31] Even when courts become involved, a full consideration of the online speaker's privacy interests is far from certain.[32]

While it would be improper—and dangerous—to provide online actors a blanket of complete anonymity,[33] the routine reporting of information linking individuals to their online activity is a major privacy concern.[34] For now, much of this data collection occurs "without our awareness, much less our approval."[35] As society becomes more aware of this reporting, however, individuals may begin to censor their online conduct for fear of censure or liability, substantially undermining the right to free speech and the free exchange of ideas.[36]

This Comment explores the possibility of protecting the IP address itself as PII,[37] putting the IP address in the same category as a home

29. Shaun B. Spencer, *CyberSLAPP Suits and John Doe Subpoenas: Balancing Anonymity and Accountability in Cyberspace*, 19 J. MARSHALL J. COMPUTER & INFO. L. 493, 493 (2000); *see, e.g.*, State v. Reid, 945 A.2d 26, 29 (N.J. 2008).

30. *See* James X. Dempsey, *Digital Search & Seizure: Standards for Government Access to Communications and Associated Data*, *in* 2 TENTH ANNUAL INSTITUTE ON PRIVACY DATA SECURITY L. 687, 703 (2009).

31. *See* Spencer, *supra* note 29, at 493; *see also* Dempsey, *supra* note 30, at 718 ("If the government obtains from the search engine the IP addresses associated with particular queries, it can compel ISPs to identify those individuals.").

32. *See* Matthew Mazzotta, Note, *Balancing Act: Finding Consensus on Standards for Unmasking Anonymous Internet Speakers*, 51 B.C. L. REV. 833, 855–59 (2010) (examining the emerging discovery standards for unmasking online speakers and noting that "only one standard in the survey requires a court to consider the anonymous speaker's expectation of privacy").

33. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) ("The right to remain anonymous may be abused when it shields fraudulent conduct."); Lidsky, *supra* note 5, at 884 (noting that an anonymous online speaker could "inflict serious harm on [a] corporation" by "pollut[ing] the information stream with defamatory falsehoods, which may in turn influence other investors to question the corporation's credibility or financial health").

34. *See* Kang, *supra* note 23, at 1193 ("The potential for wide-ranging surveillance of all our cyber-activities presents a serious threat to information privacy."); *cf. McIntyre*, 514 U.S. at 355 (stating that the "identification of the author [of a political handbill] against her will is particularly intrusive . . . [because] it reveals unmistakably the content of her thoughts on a controversial issue").

35. Nicholas Carr, *The Great Privacy Debate: Tracking Is an Assault on Liberty, with Real Dangers*, WALL ST. J., Aug. 7–8, 2010, at W1.

36. *See* Cahill v. Doe, 879 A.2d 943, 952 (Del. Super. Ct. 2005) ("[I]f subpoenas can be obtained merely by filing suit, people will be reluctant to speak their mind knowing that their anonymity is tenuous and that retribution for whatever they might say is all the more likely."), *rev'd*, 884 A.2d 451 (Del. 2005); Lidsky, *supra* note 5, at 861 ("Internet defamation actions threaten not only to deter the individual who is sued from speaking out, but also to encourage undue self-censorship among the other John Does who frequent Internet discussion fora.").

37. This is not a novel concept, as some commentators have expressed support for recognizing an IP address as PII. *See, e.g.*, Tene, *supra* note 18, at 1446 ("[E]ven a dynamic address is per-

address, telephone number, or Social Security number and providing it and the corresponding user protection under current federal privacy law. Part II of this Comment outlines the relevant technical aspects of IP addresses[38] and the many definitions and examples of PII.[39] Part III argues that IP addresses are functionally similar to other types of PII and should be protected when in the hands of an ISP or otherwise correlated to identifying information. The argument proceeds by examining what it means for data to be "personally identifiable,"[40] when IP addresses can and cannot be linked to individuals,[41] and how IP addresses are being protected at the state, federal, and international levels.[42] Finally, Part IV examines the predominate subpoena standards by which a litigant may unmask an anonymous online speaker,[43] as well as the current lack of Fourth Amendment protection for subscriber information on file with ISPs,[44] and anticipates how recognizing an IP address as PII may affect these standards and future litigation.[45]

II. BACKGROUND

This Part reviews the basics of IP addresses, including some technical limitations that are later examined—and rejected—as possible barriers to identifying an individual based upon his IP address.[46] It also examines the various definitions of PII[47] and the types of data that are traditionally protected by federal law because they have the potential to identify a particular individual.[48]

A. *IP Addresses and Related Technology*

An IP address is a string of four numbers, each ranging from 0 to 255,[49] that serves as a unique identifier on a network to facilitate on-

sonally identifiable in cyberspace, given the ability of a user's ISP to link such an address to the individual (or company) that used it."); *see also* Helms, *supra* note 9, at 296 ("[O]ne only needs the TCP/IP address and a cooperative ISP to link online activity to a user's biological identity.").

38. *See infra* notes 49–75 and accompanying text.
39. *See infra* notes 76–114 and accompanying text.
40. *See infra* notes 118–30 and accompanying text.
41. *See infra* notes 131–230 and accompanying text.
42. *See infra* notes 231–63 and accompanying text.
43. *See infra* notes 273–324 and accompanying text.
44. *See infra* notes 325–50 and accompanying text.
45. *See infra* notes 351–77 and accompanying text.
46. *See infra* notes 49–75 and accompanying text.
47. *See infra* notes 76–114 and accompanying text.
48. *See infra* notes 82–97 and accompanying text.
49. United States v. Heckenkamp, 482 F.3d 1142, 1144 n.1 (9th Cir. 2007). An example would be 74.125.95.99, which is the IP address assigned to one of the servers hosting http://www.google.com as of this writing.

line communications.[50] An IP address is tied to a computer, not its user,[51] and will normally not change when a new user logs in.[52] In this way, an IP address is analogous to a physical mailing address, which is required for the sending and receiving of postal mail.[53] However, unlike an envelope, which need not contain a return address to convey its message to the recipient, every Internet communication must contain both the sending and receiving IP addresses.[54] Because of the Internet Protocol, users communicate their return addresses to the world whether or not they know of or want this transparency.[55]

Although there are approximately four billion addresses in the current Internet Protocol,[56] many of these are reserved or unassignable,[57] and most of the useable addresses have already been assigned.[58] As a result, methods have been developed to share the limited number of remaining, viable addresses.[59] The two methods relevant here are dynamic addressing and Network Address Translation.

Critical network resources, such as servers and printers, are often given "static," or permanent, addresses so that they are easily found by other devices on the computer network.[60] Most end-user computers, however, are provided a "dynamic" address selected out of a pool and administered by an ISP.[61] An ISP may have more customers than it has assignable addresses, but dynamic addressing allows it to provide an address only to those users connected at any given time.[62] When a user disconnects, his address is put back in the pool and may

50. Klimas v. Comcast Cable Commc'ns, Inc., 465 F.3d 271, 273 (6th Cir. 2006); United States v. Steiger, 318 F.3d 1039, 1042 (11th Cir. 2003).

51. Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *3 n.10 (C.D. Cal. May 29, 2007); *see also* Helms, *supra* note 9, at 296 n.44.

52. *See* Alma Whitten, *Are IP Addresses Personal?*, GOOGLE PUB. POL'Y BLOG (Feb. 22, 2008, 12:31 PM), http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html ("[I]f you share your computer or even just your connection to your ISP with your family, then multiple people are sharing one IP address.").

53. *See* State v. Reid, 945 A.2d 26, 33 (N.J. 2008).

54. *Id.*

55. *See* Gandy, *supra* note 14, at 1093.

56. Kevin Werbach, *The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart*, 42 U.C. DAVIS L. REV. 343, 361 (2008).

57. Due to the structure of IP addressing, certain addresses cannot be used on the Internet. This reduces the assignable address space from the theoretical maximum of more than four billion. *See id.*

58. *See id.*; *see also* Lah, *supra* note 24, at 690.

59. Werbach, *supra* note 56, at 361.

60. *See* Lah, *supra* note 24, at 690.

61. *Id.* at 690–91; Tene, *supra* note 18, at 1446. The protocol that enables dynamic addressing is known as DHCP, which stands for Dynamic Host Configuration Protocol. Lah, *supra* note 24, at 689.

62. State v. Reid, 945 A.2d 26, 28 (N.J. 2008); Cahill v. Doe, 879 A.2d 943, 948 (Del. Super. Ct. 2005), *rev'd*, 884 A.2d 451 (Del. 2005).

later be assigned to a different user.[63] Dynamic addressing allows a large number of computers to share a small number of addresses.

The current Internet Protocol is further modified by a protocol called Network Address Translation, or NAT.[64] NAT allows network administrators to assign a single public IP address to the router or modem that provides the central point of access to the Internet.[65] All of the computers and devices connected to that router are then given a local, private IP address.[66] To the internal network administrator, all of the computers retain separately identifiable IP addresses and can be tracked down with these numbers.[67] To the world, however, hundreds or even thousands of internal computers appear as a single public IP address.[68] No matter which computer accesses a Web site, the Web site will see only the address of the router.[69]

While dynamic addressing and NAT have slowed address exhaustion, the current Internet Protocol is expected to be completely assigned by 2011 or 2012.[70] As a result, the transition to the new Internet Protocol, called IPv6,[71] will soon be accelerated. Unlike current IP addresses, many IPv6 addresses will include a unique code dictated by a computer's hardware, in effect making IPv6 addresses globally unique and permanently assigned to particular devices.[72] IPv6 is unlikely to suffer from the address exhaustion that plagues the current protocol: the new system creates a 128-bit address, providing for approximately 340 undecil-

63. *See* Whitten, *supra* note 52.

64. Helms, *supra* note 9, at 318. For the technical proposal, see Kjeld Borch Egevang & Paul Francis, The IP Network Address Translator (NAT) (Network Working Group, Request for Comments No. 1631) (May 1994), *available at* http://www.ietf.org/rfc/rfc1631.txt.

65. Helms, *supra* note 9, at 318.

66. *See* Jonathan Weinberg, *Hardware-Based ID, Rights Management, and Trusted Systems*, 52 STAN. L. REV. 1251, 1260 n.22 (2000).

67. Because the link is made with reference to a Media Access Control (MAC) address—a physical address that cannot normally be altered—the network administrator may track down an internal computer even if the internal address changes. *See, e.g.*, United States v. Heckenkamp, 482 F.3d 1142, 1144 (9th Cir. 2007) (university's network investigator traced an internal IP address to a specific dorm room and then to a specific user even after the user had altered his internal address).

68. *See* Paul Ham, *Warrantless Search and Seizure of E-Mail and Methods of Panoptical Prophylaxis*, B.C. L. INTELL. PROP. & TECH. F. & J., Sept. 2008, at 1, 14.

69. *See id.*; Helms, *supra* note 9, at 318.

70. Werbach, *supra* note 56, at 361.

71. *Id.* at 361–62.

