NOTE

Electronic Filing and Informational Privacy

By KYLA KITAJIMA*

Introduction

Imagine that you are involved in a messy lawsuit. Would you want your pleadings to be available on the Internet for anyone to see? This might soon be a reality. Already, some courts have implemented electronic filing pilots programs.[1] Eventually, court pleadings and documents will be available to anyone with Internet access.

By transmitting court information through an electronic medium,[2] Internet filing is the newest way to process legal documents. There are tremendous benefits to filing court documents over the Internet.[3] Electronic filing increases judicial efficiency and cuts costs for attorneys, clients, and courts.[4] Attorneys can file documents without ever leaving their offices.[5] The system also provides easier public access to court documents and the judicial system.[6] Anyone can view documents and court calendars, retrieve court information

---

* J. D. University of California, Hastings College of the Law (2000); B.A. University of California, San Diego (1997). The author thanks Professor Ashutosh Bhagwat for his help and substantive review and Cary Zak and Megan Jellinek for their editing and support.

1. *See, e.g.*, Rinat Fried, *