72. Weinberg, *supra* note 66, at 1260–61; *see also* Helms, *supra* note 9, at 299 (indicating that the uniqueness of IPv6 addresses will "mak[e] it nearly impossible for people to remain anonymous on the Internet").

lion—340,000,000,000,000,000,000,000,000,000,000,000—possible addresses.[73]

Whether the address is from the current or future Internet Protocol, the take-away points are few. An IP address is assigned to a computer or other device accessing the Internet and is communicated between devices as part of the normal data exchange.[74] Some of these devices, especially those that host Web sites, record these numbers for future use.[75]

B. Defining Personally Identifiable Information

Determining what kinds of data should be protected under federal privacy law remains difficult, as there is no single definition of PII.[76] To date, Congress has rejected comprehensive privacy legislation in favor of a large collection of statutes, each of which protects specific types of information in particular circumstances.[77] The Children's Online Privacy Protection Act (COPPA), for example, regulates the online collection of information from children under the age of thirteen[78] but applies only if the Web site is directed to children or the operators have actual knowledge that their visitors are not of age.[79] The Video Privacy Protection Act of 1988 protects the disclosure of a customer's video rental records[80] but may not protect similar records collected online.[81]

These privacy statutes enumerate the data that they are enacted to protect, and these bits of information can be divided into three distinct groups.[82] The first group consists of information that is com-

---

73. *How to Say the IPv6 Number*, eLAMB SECURITY BLOG (Dec. 12, 2006), http://elamb.org/howto-say-the-ipv6-number.

74. *See supra* notes 49–55 and accompanying text.

75. United States v. Steiger, 318 F.3d 1039, 1042 (11th Cir. 2003); State v. Reid, 945 A.2d 26, 29 (N.J. 2008).

76. Lah, *supra* note 24, at 684.

77. *Id.*; Berman & Mulligan, *supra* note 10, at 567; Norian, *supra* note 28, at 811.

78. 15 U.S.C. §§ 6501, 6502 (2006).

79. 15 U.S.C. § 6502(a)(1); Corey A. Ciocchetti, *E-Commerce and Informational Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 75 (2007); Norian, *supra* note 28, at 816–17.

80. 18 U.S.C. § 2710 (2006).

81. In 2008, the Southern District of New York refused to apply the Act when it compelled the production of logs linking YouTube visitors to their viewing records. Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 262 & n.5 (S.D.N.Y. 2008); *see also infra* notes 361–68 and accompanying text.

82. *See* S. REP. NO. 107-240, at 2–3 (2002) ("Taken together, these laws appear designed . . . to ensure that certain types of information collection are fair, transparent, and subject to law.").

monly protected because it can identify a specific individual: names,[83] home addresses,[84] e-mail addresses,[85] telephone numbers,[86] and Social Security numbers.[87] The second group contains data that is easily combined with PII,[88] acts as PII,[89] or is central to the purpose of the enacting statute. This second group includes dates of birth,[90] photographs,[91] video rental records,[92] driver's license numbers,[93] biometric data,[94] and alien registration numbers or other unique identification numbers.[95] In the third group is aggregate data, which is a collection of data that "does not identify particular persons."[96] Aggregate data typically is not viewed as privacy-threatening and is usually excluded from protection.[97]

Some commentators believe this enumerative approach to privacy law fails to protect important pieces of private data.[98] Statutory attempts at defining PII,[99] "personal information,"[100] or "means of identification,"[101] however, have provided little direction in determining

83. Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501(8)(A); False Identification Crime Control Act of 1982, 18 U.S.C. § 1028(d)(7)(A); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2725(3).

84. 15 U.S.C. § 6501(8)(B); 18 U.S.C. § 2725(3).

85. 15 U.S.C. § 6501(8)(C).

86. 15 U.S.C. § 6501(8)(D); 18 U.S.C. § 2725(3).

87. 15 U.S.C. § 6501(8)(E); 18 U.S.C. §§ 1028(d)(7)(A), 2725(3).

88. 15 U.S.C. § 6501(8)(G).

89. 15 U.S.C. § 6501(8)(F) (protecting as personal information "any other identifier that the Commission determines permits the physical or online contacting of a specific individual"). "Online contact information" is further defined as "an e-mail address or another substantially similar identifier that permits direct contact with a person online." § 6501(12).

90. 18 U.S.C. § 1028(d)(7)(A).

91. 18 U.S.C. § 2725(3).

92. Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(a)(3).

93. 18 U.S.C. §§ 1028(d)(7)(A), 2725(3).

94. § 1028(d)(7)(B).

95. § 1028(d)(7)(A).

96. Cable Communication Policy Act of 1984, 47 U.S.C. § 551(a)(2)(A) (2006).

97. *See, e.g.*, *id.*; *see also* 45 C.F.R. § 164.514(a) (2009) ("Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.").

98. *See* Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91, 118 (2009) (noting that the laws "miss a vast amount of data stored by merchants and various businesses"). Others have labeled the mass of statutes a "[c]obweb [f]ull of [h]oles," Tene, *supra* note 18, at 1476, or a "patchwork" with "significant gaps," Norian, *supra* note 28, at 811.

99. *See* 18 U.S.C. § 2710(a)(3); 47 U.S.C. § 551(a)(2)(A).

100. 15 U.S.C. § 6501(8); 18 U.S.C. § 2725(3).

101. 18 U.S.C. § 1028(d)(7).

what other types of information should be protected.[102] COPPA, for example, merely defines personal information as "individually identifiable information about an individual."[103] Likewise, the Stored Communications Privacy Act defines personal information as "information that identifies an individual."[104]

In recent years, Congress has attempted to create new definitions of PII that would specifically address online privacy concerns,[105] but the bills carrying these failed in their respective houses.[106] The Online Personal Privacy Act of 2002 would have largely followed COPPA's definition of PII[107] but would have excluded any information inferred from the data actually collected.[108] The accompanying Senate Report gave an example: if a particular user purchased a book about diabetes from an online retailer, the name, address, and other information provided to assist the delivery of that book would be PII, but the inference that the user has diabetes or a particular interest in diabetes would not be PII.[109]

The Consumer Privacy Protection Act of 2002 would have defined PII as "individually identifiable information relating to a living individual who can be identified from that information."[110] The Act would have excluded from protection any anonymous data, inferred data, or data obtained from public records.[111]

Because of the confusion in what should be protected as personal data, other entities have constructed their own definitions. The Federal Trade Commission (FTC), for example, defined "personal information" in a consent order requiring TJX Companies, the parent company of T.J. Maxx and other discount department stores, to pro-

---

102. Thus, many scholars have used the statutes to craft their own definitions. *See, e.g.*, Tene, *supra* note 18, at 1445 (defining PII as "information which can be used to uniquely identify, contact, or locate a specific individual person").

103. 15 U.S.C. § 6501(8).

104. 18 U.S.C. § 2725(3).

105. *See* Online Personal Privacy Act, S. 2201, 107th Cong. § 401 (2002); Consumer Privacy Protection Act of 2005, H.R. 4678, 107th Cong. § 401 (2002).

106. Ciocchetti, *supra* note 79, at 98–99. For a comparison of the two bills, see Norian, *supra* note 28, at 822–27, 831–35.

107. *Compare* Online Personal Privacy Act, S. 2201 § 401 ("The term 'personally identifiable information' means individually identifiable information about an individual collected online . . . ."), *with* 15 U.S.C. § 6501(8) ("The term 'personal information' means individually identifiable information about an individual collected online . . . .").

108. S. 2201 § 401.

109. S. REP. NO. 107-240, at 40 (2002).

110. H.R. 4678 § 401(4A).

111. *Id.*

tect its customers with reasonable security measures.[112] Among the classic examples of PII identified by the FTC were a person's name, address, telephone number, and Social Security number.[113] The order went further, demanding that TJX protect its customers' e-mail addresses, other online contact information, credit or debit card numbers, and "persistent identifier[s]," "such as a customer number held in a 'cookie.'"[114]

While several new laws at both the federal and state level have begun to recognize the identifying power of IP addresses, most courts continue to refuse to classify them as PII. The remainder of this Comment argues that Congress should adopt—and courts should recognize—a definition of PII that incorporates and protects a user's IP address when it may be linked to that user's identifying information.

III. IP ADDRESSES ACTING AS PERSONALLY IDENTIFIABLE INFORMATION

This Part examines the circumstances in which an IP address should be recognized as PII. Because an IP address is similar in form to other PII and can be used to identify an individual and his online activity, it should be protected as PII when in the hands of an ISP or otherwise correlated to personal information about the user.[115] When an IP address cannot be linked to an individual, such as when it is stored by Web servers without any of the user's contact information, it should not be regarded as personal data.[116] This conclusion is supported by the apparent overall purpose of federal privacy law: to protect data only when it may be linked to a particular individual.[117]

---

112. *In re* The TJX Cos., No. 072 3055, at 2 (F.T.C. Mar. 27, 2008). In that case, an intruder breached TJX's insufficient electronic security measures and stole an estimated ninety-four million customer records, which contained credit card numbers, Social Security numbers, and driver's license numbers. Sprague & Ciocchetti, *supra* note 98, at 97–100. *See also* Martin B. Robins, *Intellectual Property and Information Technology Due Diligence in Mergers and Acquisitions: A More Substantive Approach Needed*, 2008 U. ILL. J.L. TECH. POL'Y 321, 351 n.161 (indicating that the FTC's definition is "often used interchangeably" with statutory definitions of PII).

113. *In re* The TJX Cos., No. 072 3055, at 2 (F.T.C. Mar. 27, 2008).

114. *Id.* A "cookie" is a file stored on the user's hard drive that contains a unique identifying number and other information, such as the user's preferred settings and the previous Web sites he visited. Michelle Z. Hall, *Internet Privacy or Information Piracy: Spinning Lies on the World Wide Web*, 18 N.Y.L. SCH. J. HUM. RTS. 609, 614–15 (2002). Cookies are a privacy concern because they can communicate a wealth of information to Web sites and may do so without the user's consent. *Id.*

115. *See infra* notes 167–230 and accompanying text.

116. *See infra* notes 131–66 and accompanying text.

117. *See infra* notes 118–30 and accompanying text.

A. *PII Is Information That Has the Potential to Identify an Individual*

As examined above, Congress has found it difficult to clearly define PII and the types of data that should be protected.[118] There is an inherent conflict between enumerating bright-line examples of PII and protecting data only when it identifies an individual in practice.[119] In fact, four of the most protected pieces of data need not identify a single person: multiple people may have the same name,[120] multiple residents may share the same home address and telephone number, and multiple users may log in to the same e-mail address.[121] Date of birth, which is listed as a "means of identification" under the False Identification Crime Control Act,[122] is arguably the least tied to a single individual because of the vast number of people who share the same birthday. Of the most commonly listed examples of PII, only a Social Security number appears to be completely tied to one individual.[123] In contrast, biometric data, "such as fingerprint, voice print, retina or iris image,"[124] is probably the most effective type of PII due to its uniqueness but is rarely listed as PII among the statutes.

Taken together,[125] the various definitions and examples of PII suggest that what is meant by "personally identifiable information" is not a piece of data that *always* identifies an individual but a piece of data that *could* identify an individual given the totality of the circum-

118. *See supra* notes 76–111 and accompanying text.

119. *See* Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN/WP136, at 13–15 (June 20, 2007) [hereinafter WP136] (discussing how the ability of particular types of data to identify a person depends upon the circumstances).

120. Brief for Electronic Frontier Foundation as Amicus Curiae Supporting Defendant, Klimas v. Comcast Cable Commc'ns, Inc., (No. 02-CV-72054-DT), at 3–4, *available at* http://w2.eff.org/Privacy/20040408_Klimas_v_Comcast_Amicus_Brief.pdf [hereinafter EFF Amicus Brief].

121. E-mail addresses may be shared, for example, by multiple people in one household (familyname@serviceprovider.com) or by multiple employees who sign in to a generic company account (info@company.com).

122. 18 U.S.C. § 1028(d)(7)(A) (2006).

123. Sprague & Ciocchetti, *supra* note 98, at 93. A Social Security number is, of course, not intrinsically personally identifiable but is rather made so by accurately and consistently recording the link between the number and an individual. *See* Kang, *supra* note 23, at 1208. Thus, even this form of PII is not personally identifiable by itself.

124. 18 U.S.C. § 1028(d)(7).

125. *Compare* 18 U.S.C. § 2725(3) (defining personal information as "information that *identifies* an individual" (emphasis added)), *with* H.R. 4678 § 401, 107th Cong. (2002) (defining PII as "information relating to a living individual who *can be identified* from that information" (emphasis added)). *See also* 45 C.F.R. § 164.514(a) (2009) (excluding from the definition of individually identifiable health information any data to which there is "no reasonable basis to believe that the information *can be used to identify* an individual" (emphasis added)).

stances.[126] When aggregated, even trivial data may help identify a person, making that data collectively worthy of protection.[127]

If this is the proper definition of PII, privacy law should seek to protect any data that could identify an individual, excusing that data from protection only if it is rendered sufficiently anonymous or incapable of identifying an individual in practice.[128] Because it may be impossible to determine, ex ante, whether a particular piece of information will actually identify an individual, precautions must be taken to protect information that is likely to do so.[129] Federal privacy statutes appear to address this concern by providing protection to bits of data—such as name, phone number, and house address—that are widely considered personal even if they do not always point to a specific individual.[130]

This understanding of what it means for information to be "personally identifiable" supports a detailed examination of when IP addresses can and cannot be linked to individuals. As the following Sections explore, an IP address should not be considered personal data by itself, but it may become personally identifiable when correlated to other data about an individual.

---

126. *See* 1-2A Computer Law § 2A.02, at 16 (2009) ("A person can be identified . . . by a combination of significant criteria that permits narrowing down the group to which he or she belongs . . . . Whether an individual is identified depends on the circumstances."); EFF Amicus Brief, *supra* note 120, at 5–8 (distinguishing "personally identifiable" from "personally identifying," the former being *capable* of identifying a person and the later *actually* identifying a person).

127. "What seems nonsensitive in isolation becomes sensitive in aggregation." Kang, *supra* note 23, at 1289 n.370. The danger aggregated data poses to individual privacy is demonstrated by a scandal involving the online video rental service, Netflix. In 2006, as part of a contest to improve its movie recommendation service, Netflix released 100 million records revealing the viewing and rating habits of 500,000 of its users. Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, 2008 IEEE SYMP. ON SECURITY & PRIVACY 111, *available at* http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf. The company had intended to remove all identifying information linking the habits to specific users, but a subsequent study showed that 84% of the users could be re-identified with the released data. *Id.* (concluding that, even if users are not overly concerned about the release of their movie ratings, the disclosure presented privacy concerns because "it is possible to learn sensitive non-public information about a person from his or her movie viewing history").

128. *See* WP136, *supra* note 119, at 15 ("If . . . [the] possibility [to single out an individual] does not exist or is negligible, the person should not be considered as 'identifiable,' and the information would not be considered as 'personal data.'"); *see also* 45 C.F.R. § 164.514 (health privacy rule allowing release of medical information only after it is scrubbed of identifying data); H.R. 5777, 111th Cong. § 501(a)(2) (2010) (online privacy bill excluding from protection any information that has been obscured so as not to identify particular individuals).

129. *See* WP136, *supra* note 119, at 17 (reasoning that an ISP should protect IP addresses as personal data unless it knows "with absolute certainty" that a particular user cannot be identified).

130. *See supra* notes 82–97 and accompanying text.

B. *By Itself, an IP Address Is Not Personal Data*

An IP address cannot identify an individual by itself because it is merely a string of numbers.[131] Instead, it must be correlated to other information about the user, such as addressing logs maintained by ISPs.[132] Privacy law should not, therefore, protect IP addresses when they are not correlated to other PII, such as when they are maintained by Web site operators in normal network traffic logs.

In 2006, the Sixth Circuit Court of Appeals had an opportunity to examine whether an IP address could qualify as PII in the case *Klimas v. Comcast Cable Communications, Inc.*[133] An Internet subscriber alleged that his ISP, Comcast, violated the Cable Communications Policy Act by creating and storing a database linking each user's IP address to the Web sites he visited.[134] The subscriber claimed that Comcast had the ability to correlate this database with its addressing database linking each subscriber to his IP address and could, therefore, associate online activity with the actual identity of its subscribers.[135] The parties agreed that the dispositive issue was whether an IP address could be PII as defined in the Act.[136]

The district court first ruled that dynamic IP addresses, such as those stored in Comcast's database, are not PII because "a dynamic IP address is constantly changing. . . . [U]nless an IP address is correlated to some other information, such as Comcast's log of IP addresses assigned to its subscribers . . . it does not identify any single subscriber by itself."[137] The court granted Comcast's motion to dismiss, reasoning that an IP address could not be PII as defined in the statute absent evidence of actual correlation with the subscriber information.[138]

While ultimately affirming the district court's dismissal of the case, the Sixth Circuit avoided addressing the question of PII by holding that Comcast, as a provider of broadband Internet service, was not an operator of a "cable system" as defined in the Act.[139] The court noted, however, that not all IP addresses are dynamic, and while "IP addresses do not in and of themselves" reveal a subscriber's identity, that information could be "gleaned if a list of individual subscribers is

131. *See supra* notes 49–55 and accompanying text.

132. *See* Klimas v. Comcast Cable Commc'ns, Inc., 465 F.3d 271, 276 n.2 (6th Cir. 2006).

133. *Id.* at 271.

134. *Id.* at 273.

135. *Id.* at 274.

136. Klimas v. Comcast Cable Commc'ns, Inc., No. 02-CV-72054-DT, 2003 U.S. Dist. LEXIS 27765, at *8 (E.D. Mich. July 1, 2003).

137. *Id.* at *10.

138. *Id.* at *10–11.

139. *Klimas*, 465 F.3d at 273.

matched up with a list of their individual IP addresses."[140] The court stated that the collection of data linking a subscriber's IP address to the Web sites he visited could be a proper injury under the Act only if this information was subsequently correlated to subscriber identities.[141] The court pointed to the Act's language that "aggregate data which does not identify particular persons" cannot be PII.[142] Without a correlation between databases, Comcast could not link its subscribers to their online conduct.[143]

While the Sixth Circuit did not have an opportunity to rule whether an IP address is PII within the definition of the Cable Communications Policy Act, the court's language makes clear that under its standard, an IP address *by itself* is not personally identifiable, while an IP address correlated to subscriber information could be PII.

This conclusion is fairly intuitive.[144] An IP address is only a group of four numbers between 0 and 255; the address is not intended to have any special relationship with an individual but is instead dispersed at random from a pool of available addresses maintained by the ISP.[145] Because the address may change whenever the user connects to the Internet, the use of any particular address will be measured in hours, days, or weeks but will not become permanent in most circumstances.[146] Without a correlation to other identifying information, an IP address is only a number and cannot point to the identity of an individual user.[147]

This fact does not, however, support completely excluding IP addresses from the list of personal data. As examined above, most of the data typically regarded as "personally identifiable" has no inherent connection to an individual.[148] A street address does not contain

140. *Id.* at 276 n.2.

141. *Id.* at 276, 280.

142. *Id.* at 280 (quoting 47 U.S.C. § 551(a)(2)(A) (2006)).

143. *Id.*

144. *See* 1-2A Computer Law § 2A.02 n.4 ("An IP address standing alone would merit only the lowest degree of security."); *see also* Whitten, *supra* note 52 ("[T]he IP addresses recorded by every Web site on the planet without additional information should not be considered personal data, because these Web sites usually cannot identify the human beings behind these number strings.").

145. *See supra* notes 61–63 and accompanying text.

146. *See* Lah, *supra* note 24, at 689; Weinberg, *supra* note 66, at 1260 & n.24; *see also* United States v. Vosburgh, 602 F.3d 512, 523 (3d Cir. 2010) ("Comcast's . . . 'lease period' for each IP address is approximately 6–8 days. At the expiration of that lease period, the assignment of an address to a particular computer may or may not be renewed.").

147. *Klimas*, 465 F.3d at 276 n.2.

148. *See* Tene, *supra* note 18, at 1446 (comparing IP addresses to mailing addresses and telephone numbers, which are PII only when they "might be linked to a specific individual through reasonable means").

the name of the person living there. Telephone numbers, Social Security numbers, and driver's license numbers are, like IP addresses, simply numerical sequences.[149] Most of the information protected by federal statute as personally identifiable must be correlated to other data in order to actually identify an individual.[150] IP addresses, therefore, are not unique in their need for correlation to other data to render them protectable PII.[151]

C. *IP Addresses Are Assigned to Computers, Not People*

Some courts have refused to recognize an IP address as PII because the number is assigned to a computer rather than to a particular user. The U.S. District Court for the Central District of California, in ruling on a motion to preserve and produce logs of IP addresses that had been used to download copyrighted music files, noted, "As an IP address identifies a computer, rather than a specific user of a computer, it is not clear that IP addresses . . . are encompassed by the term 'personal information.'"[152] Similarly, the U.S. District Court for the Western District of Washington, faced with an allegation that Microsoft violated its own privacy policy by storing its customers' IP addresses, held that an IP address is not personally identifiable.[153] The court reasoned that, "[i]n order . . . to be personally identifiable, [information] must identify a person. But an IP address identifies a computer, and can do that only after matching the IP address to a list of a particular Internet service provider's subscribers."[154]

These decisions rely too heavily on a colloquial understanding of the words "personally identifiable" without examining the qualities of other PII.[155] It is true that an IP address is assigned to a computer, not a person.[156] This rationale is equally applicable, however, to other types of data that federal statutes nonetheless protect as PII. A house

149. *See* EFF Amicus Brief, *supra* note 120, at 3 ("[W]ithout the equivalent of a reverse telephone directory, a person's telephone number is just a telephone number.").

150. *Id.*

151. *See id.*

152. Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *3 n.10 (C.D. Cal. May 29, 2007). The court examined the question under the defendant's privacy policy rather than a federal statute. *Id.* Problematically, the defendant did not provide the court with a definition of the term "personal information" as used in its policy. *Id.*

153. Johnson v. Microsoft Corp., No. C06-0900RAJ, 2009 U.S. Dist. LEXIS 58174, at *13 (W.D. Wash. June 23, 2009).

154. *Id.* at *12–13.

155. *See supra* notes 82–97 and accompanying text.

156. *See Bunnell*, 2007 WL 2080419, at *3 n.10; Helms, *supra* note 9, at 296 n.46.

address, for example, is assigned to a building, not a person.[157] A telephone number is assigned to a telephone line, not a person.[158] An e-mail address identifies an electronic mailbox stored on a computer hard drive, and a date of birth identifies a specific day in history.

These types of information may be personally identifiable in some circumstances but not in others.[159] If only one person lived at a particular house address or had access to a specific telephone, the address and telephone number would be directly linked to that person. It would be reasonable, for example, to attribute calls made from a particular cell phone number to the individual who carries the phone every day. Attributing a call to a particular individual may not be fair, however, if many people have ready access to the phone.[160]

Whether or not these pieces of data identify an individual on their own, they often can identify an individual when aggregated.[161] As one study found, combining a gender, a birthdate, and a ZIP code is enough to uniquely identify 87% of the United States population.[162] It is prudent, therefore, to provide more protection to compilations of data than that afforded individual bits of information.[163]

IP addresses present the same possibilities: they may be closely linked with a particular person and may become personally identifiable when combined with other PII.[164] When an IP address can be associated with a particular computer to which one person or a small number of persons has access, the IP address becomes more akin to

---

157. Therefore, an address may not be personally identifiable in some circumstances, such as when it identifies an apartment building but not the particular apartment. *See* Tene, *supra* note 18, at 1446.

158. When a telephone is available for use by more than one person, the calls made from the telephone are less likely to be fairly attributable to an individual. *See* Nancy J. King, *When Mobile Phones Are RFID—Equipped: Finding E.U.-U.S. Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce*, 15 MICH. TELECOMM. & TECH. L. REV. 107, 181 n.287 (2008).

159. *See* WP136, *supra* note 119, at 13 ("[T]he question of whether the individual to whom the information relates is identified or not depends on the circumstances of the case.").

160. *See* King, *supra* note 158, at 181 n.287.

161. *See* Sprague & Ciocchetti, *supra* note 98, at 93.

162. Latanya Sweeney, *Computational Disclosure Control: A Primer on Data Privacy Protection* 20 (Jan. 8, 2001), *available at* http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/sweeney-thesis-draft.pdf; *see also* Seth Schoen, *What Information Is "Personally Identifiable"?*, ELECTRONIC FRONTIER FOUNDATION (Sept. 11, 2009), http://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable; Kang, *supra* note 23, at 1289 n.370 ("[T]he true privacy threat arises from the systematic, detailed aggregation of otherwise trivial data that allows the construction of a telling personal profile.").

163. *See* Ciocchetti, *supra* note 79, at 56.

164. *Compare* Gandy, *supra* note 14, at 1093 ("[I]t is in the nature of the Internet Protocol (IP) that personally identifiable information is made available for capture in every interaction between computers."), *with* King, *supra* note 158, at 181 ("[C]ertain types of IP addresses that do not allow identification of the user may not be personal data.").

traditional PII.[165] Unlike other PII, the IP address can go beyond identification and actually associate a person with the content of his online activity.[166]

D. An IP Address Can Identify an Individual and His Online Activity

Three primary concerns may lead a court to question whether an IP address can constitute personally identifiable information. First, most computers use a dynamic IP address that, by definition, can change.[167] A court may ask how an IP address can be PII when it may be assigned to multiple subscribers in any given timeframe.[168] Second, the Network Address Translation protocol may operate to provide many computers with a single external IP address, restricting the ability to track online conduct to a particular computer or user.[169] Third, even if an IP address were tethered to a single computer,[170] the online conduct may have been initiated by any person who had access to that computer and might not, therefore, be fairly attributable to any individual.[171]

Courts that have faced these circumstances have had no problem utilizing IP addresses to attribute online conduct to particular persons. The following Sections examine why these technical aspects of IP addressing should not prevent the proper conclusion that IP addresses may be PII.

1. Dynamic IP Addresses Can Be Traced Back to an Individual

While most computers utilize dynamic IP addresses assigned to them by an ISP, ISPs commonly log these assignments.[172] When provided with a particular date and time of interest, an ISP can often determine to which subscriber account a particular IP address was assigned.[173] Because ISPs retain these logs for only a limited amount of time, the crucial factor in this process is the timeliness of the request

165. *See* EFF Amicus Brief, *supra* note 120, at 9.

166. *See* Berman & Mulligan, *supra* note 10, at 554 (noting online transactional data, such as IP address and Web site history, can "reveal the blueprint of an individual's life").

167. *See supra* notes 60–63 and accompanying text.

168. *See, e.g.*, Klimas v. Comcast Cable Commc'ns, Inc., No. 02-CV-72054-DT, 2003 U.S. Dist. LEXIS 27765, at *10 (E.D. Mich. July 1, 2003).

169. *See supra* notes 64–68 and accompanying text.

170. An IP address is tied to a specific computer when the computer uses a static, public IP address. Lah, *supra* note 24, at 690.

171. *See infra* notes 205–24 and accompanying text.

172. United States v. Steiger, 318 F.3d 1039, 1042 (11th Cir. 2003).

173. *See* Klimas v. Comcast Cable Commc'ns, Inc., 465 F.3d 271, 273 (6th Cir. 2006); United States v. Kennedy, 81 F. Supp. 2d 1103, 1108 (D. Kan. 2000).

for identification.[174] Nevertheless, most ISPs reassign the same address to a subscriber every time he logs on to the network.[175] Even with dynamic addressing, a computer may retain a single IP address assignment for months at a time.[176] In practice, then, even dynamic IP addresses can be associated with particular individuals.[177]

In the 2010 case *United States v. Vosburgh*,[178] the Third Circuit Court of Appeals examined the process by which an ISP links an IP address back to a particular subscriber. There, an undercover FBI agent posted a dummy Web link advertising child pornography.[179] When the defendant clicked on the link, his IP address was recorded into a log file on the agent's computer.[180] In reviewing the trial testimony provided by the defendant's ISP, Comcast, the Third Circuit explained how the defendant was linked to his IP address.[181]

> A witness from Comcast . . . explained that Comcast can trace an IP address back to a particular customer's account, through IP assignment logs that go back 180 days. Finally, he testified that between October 20 and October 30 of 2006, IP address 69.136.100.151 was assigned to an account registered to [the defendant].[182]

Identifying a defendant through IP addressing logs is often a crucial step in criminal cases arising from online activity. In *United States v. Steiger*, for example, an anonymous source provided a police department with evidence of child pornography originating from three dynamic IP addresses.[183] The police department notified the FBI, which issued a subpoena to the ISP that had assigned the addresses.[184] The ISP reviewed its logs, determined that all three addresses had been used by the defendant, and provided the FBI with the defendant's

174. *See, e.g.*, United States v. Vosburgh, 602 F.3d 512, 523 (3d Cir. 2010) (noting that the defendant's ISP maintained IP assignment logs for 180 days). Note, however, that the FBI is currently pressuring ISPs to retain assignment logs for as long as two years. Declan McCullagh, *FBI Wants Records Kept of Web Sites Visted*, CNET NEWS (Feb. 5, 2010, 9:16 AM), http://news.cnet.com/8301-13578_3-10448060-38.html.

175. Weinberg, *supra* note 66, at 1260 n.24.

176. *Id.*

177. Tene, *supra* note 18, at 1446.

178. United States v. Vosburgh, 602 F.3d 512, 523 (3d Cir. 2010).

179. *Id.* at 517.

180. *Id.*

181. *Id.* at 523.

182. *Id.*

183. United States v. Steiger, 318 F.3d 1039, 1042 (11th Cir. 2003).

184. *Id.*

name and home address.[185] The defendant was indicted and convicted of various child pornography charges.[186]

Identifying an online actor through ISP logs is not limited to criminal cases. In *In re Charter Communications, Inc.*, more than two hundred file-sharers were personally identified by their dynamic IP addresses.[187] The Recording Industry Association of America (RIAA) used tracking software to discover the IP addresses assigned to ninety-three Charter subscribers who were suspected of downloading and distributing copyrighted music.[188] The RIAA obtained subpoenas from the district court clerk requiring Charter to release the names, addresses, and e-mail addresses of the subscribers.[189] Charter opposed the subpoena, but its motion to quash was denied and the district court ordered production of the information.[190] Charter subsequently released the names and addresses of 150 subscribers who had been notified of the subpoenas and another 50 to 70 who had not received notice.[191] The Eighth Circuit Court of Appeals later vacated the order, reasoning that it had been improperly issued under § 512(h) of the Digital Millennium Copyright Act.[192] The court ordered the RIAA to return the data without making any record or any further use of the subscribers' personal information.[193]

2. *An IP Address Can Identify an Individual Even on a Private Network*

The commonplace use of Network Address Translation may be seen as a barrier to identifying an individual with an IP address.[194] With NAT, each computer on an internal network uses a "private" IP address, while the entire network shares a "public" IP address.[195] This means that external Web servers will log the one public IP address no matter which private computer initiated the connection. However, data logs maintained in the normal course of business will often allow the private network manager to trace specific transmissions and online

185. *Id.*
186. *Id.* at 1043, 1045.
187. *See In re* Charter Commc'ns, Inc., 393 F.3d 771 (8th Cir. 2005).
188. *Id.* at 774.
189. *Id.*
190. *Id.*
191. *Id.* The opinion does not explain the discrepancy between the number of subscribers originally identified by Charter and the number subpoenaed. *See id.*
192. *Id.* at 777.
193. *Id.* at 778.
194. *See* Weinberg, *supra* note 66, at 1260 n.22 ("The extent to which . . . traffic can be traced to [a user behind NAT] . . . depends on the information retained by that server.").
195. *See* Egevang & Francis, *supra* note 64, at 1.

activity to a single internal address in much the same way that an ISP traces communications on its network to a single subscriber account.[196] As a result, the NAT protocol does not prevent the identification of a user when the network manager cooperates with attempts to track down the source of online activity.[197]

The 2007 case *United States v. Heckenkamp* provides an example.[198] Qualcomm Corporation's computer administrator discovered that the company's computer systems had been accessed without authorization.[199] Through a reverse lookup procedure, the administrator determined that the hacker's public IP address had been assigned to the University of Wisconsin.[200] The administrator contacted the university's network investigator, who discovered that the hacker had utilized a computer with a private IP address ending in "117."[201] By cross-referencing the private IP address on multiple university servers, the investigator discovered that the address had recently been assigned to the defendant, an on-campus student.[202] After the investigator physically inspected the defendant's computer to confirm his findings, the FBI obtained a search warrant to seize the computer.[203] The defendant was indicted on multiple counts of recklessly causing damage through unauthorized access to a computer system in violation of federal law.[204]

3. *An IP Address Can Provide Probable Cause to Suspect an Individual of Online Activity*

The two preceding arguments do not represent any real limitation on the ability of an IP address to identify an individual, provided that the appropriate addressing logs are available. The third concern, however, is not easily dismissed: there may, in fact, be no way to definitively link a particular person with the online conduct emanating from a particular computer or IP address.[205] A user may, for example, access online content without ever providing identifying credentials.[206] If many people use a single computer, it would be difficult to attribute

196. *See* United States v. Heckenkamp, 482 F.3d 1142, 1148 (9th Cir. 2007).
197. *See* Weinberg, *supra* note 66, at 1260 n.22.
198. *See generally Heckenkamp*, 482 F.3d at 1142.
199. *Id.* at 1143.
200. *Id.*
201. *Id.* at 1144.
202. *Id.*
203. *Id.* at 1145.
204. *Id.*
205. *See* WP136, *supra* note 119, at 17 (presenting the scenario of an anonymous user of a computer in an Internet cafe).
206. *See* King, *supra* note 158, at 181; *see also* WP136, *supra* note 119, at 17.

online conduct to any one of them based solely on that computer's IP address.[207]

This dilemma may be avoided by requiring some authentication at the computer terminal.[208] When a user signs in to a personal account by entering a username and password, the authentication process is logged by either the local computer or the network servers.[209] By cross-referencing the IP logs with the user authentication logs, a network administrator can identify what user account was signed in at the time of some questionable online activity.[210] Absent photographs or video of the person sitting at the computer at the time in question, a user authentication log is likely to provide the strongest evidence of who actually accessed the online material.

Even without an authentication log, however, the link between an IP address and the Internet subscriber may provide enough circumstantial evidence to suspect a particular individual of some litigious or criminal online activity.[211] Since 2000, the Third, Fifth, Sixth, Eighth, Ninth, and Tenth Circuit Courts of Appeals have all held that a search warrant is supported by probable cause when it uses an IP address and an ISP logging database to identify a defendant.[212]

In the 2007 case *United States v. Perez*,[213] for example, the FBI subpoenaed an ISP to obtain the name and home address of a subscriber whose IP address had recently been used to post child pornography.[214] Upon executing a search warrant on the subscriber's address, the FBI discovered that three people resided in the house, each maintaining a separate "occupancy unit."[215] The defendant argued that the occupancy by two other persons and the wires running into each bedroom

207. This scenario would be identical to that of the office telephone to which multiple people have easy access. *See* King, *supra* note 158, at 181 n.287.

208. Kang, *supra* note 23, at 1226; *see also* CHRISTOPHER KUNER, EUROPEAN DATA PRIVACY LAW & ONLINE BUSINESS 50 (2003).

209. KUNER, *supra* note 208, at 50.

210. *Id.*

211. *See* United States v. Kennedy, 81 F. Supp. 2d 1103, 1107, 1114 (D. Kan. 2000) (finding the defendant's admission that he was the primary user of an Internet account provided probable cause for a search of his computer).

212. United States v. Vosburgh, 602 F.3d 512, 526 (3d Cir. 2010) (noting that "several Courts of Appeals have held that evidence that the user of a computer employing a particular IP address possessed or transmitted child pornography can support a search warrant for the physical premises linked to that IP address"); United States v. Stults, 575 F.3d 834, 844 (8th Cir. 2009); United States v. Perrine, 518 F.3d 1196, 1199–1200, 1206 (10th Cir. 2008); United States v. Perez, 484 F.3d 735, 740 (5th Cir. 2007); United States v. Wagers, 452 F.3d 534, 539 (6th Cir. 2006); United States v. Hay, 231 F.3d 630, 635–36 (9th Cir. 2000).

213. *Perez*, 484 F.3d at 735.

214. *Id.* at 738.

215. *Id.* at 738, 741.

should have alerted the officers to the possibility that one of the other housemates had been responsible for the online conduct.[216] On appeal, however, the Fifth Circuit held that the officers had probable cause to search the defendant's premises, reasoning that the Internet account had been registered in the defendant's name, which created a "fair probability" that the defendant was responsible for the online conduct.[217] The court noted that, although "it was possible that the transmissions originated outside of the residence to which the IP address was assigned, it remained *likely* that the source of the transmissions was inside that residence."[218]

In *United States v. Kennedy*,[219] the FBI obtained a court order directing disclosure of the subscriber information related to an IP address assigned to a computer allegedly containing child pornography.[220] The Internet account was registered in a woman's name but also listed an e-mail address for a man.[221] Upon questioning the man, the FBI determined that he was the primary user of the Internet service.[222] This admission, along with other supporting facts obtained during the questioning,[223] provided probable cause to search the defendant.[224]

As the above cases demonstrate, an Internet user can often be identified by the IP address assigned to his computer despite the alleged technical barriers.[225] An IP address, then, must be PII when in the hands of an ISP or another entity that can make the correlation between the address and the individual.[226] The reservations that some courts have about recognizing an IP address as PII likely stem from the fact that only an ISP can consistently correlate an IP address to a subscriber account.[227] When the IP address is collected by entities

216. *Id.* at 742.

217. *Id.* at 744.

218. *Id.* at 740 (emphasis added).

219. United States v. Kennedy, 81 F. Supp. 2d 1103 (D. Kan. 2000).

220. *Id.* at 1106–07.

221. *Id.*

222. *Id.* at 1107–08.

223. The FBI also determined that the defendant liked to download pictures from the Internet and was suspicious that others were reading his computer files. *Id.* at 1107. This information was obtained in a pretextual phone call in which the FBI agent pretended to be a representative of the defendant's ISP. *Id.* at 1114.

224. *Id.*

225. For a useful visual representation of the technical process used to trace IP address assignments, see Helms, *supra* note 9, at 296.

226. *See* Aoife White, *IP Addresses Are Personal Data, E.U. Regulator Says*, WASH. POST, Jan. 22, 2008, at D1 (paraphrasing Germany's data-protection commissioner as saying "when someone is identified by an IP . . . address, 'then it has to be regarded as personal data'").

227. *See In re* Charter Commc'ns, Inc., 393 F.3d 771, 774 (8th Cir. 2005).

other than the ISP, the address must be specifically correlated with other personal data in order to identify an individual user.[228] If Web sites do not collect other PII, or do not correlate other PII to IP addresses, the Web site owners cannot trace the IP address back to an individual.[229] Regulating the use of IP addresses by these entities would restrict their legitimate business operations without providing a significant counterbalancing benefit to user privacy.

This is a clear distinction, and one that may be used to establish legal rules protecting a user's IP address only when it may act as personal data. In addition, rules protecting IP addresses only when they are in the hands of an ISP or are correlated to other PII would fit within the federal framework of privacy law, which protects data only when the specific circumstances threaten individual privacy.[230]

E. The Movement to Protect IP Addresses

Despite the skepticism, there is a growing movement recognizing the identifying power of IP addresses. For one, a number of states have adopted definitions of PII affording protection to IP address information and the individual behind the computer.[231] In Indiana, for example, a criminal procedure law protects information that identifies a victim of domestic violence, dating violence, sexual assault, or stalking.[232] The list of protected information includes the victim's name, address, telephone number, and IP address.[233] Likewise, a Connecticut law lists IP addresses among the "basic subscriber information" that may be obtained during a criminal investigation of a registered sex offender only upon judicial order.[234]

Minnesota's "Internet Privacy" statute is the first state law to explicitly regulate an ISP's disclosure of its subscribers' personal information and browsing habits.[235] The statute defines PII to include any

228. *See supra* notes 140–50 and accompanying text.

229. *See* Klimas v. Comcast Cable Commc'ns, Inc., No. 02-CV-72054-DT, 2003 U.S. Dist. LEXIS 27765, at *10 (E.D. Mich. July 1, 2003) ("[U]nless an IP address is correlated to some other information . . . it does not identify any single subscriber by itself.").

230. *See supra* notes 77–81 and accompanying text (discussing the limited scope of federal privacy law).

231. *See* CONN. GEN. STAT. § 54-260b (2009); IND. CODE § 35-37-6-2.5 (1998); MINN. STAT. § 325M.01-09 (2004); MONT. CODE ANN. § 2-17-551 (2009); WIS. STAT. § 19.68 (2003).

232. IND. CODE § 35-37-6-2.5.

233. IND. CODE § 35-37-6-2.5(a).

234. CONN. GEN. STAT. § 54-260b (2009).

235. MINN. STAT. § 325M.02–04; *see also* Jordan M. Blanke, *Minnesota Passes the Nation's First Internet Privacy Law*, 29 RUTGERS COMPUTER & TECH. L.J. 405, 405, 413 (2003). The statute also protects "clickstream data," data that indicates where a user has been and how he found the current Web site. Blanke, *supra*, at 408–09 & n.18.

information that (1) identifies a subscriber by "physical *or electronic address* or telephone number"; (2) discloses the subscriber's Web site visits or requested materials; or (3) contains any of the contents of the subscriber's data-storage devices.[236] ISPs are prohibited from releasing this information except in limited circumstances.[237] However, because those circumstances include the issuance of a standard subpoena, warrant, or court order,[238] the actual level of protection afforded will continue to depend upon courts' willingness to allow the identification of online speakers.

The new federal Health Insurance Portability and Accountability Act (HIPAA) privacy rule explicitly protects IP addresses.[239] The regulation allows health providers to release patient information only after it is scrubbed of all "individually identifiable . . . information."[240] Data that must be removed includes most of the commonly recognized forms of PII, including telephone numbers, Social Security numbers, and biometric data.[241] The regulation adds IP addresses to this list.[242]

In July of 2010, U.S. Representative Bobby Rush introduced an online privacy bill to the House Committee on Energy and Commerce that would protect IP address information when it is used to build an online profile for behavioral advertising.[243] In addition to traditional forms of PII, the Best Practices Act would protect

> any unique persistent identifier, such as a customer number, unique pseudonym or user alias, IP address, or other unique identifier, where such identifier is used to collect, store or identify information about a specific individual or to create or maintain a preference profile.[244]

---

236. MINN. STAT. § 325M.01 (emphasis added).

237. *See* MINN. STAT. § 325M.02.

238. MINN. STAT. § 325M.03(6), (7).

239. 45 C.F.R. § 164.514(b)(2)(i)(O) (2009).

240. 45 C.F.R. § 164.514(b).

241. *Id.*

242. *Id.* § 164.514(b)(2)(i)(O).

243. H.R. 5777, 111th Cong. (2010). Behavioral advertising, also known as behavioral targeting, "is a method of tracking the online behavior of Internet users in order to serve those consumers with advertising targeted to the specific interests 'expressed' through Web-browsing activity." Andrew Hotaling, *Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting*, 16 COMMLAW CONSPECTUS 529, 530 (2008). Behavioral advertising is a controversial practice because of the challenge to expectations of privacy online. *Id.*

244. H.R. 5777 § 2(4)(vii).

The Act, which builds upon a May 2010 proposal drafted by U.S. Representatives Rick Boucher and Cliff Stearns,[245] would require any "covered entity"[246] that collects such information to provide notice of collection practices and provide users an opportunity to opt out of data collection.[247] Disclosure of the protected information to third parties would require the individual's express consent,[248] except in cases of prior consent, fraud detection, imminent danger, publicly available information, or compliance with law—such as a statute, subpoena, or summons.[249]

Notably, the Act would not require covered entities to allow users to opt out when data collection is required for an "operational purpose."[250] This exception would likely allow ISPs and Web site operators to continue to use and maintain IP address information necessary to deliver Internet services.[251] Consistent with the position taken in this Comment, the exception implicitly recognizes that IP addresses are necessary for the operation of Internet services and should only be protected as personal data when correlated to other identifying information.[252]

Abroad, the European Union Data Protection Working Party found in 2008 that IP addresses should be protected as "personal data."[253] As the Working Party concluded,

> An individual's search history is personal data if the individual to which it relates, is identifiable. Though IP addresses in most cases are not directly identifiable by search engines, identification can be achieved by a third party. Internet access providers hold IP address

245. *US Lawmakers Publish Internet Privacy Bill*, THE REGISTER (May 6, 2010, 8:13 AM), http://www.theregister.co.uk/2010/05/06/internet_privacy_bill/.

246. "Covered entity" is defined as "a person engaged in interstate commerce that collects or stores data containing covered information or sensitive information," except for government entities and any person who (i) stores information from fewer than 15,000 individuals, (ii) collects information from fewer than 10,000 persons in a twelve-month period, (iii) does not collect sensitive information, and (iv) does not use the information to study individuals as its primary business. H.R. 5777 § 2(3).

247. *Id.* §§ 101–103.

248. *Id.* § 104(a)(1).

249. *Id.* § 106.

250. *Id.* § 103(e).

251. *See id.* § 2(5)(A) (defining "operational purpose" in part as "a purpose reasonably necessary to facilitate . . . the logistical or technical ability of a covered entity to provide goods or services").

252. *See id.* § 2(5)(B) (defining "operational purpose" to exclude information used for a marketing or advertising purpose or any purpose that "would likely affect the individual's conduct or decisions with respect to the covered entity's products or services").

253. Article 29 Data Protection Working Party, Opinion 1/2008 on Data Protection Issues Related to Search Engines, 00737/EN/WP148, at 3, 8 (Apr. 4, 2008) [hereinafter WP148]. For a more detailed analysis of the EU's approach, see Lah, *supra* note 24, at 695–99.

> data. Law enforcement and national security authorities can gain access to these data and in some Member States private parties have gained access also through civil litigation. Thus, in most cases—including cases with dynamic IP address allocation—the necessary data will be available to identify the user(s) of the IP address.[254]

The Working Party went beyond regulation of ISPs, imposing limitations on Web site operators who use and maintain IP address information whenever the addresses are correlated with other personal information.[255]

The High Court of Ireland reached an opinion consistent with the position proposed in this Comment in its 2010 decision, *EMI Records Limited v. Eircom Limited*.[256] EMI and other copyright owners sued Eircom, an ISP, for the peer-to-peer file sharing of copyrighted material conducted on Eircom's network.[257] The parties settled, developing a protocol by which EMI would inform Eircom of the IP addresses used to download its copyrighted material, and Eircom would warn, and possibly disconnect service to, the associated subscribers.[258] In examining the lawfulness of the settlement terms, the High Court asked whether IP addresses, in the hands of EMI and its agents, constituted "personal data" under the Data Protection Act.[259] Unlike the laws of the United States, the Act provided significant direction by defining personal data as "[d]ata relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller."[260]

Examining the specifics of the settlement protocol, the High Court concluded that IP addresses *in the hands of EMI or its agents* could not qualify as personal data.[261] The court reasoned that

> none of the plaintiffs have any interest in personally identifying any living person who is infringing their copyright by means of the settlement and protocol. . . . [T]here seems no legal avenue open to them to get that information apart from an application for the names and addresses of the copyright thieves to the internet service provider.[262]

---

254. WP148, *supra* note 253, at 8.

255. *Id.* at 19–21. *See* Lah, *supra* note 24, at 696.

256. EMI Records Ltd. v. Eircom Ltd., [2010] I.E.H.C. 108 (Ire.).

257. *Id.* ¶ 1.

258. *Id.* ¶¶ 2, 9.

259. *Id.* ¶ 16.

260. *Id.* ¶ 19. Note that this definition protects both data that actually identify an individual and data that could identify an individual if correlated to other data in the party's possession.

261. *Id.* ¶ 25.

262. *Id.*

This conclusion is consistent with the above argument that an IP address is personally identifiable only when correlated to other personal data, such as when in the hands of an ISP. During execution of the settlement protocol, EMI would know only the IP address of a user suspected of copyright infringement and would have no means by which to link that information to particular persons.[263] The court correctly concluded that IP addresses should not be protected as personal data in such circumstances. The court did not, however, have occasion to question whether the IP address information should be protected when in the hands of Eircom itself.

The next Part examines the possible practical results of this movement to classify IP addresses as PII. It examines how IP addresses could be incorporated into the federal statutory framework,[264] how doing so may affect the current subpoena standards by which a private litigant may unmask an anonymous online speaker,[265] and how online actors' expectations of privacy in online communications may be affected.[266]

IV. IMPACT

Both the feasibility and the effect of incorporating protections for IP addresses into current privacy law would depend upon the statutory scheme at issue.[267] Some statutes provide a catch-all clause allowing courts to afford protections to unspecified—but nonetheless private—information.[268] If an IP address falls within these catch-all clauses because it can identify a particular person, then the release of such an IP address and the associated subscriber information held by an ISP would be subject to the particular statute's subpoena standards.

Other statutes, however, leave no room for new types of PII or do not set specific standards by which a litigant can subpoena the release of the information protected. In cases brought under those statutes, courts must balance the litigants' competing interests in the production of the information. When IP address information is at issue, courts would be better able to balance these interests if they explicitly

263. *Id.* ¶ 12.

264. *See infra* notes 351–68 and accompanying text.

265. *See infra* notes 369–75 and accompanying text.

266. *See infra* notes 331–74 and accompanying text.

267. *See infra* notes 276–87 and accompanying text.

268. *See, e.g.*, 15 U.S.C. § 6501(8)(F) (2006) (protecting "any other identifier that the Commission determines permits the physical or online contacting of a specific individual").

recognized the personal nature of the IP address and its ability to link an individual to his online conduct.

In addition, classifying IP addresses as PII would support reexamining Fourth Amendment law as applied to basic subscriber information.[269] Current law holds that, under the third party doctrine, Internet subscribers do not have a reasonable expectation of privacy in this information because they have voluntarily exposed it to their ISPs.[270] Protecting an IP address as personal information, however, would support providing stronger protections to the data linking online content to particular subscribers, especially when Internet users must release this information in order to obtain Internet service.[271]

The following Sections briefly examine the myriad of subpoena standards applicable when unmasking online speakers[272] and the current Fourth Amendment law as applied to basic subscriber information before imagining how these may change when IP addresses are considered personal information.

A. Subpoena Standards for Unmasking Online Defendants

The thin veil of anonymity that the Internet provides often requires that a litigant seeking redress from actions conducted online initially file his complaint against an unnamed party, the Doe defendant.[273] The plaintiff will then seek a subpoena or court order requiring the appropriate third party to expose the Doe defendant's true identity.[274] The statute providing protection to the personal information at issue may stipulate the appropriate subpoena standard.[275] If the plaintiff obtains a subpoena pursuant to a statutory provision, the Doe defendant may not have a viable method by which to avoid his identification.[276]

Some statutory standards strongly favor the plaintiff's interest in identifying a defendant. The Digital Millennium Copyright Act (DMCA), for example, expressly allows copyright owners to subpoena

269. *See infra* notes 325–50 and accompanying text.

270. *See, e.g.*, United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (holding that an Internet user did not have an objectively reasonable expectation of privacy in the information on file with his ISP, including his name, e-mail address, telephone number, and physical address).

271. *See* State v. Reid, 195 A.2d 26, 33 (N.J. 2008).

272. *See infra* notes 273–322 and accompanying text.

273. *See* Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 577–78 (N.D. Cal. 1999).

274. Spencer, *supra* note 29, at 495. *See, e.g.*, Doe v. Cahill, 884 A.2d 451, 455 (Del. 2005); Solers, Inc. v. Doe, 977 A.2d 941, 944 (D.C. Cir. 2009).

275. *See, e.g.*, 18 U.S.C. § 2710(b)(2)(F) (2006) (requiring a showing of "compelling need" before a subpoena may issue).

276. *See* Spencer, *supra* note 29, at 493.

ISPs for the identification of alleged infringers.[277] If the plaintiff submits a subpoena request having the required form and content, the district court clerk is instructed to "expeditiously issue" the subpoena.[278] The ISP, upon its receipt of the subpoena, must "expeditiously disclose" the information requested.[279] While the circumstances in which the DMCA authorizes disclosure are limited,[280] exposing a Doe defendant can be fairly automatic and quickly accomplished under the DMCA standard.

Other statutes provide more protection to the defendant's personal information. The Video Privacy Protection Act, for example, requires that a party seeking a court order to expose video rental records make a showing of "compelling need" and provide the consumer with reasonable notice and an opportunity to contest the disclosure.[281] The plaintiff may obtain an individual's name and address only if that person is given an opportunity to prevent the disclosure.[282] Likewise, the Cable Communications Policy Act requires that an individual be notified of a court order authorizing the disclosure of his PII to a private entity.[283] If the information is to be disclosed to a government entity, there must be clear and convincing evidence that the individual is suspected of a crime and that the information sought will be material to the case; the individual must also be given the opportunity to appear and contest the claim.[284]

Finally, some statutes provide strong protections to individuals in only limited circumstances. The Stored Communications Act, for example, requires a warrant or court order before a stored electronic communication or PII is released to a government entity.[285] A court order is obtainable only upon specific and articulable facts supporting a reasonable belief that the information is relevant and material to an ongoing criminal investigation.[286] Because the Act is concerned only with governmental invasions of privacy, however, it provides no protection when a private entity seeks the release of customer records: the statute explicitly authorizes the release of customer records or

277. 17 U.S.C. § 512(h)(1) (2006).

278. § 512(h)(4).

279. § 512(h)(5).

280. *See Charter Commc'ns*, 393 F.3d at 777 (holding that the DMCA does not authorize the issuing of a subpoena when the ISP merely acts as a "conduit" to infringing conduct).

281. 18 U.S.C. § 2710(b)(2)(F) (2006).

282. § 2710(b)(2)(D).

283. 47 U.S.C. § 551(c)(2)(B) (2006).

284. § 551(h).

285. 18 U.S.C. § 2703(c).

286. § 2703(d).

other information to "any person other than a governmental entity."[287]

Absent statutory direction, courts must weigh the parties' competing interests: the plaintiff's interest in seeking redress for alleged harms and the defendant's interest in remaining anonymous.[288] Setting the subpoena standard too high might leave the plaintiff without an opportunity to proceed upon even a valid claim,[289] while setting the standard too low will fail to provide defendants with adequate privacy protection and might allow their identities to be exposed without adequate notice.[290] More importantly, a standard set too low could allow the plaintiff to use the legal process to unmask an online actor merely to later seek extra-judicial retribution.[291]

Many courts have recently addressed this balancing act in the context of defamation actions.[292] The defamation claim is particularly interesting because it already requires balancing the speaker's right in free speech against the subject's interest in redressing harms to his reputation.[293] In the online world, the relevant factors may tip in the plaintiff's favor: the Internet allows speakers to reach more people at a faster rate,[294] potentially multiplying the effects of defamatory speech,[295] and the underlying technology provides a method by which

287. 18 U.S.C. § 2702(c)(6); United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) ("[T]he ECPA's concern for privacy extends only to government invasions of privacy. ISPs are free to turn stored data and transactional records over to nongovernmental entities.").

288. *See* Doe v. Individuals Whose True Names Are Unknown, 561 F. Supp. 2d 249, 254 (D. Conn. 2008); Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

289. *See* Michael S. Vogel, *Unmasking "John Doe" Defendants: The Case Against Excessive Hand-Wringing over Legal Standards*, 83 OR. L. REV. 795, 807–08 (2004).

290. *Seescandy.com*, 185 F.R.D. at 578; Spencer, *supra* note 29, at 499.

291. *See Seescandy.com*, 185 F.R.D. at 578 ("People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity."); Spencer, *supra* note 29, at 498 (discussing a case in which an employer discovered the identities of twenty-one online speakers, dropped its trade secret suit, and fired the four who were its employees).

292. *See Doe v. Individuals*, 561 F. Supp. 2d at 255 (reviewing subpoena standards for unmasking an anonymous defendant). For further analysis of this line of cases, see generally Mazzotta, *supra* note 32, at 833, and Ryan M. Martin, *Freezing the Net: Rejecting a One-Size-Fits-All Standard for Unmasking Anonymous Internet Speakers in Defamation Lawsuits*, 75 U. CIN. L. REV. 1217 (2007).

293. Doe v. Cahill, 884 A.2d 451, 456 (Del. 2005). When a plaintiff shows sufficient evidence of a defamation claim, however, further balancing against a defendant's free speech interest is unnecessary because truly defamatory speech is not protected by the First Amendment. Beauharnais v. Illinois, 343 U.S. 250, 266 (1952); Solers, Inc. v. Doe, 977 A.2d 941, 956 (D.C. Cir. 2009).

294. *See In re* Subpoena Duces Tecum to Am. Online, Inc., No. 40570, 2000 WL 1210372, at *6 (Va. Cir. Ct. Jan. 31, 2000), *rev'd on other grounds*, 542 S.E.2d 377 (Va. Ct. App. 2001).

295. *Id.* at *7.

the speaker may be easily identified.[296] Courts have, therefore, grappled with setting a standard that appropriately protects online speakers.

Three distinct standards have emerged from the case law.[297] Providing the least protection to a speaker's anonymity is the "good faith" standard articulated by a Virginia trial court in *In re Subpoena Duces Tecum to America Online*.[298] In that case, an anonymous publicly traded company sought to expose the identities of five John Doe defendants who had allegedly made defamatory comments in an America Online chatroom.[299] Although recognizing the Does' right to anonymous free speech on the Internet,[300] the court found in favor of the compelling state interest in protecting companies from actionable communication.[301] The court held that it may order an ISP to disclose the identity of a subscriber when the plaintiff's pleadings or evidence show a "legitimate, good faith basis" to claim that it was the victim of actionable conduct and the identity of the subpoenaed party is "centrally needed to advance that claim."[302] This standard is fairly deferential to the plaintiff's interest in seeking redress for alleged harms.[303]

At the other end of the spectrum is the "summary judgment" standard established by the Supreme Court of Delaware in *Doe v. Cahill*.[304] A public official sought to expose the identity of an online poster who allegedly made defamatory remarks on a newspaper blog lambasting the official's "failed leadership" and "character flaws."[305] The trial court adopted the "good faith" standard and held that the official could subpoena the speaker's ISP for his identifying information.[306] On Doe's interlocutory appeal, the state supreme court expressed concern that setting the subpoena standard too low may cause online actors to self-censor out of fear of future liability.[307] A "sue first, ask questions later" approach and a minimally protective subpoena standard could act to "discourage debate on important issues of

296. Martin, *supra* note 292, at 1220.

297. For further examination of subpoena standards in defamation cases, see *id.* at 1228–37.

298. *Am. Online*, 2000 WL 1210372, at *8.

299. *Id.* at *1.

300. *Id.* at *6.

301. *Id.* at *7.

302. *Id.*

303. *See* Doe v. Individuals Whose True Names Are Unknown, 561 F. Supp. 2d 249, 255 (D. Conn. 2008); Doe v. Cahill, 884 A.2d 451, 458 (Del. 2005).

304. *Cahill*, 884 A.2d at 461.

305. *Id.* at 454.

306. *Id.* at 455.

307. *Id.* at 457.

public concern."[308] Finding the good faith standard too easily met, the court adopted a stricter "summary judgment" standard.[309] Under this standard, a plaintiff seeking to expose an anonymous defendant must provide prima facie evidence of his claim and make reasonable efforts to notify the defendant of a subpoena or application for court order.[310] Because the plaintiff would have easy access to proof of most of the elements of the claim, the court said, it would not be overly burdensome to require prima facie proof before disclosing the defendant's identity.[311]

The U.S. Court of Appeals for the District of Columbia Circuit recently adopted a standard very near the *Cahill* summary judgment standard.[312] In *Solers, Inc. v. Doe*, a Virginia corporation subpoenaed a trade association for the identifying information of a tipster who had falsely alleged that the corporation violated copyright law by using unlicensed software.[313] Unlike other defamation cases, the Doe defendant had not posted his accusation on an Internet message board but had rather sent a personal message using the trade association's Web site.[314] Despite this factual difference, and the recognition that a trial court may need to modify the test "depending on the type of injury alleged,"[315] the court adopted a summary judgment standard.[316] The *Solers* test required that the plaintiff (1) adequately plead the elements of his claim and offer evidence creating a genuine issue of material fact on every element within his control; (2) use reasonable efforts to notify the defendant of the subpoena; (3) show that the information sought would enable the plaintiff to proceed with his lawsuit;[317] and (4) delay further action to allow the defendant a reasonable time to move to quash the subpoena.[318]

---

308. *Id.*

309. *Id.* at 458, 460. The court relied heavily upon a similar standard imposed by the Superior Court of New Jersey in the case *Dendrite International, Inc. v. Doe*, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).

310. *Cahill*, 884 A.2d at 461.

311. *Id.* at 464. The court noted that it could be difficult or impossible to prove a defendant's actual malice without discovering the defendant's identity. *Id.* Therefore, proof of that element of a public figure's defamation claim could be postponed, and the plaintiff would only be required to show proof of elements within its control. *See id.*

312. *See* Solers, Inc. v. Doe, 977 A.2d 941 (D.C. Cir. 2009).

313. *Id.* at 944–45.

314. *Id.* at 957.

315. *Id.* at 952.

316. *Id.* at 954.

317. This factor is easily satisfied when the anonymous speaker the plaintiff seeks to identify is the defendant, for the plaintiff cannot proceed with his action until he knows who the defendant is. *Id.* at 955.

318. *See id.* at 954.

Between the stringent "summary judgment" standard and the deferential "good faith" standard lies the standard established by the U.S. District Court for the Northern District of California in *Columbia Insurance Co. v. Seescandy.com*.[319] A trademark owner sought to identify the party who started a Web site using the owner's registered trademark.[320] The court held that a "motion to dismiss" standard sufficiently balanced the parties' competing interests.[321] By requiring the plaintiff to plead an actionable claim and a likelihood that the discovery would reveal the identity of the Doe defendant, the standard would help "to prevent abuse of this extraordinary application of the discovery process."[322]

While these subpoena standards are quite varied, there are certain elements consistent within each.[323] Before unmasking a Doe defendant, most courts require a plaintiff to provide adequate notice to the defendant, to make some evidentiary showing of the merits of his claim, and to explain why the need to expose the online actor's identity outweighs that person's First Amendment right to anonymous speech.[324]

B. The Fourth Amendment Provides No Protection to Transactional Information

Although an in-depth discussion of Fourth Amendment jurisprudence as applied to the Internet is outside the scope of this Comment,[325] one critical concern must be mentioned in light of the many criminal cases discussed above. A criminal defendant may be tempted to argue that he has an objectively reasonable expectation of privacy in the subscriber information on file with his ISP.[326] The defendant may reason that he disclosed his name, address, browsing history, and other personal information to his ISP only for the limited purpose of

319. Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999).

320. *Id.* at 575–76.

321. *See id.* at 579. The court's full test contained four prongs, requiring the plaintiff to (1) "identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person," (2) "identify all previous steps taken to locate the elusive defendant," (3) establish that the case could withstand a motion to dismiss, and (4) file a discovery request with the court identifying the persons on whom discovery could be served. *Id.* at 578–80.

322. *See id.* at 579–80. The motion to dismiss standard has been criticized as potentially confusing because of variations in standards across jurisdictions. Doe v. Individuals Whose True Names Are Unknown, 561 F. Supp. 2d 249, 255 (D. Conn. 2008).

323. *See* Mazzotta, *supra* note 32, at 846.

324. *Id.* at 847–56.

325. For more on Fourth Amendment protections online, see generally Solove, *supra* note 9, at 1083, and Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010).

326. *See, e.g.*, United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010).

obtaining Internet services and did not consent to the release of that information to third parties.[327]

This argument, however, would probably be unavailing. "Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."[328] Under the third party doctrine, all objectively reasonable expectations of privacy are extinguished when users voluntarily expose data to third parties.[329] Because Internet users "voluntarily convey[ ] all this information to [their] internet and phone companies . . . [they] assume[ ] the risk that those companies [will] reveal the information to the police."[330]

This result is generally in accordance with similar case law governing the disclosure of information voluntarily exposed to telephone operators and similar entities.[331] The apparent unwillingness to distinguish between older technology and the Internet is understandable.[332] As the Supreme Court recently noted in a case examining whether a government employee had a reasonable expectation of privacy in the text messages sent from his employer-issued pager, "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[333]

Nevertheless, it may be time to reexamine Fourth Amendment law, particularly the third party doctrine, as applied to the Internet.[334] In his famous dissent to the 1928 wire-tapping case *Olmstead v. United States*,[335] Justice Louis Brandeis expressed concern that "[w]ays may some day be developed by which the Government, without removing

327. *See id.*

328. *Id.* (quoting United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008)); *see also* Kerr, *supra* note 325, at 1026 ("Courts . . . have uniformly concluded that the Fourth Amendment does not protect [basic subscriber information].").

329. *See* David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2227 (2009).

330. *Bynum*, 604 F.3d at 164 (alterations omitted) (internal quotations omitted) (quoting Smith v. Maryland, 442 U.S. 735, 744 (1979)); *see, e.g.*, Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (concluding that "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator").

331. *See* Couillard, *supra* note 329, at 2214–15, 2227; Robert A. Pikowsky, *An Overview of the Law of Electronic Surveillance Post September 11, 2001*, 94 L. LIBR. J. 601, 608 (2002).

332. The lethargic way in which courts have approached Fourth Amendment concerns online is certainly not unprecedented: "[I]t took the Supreme Court until 1967—nearly a full century after the invention of the telephone—to recognize telephone conversations as constitutionally protected against unreasonable searches." Couillard, *supra* note 329, at 2206.

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

334. *See* Kerr, *supra* note 325, at 1006–07.

335. Olmstead v. United States, 277 U.S. 438 (1928).

papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[336] Today, with the help of ISPs, the government has easy access to these "papers." IP addresses allow the "government [to] learn the names of stores at which a person shops, the political organizations a person finds interesting, a person's sexual fetishes and fantasies, her health concerns, and so on,"[337] but Internet users currently have no reasonable expectation of privacy in the subscriber data linking this information back to them as individuals. To say that Internet subscribers voluntarily exposed this information to ISPs is simplistic and misleading. After all, the only way to avoid releasing this information to an ISP is to not use the Internet at all.[338]

Interestingly, New Jersey constitutional law may provide a model for updating the third party doctrine. In the 2008 case *State v. Reid*,[339] the Supreme Court of New Jersey held that the state's constitution affords its citizens a reasonable expectation of privacy in the subscriber information provided to ISPs.[340] The defendant Shirley Reid was indicted for second-degree computer theft after she allegedly logged onto a Web site belonging to one of her employer's suppliers, changed her employer's password to the site, and altered the employer's shipping address.[341] The supplier subsequently informed Reid's employer of the changes and provided it with the IP address that the perpetrator had used to log onto the Web site.[342] The employer issued a municipal subpoena to the associated ISP and received Reid's name, home address, telephone number, account number, e-mail address, and method of payment in return.[343]

The trial court granted Reid's motion to suppress the subpoena evidence and the appellate court affirmed, finding various procedural flaws in the subpoena and concluding that Reid had a protected privacy interest in her subscriber information.[344] On appeal, the state supreme court began by recognizing that the New Jersey constitution affords greater protection against unreasonable searches and seizures

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

337. Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1287 (2004).

338. "To sign up for [Internet] service, a customer *must* disclose personal information including one's name, billing information, phone number, and home address." State v. Reid, 945 A.2d 26, 28 (N.J. 2008) (emphasis added).

339. *Id.* at 26.

340. *Id.* at 28.

341. *Id.* at 27.

342. *Id.*

343. *Id.* at 27, 29–30.

344. *Id.* at 30.

than that provided by the Fourth Amendment.[345] The court reviewed *State v. Hunt*,[346] a 1982 case in which the court had extended privacy protection to telephone records by reasoning that such information was released only as a necessity for obtaining phone service.[347] Analogizing ISP records to those maintained by phone companies and banks, the *Reid* court reasoned that Internet users should not lose their privacy interest in information that they must release in order to obtain Internet service.[348]

> In the world of the Internet, the nature of the technology requires individuals to obtain an IP address to access the Web. Users make disclosures to ISPs for the limited goal of using that technology and not to promote the release of personal information to others. Under our precedents, users are entitled to expect confidentiality under these circumstances.[349]

While adopting a viewpoint closer to that expressed in *Reid* would require significant retooling of Fourth Amendment jurisprudence, such changes may be necessary. As Orin Kerr, professor at George Washington University Law School, recently concluded, "[T]he application of the Fourth Amendment to computer networks will require considerable rethinking of preexisting law . . . ."[350]

C. *Recognizing IP Addresses as PII Will Help Protect Online Identity*

Unsurprisingly, the burden of incorporating IP addresses into the wide and varied framework of privacy law would itself be widely different depending upon the context. Some statutes anticipate the addition of categories of data to the list of PII. COPPA, for example, lists under its definition of personal information "any other identifier that the Commission determines permits the physical or online contacting of a specific individual."[351] The False Identification Crime Control Act includes a "unique electronic identification number, address, or routing code" as a means of identification.[352] For these and similar statutes, no change need be made other than an explicit recognition that an IP address may be personally identifiable and otherwise meets the criteria of data worth protecting.

---

345. *Id.* at 32.
346. State v. Hunt, 450 A.2d 952 (N.J. 1982).
347. *Reid*, 945 A.2d at 32.
348. *Id.* at 33.
349. *Id.*
350. Kerr, *supra* note 325, at 1006–07.
351. 15 U.S.C. § 6501(8)(F) (2006).
352. 18 U.S.C. § 1028(d)(7)(C) (2006).

Other statutes would require substantial amendment. The Stored Communications Act, for example, allows "basic subscriber information,"[353] including "any temporarily assigned network address," to be obtained with a mere subpoena.[354] To protect the user's online identity as exposed by an IP address, this category of easily accessible information could be removed. Such an amendment could be in accordance with the Act's purpose: to protect the *content* of stored e-mail.[355] Limiting access to a user's IP address would likewise prevent the easy correlation of an individual to the *content* of his online activity.[356]

Once protected by statute, the IP address would be subject to the applicable subpoena standards. As discussed above, these standards would provide varying degrees of protection to the online speaker's identity.[357] This may be a desirable result. The statutes were enacted for particular purposes[358] and already strike a balance between the plaintiff's and defendant's interests. The DMCA, for example, allows subpoenas to "expeditiously issue" in order to protect the rights of copyright owners.[359] The standard weighs in favor of the plaintiff copyright owner who desires to quickly stop the distribution of his intellectual property. The Video Privacy Protection Act, on the other hand, requires a higher showing of compelling need and ample notification to the subject.[360] This balance suggests that the release of video rental records is less important to the plaintiff, less time-sensitive, and more private.

Specifically recognizing IP addresses as PII should not alter these balances. Providing due respect for the power of an IP address to identify an individual would, however, provide a better guide for courts' analyses and could alter the outcome of close cases. The 2008 case *Viacom v. YouTube*[361] presents a pertinent example. Viacom and other copyright owners sued YouTube on direct, vicarious, and contributory infringement theories for allowing users to upload and

353. 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, 1219–20 (2004).

354. 18 U.S.C. § 2703(c)(2).

355. *See* Kerr, *supra* note 353, at 1234.

356. *See* EFF Amicus Brief, *supra* note 120, at 4 (noting that the IP information at issue in the *Klimas* case "include[d] information about what subscribers communicated, viewed or read online").

357. *See supra* notes 273–87 and accompanying text.

358. Lah, *supra* note 24, at 684; Berman & Mulligan, *supra* note 10, at 576.

359. 17 U.S.C. § 512(h)(4) (2006).

360. *See* 18 U.S.C. § 2710(b)(2)(F) (2006).

361. Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256 (S.D.N.Y. 2008).

view their copyrighted videos on the YouTube Web site.[362] During discovery, Viacom sought YouTube's logging database, which linked User IDs and IP addresses to the videos that each user had viewed or uploaded.[363] YouTube sought the protection of the Video Privacy Protection Act, arguing that releasing the data would allow Viacom to determine the viewing and uploading habits of individual users.[364] The district court refused to apply the Act, reasoning that YouTube's privacy concerns were speculative because the IDs and IP addresses could not in themselves identify individuals.[365] The court subsequently granted production of the database.[366]

Given the ability of IP addresses to identify users, YouTube's argument should have been given greater weight. Armed with YouTube's database, Viacom could, for example, choose the top one hundred IP addresses used to upload its copyrighted material. Viacom could obtain the names, addresses, and other personal information of the users tied to those IP addresses by issuing subpoenas to the appropriate ISPs. The company could then sue those users directly for copyright infringement in the same way that the RIAA has sued individual file-sharers.[367] While YouTube activity should probably not be hidden behind the Video Privacy Protection Act, which exists to protect the records of legitimate video rentals, the court's analysis would have been better served by recognizing that the logging database would allow Viacom to identify particular YouTube users and their viewing habits. Giving Viacom access to such a database is not a trivial matter, and it deserved the court's considered analysis of whether Viacom's interest in tracking down copyright infringers outweighed the privacy interests of potentially millions of users who would be linked to the content they had viewed on the Web site.[368]

Recognizing the ability of an IP address to identify an individual will also be important for a court's analysis when it must balance the parties' competing interests absent a statutory subpoena standard. In some circumstances, more may be at stake than merely identifying the defendant: whenever a plaintiff compels the production of logs that

362. *Id.* at 258–59.

363. *Id.* at 261.

364. *Id.* at 262.

365. *Id.*

366. *Id.*

367. *See supra* notes 187–93 and accompanying text (discussing a case in which the RIAA sought to use IP addresses to expose the identities of alleged downloaders of copyrighted music).

368. *See* Patricia Sánchez Abril & Anita Cava, *Health Privacy in a Techno-Social World: A Cyber-Patient's Bill of Rights*, 6 NW. J. TECH. & INTELL. PROP. 244, 251 (2008) (expressing concern that the decision could set precedent requiring social networking Web sites to disclose their users' computer locations and online activities).

identify IP traffic, users may be associated with the content of their online activity.[369]

Adequately protecting the online actor's interest requires that one of the more stringent subpoena standards be applied.[370] The *Solers* test, which requires the plaintiff to meet the summary judgment standard and use reasonable efforts to provide notice to the defendant,[371] would ensure that the plaintiff's interest in exposing the defendant outweighs the defendant's interest in remaining anonymous. By requiring a plaintiff to make a significant showing of his case, a court would deter the misuse of the discovery process to expose online actors merely for extra-judicial retribution or speech suppression.[372] Providing the defendant notice of the subpoena and sufficient time to submit a motion to quash would ensure that a defendant with important privacy concerns is afforded an opportunity to protect his interests.[373]

Finally, recognizing the reality of what an IP address can do would support reexamining the application of Fourth Amendment law to these situations. Cases that hold users have no Fourth Amendment interest in the information voluntarily exposed to ISPs have viewed IP addresses as transactional data, similar to a listing of the telephone numbers a particular user dialed.[374] As this Comment has discussed, however, IP addresses are more likely to disclose the *content* of a user's online activity. Although redialing a phone number may not reveal the content of the user's previous conversation,[375] browsing for the particular IP address may reveal that the user visited a socially unpopular Web site or even one that contained criminalized material. This possibility means that, in some circumstances, IP addresses are more akin to the content of communications than they are transactional data and should be protected appropriately.

Whatever the context, courts should recognize the value and importance of IP addresses to online conduct and the litigation that arises

369. *See* Couillard, *supra* note 329, at 2229 (discussing how the transactional nature of IP addresses may be conflated with the content of Internet communications).

370. *See supra* notes 304–18 and accompanying text.

371. Solers, Inc. v. Doe, 977 A.2d 941, 955 (D.C. Cir. 2009).

372. *See* Doe v. Cahill, 884 A.2d 451, 462 (Del. 2005) (adopting a summary judgment standard as the proper balance between the parties' interests).

373. *Accord id.*

374. *See* Couillard, *supra* note 329, at 2215; *cf.* Smith v. Maryland, 442 U.S. 735, 742 (1979) ("[W]e doubt that people in general entertain any actual expectation of privacy in the [telephone] numbers they dial.").

375. *See Smith*, 442 U.S. at 743 (distinguishing between the telephone number dialed, to which the user had no reasonable expectation of privacy, and the contents of the communication); Couillard, *supra* note 329, at 2229.

out of that activity. An IP address may be no more than a number, but it may be associated with a particular individual in the same manner as a home address or telephone number, pieces of data that are consistently protected as personal. In fact, IP addresses go further by linking users to their online activities. As the technology progresses, the likelihood of identifying a user will increase: with the new IPv6 protocol, most devices connected to the Internet will have a unique, static address that can distinguish that device anywhere in the world.[376] The technical hurdles will be removed, and all online activity will be linked to particular laptops, computers, cell phones, PDAs, and their users.[377]

Recognizing an IP address as personal data should not create a blanket of anonymity online. Crimes and civil wrongs are committed online every day, and those harmed by these actions deserve the appropriate remedies. Nevertheless, courts need to be able to factor online privacy concerns into their balancing of litigants' interests. The first step in improving that balancing analysis is recognizing that IP addresses can often be traced back to online actors and should, therefore, be considered personally identifiable information.

V. CONCLUSION

In mid-2003, the RIAA obtained seventy-five subpoenas every day, each using an IP address to unmask the identity of an alleged downloader of illegal music files.[378] Many such subpoenas are issued as a matter of course,[379] and while some courts have expressed concern for the anonymous online speaker, others have uniformly granted subpoenas without judicial oversight.[380] Often, the speaker's privacy concerns are never addressed.[381]

When courts do examine privacy interests, however, they often struggle to find the proper balance between a defendant's right to remain anonymous and a plaintiff's right to due process of law.[382] This struggle demonstrates the importance of IP addresses: armed with an IP address, a cooperating ISP, and an IP address log, any litigant can determine the identity of an online speaker. Like a Social Security number, home address, or telephone number, an IP address is often

376. *See* Weinberg, *supra* note 66, at 1260–61.
377. *See id.*
378. Vogel, *supra* note 289, at 814.
379. Tene, *supra* note 18, at 1455.
380. *See* Vogel, *supra* note 289, at 803; Ham, *supra* note 68, at 20.
381. *See* Mazzotta, *supra* note 32, at 855.
382. *See supra* notes 288–322 and accompanying text.

correlated to the identifying information of a particular individual. Although the personal information on file with an ISP may not always be the actual speaker's name, identifying the Internet subscriber will usually be enough to narrow the search to a small number of individuals, such as members of a particular household.[383]

Despite some technical shortcomings, the IP address is more often than not able to expose the person behind the computer. As the technology progresses, IP addresses will be even more consistently tied to individual devices and their users. If courts are willing to permit this correlation to provide probable cause to suspect an individual of online activity, or to serve as circumstantial evidence tending to prove a defendant's liability for online conduct, they should also be willing to consider the privacy interests involved. Protecting IP addresses as personally identifiable information will assist courts in properly considering these interests and in balancing the litigants' expectations of online privacy.

*Joshua J. McIntyre**

383. *See* EFF Amicus Brief, *supra* note 120, at 9.

* J.D. Candidate 2011, DePaul University College of Law; B.A. 2008, Saint Ambrose University. I would like to thank Associate Professor Matthew Sag of the Loyola University Chicago School of Law, whose guidance aided the direction of this Comment, as well as all of the Law Review members who have provided their excellent editorial assistance. I also want to thank my parents, David and Kimma McIntyre, and my fiancée, Ann Lamb, whose continued love and support have always kept me moving forward.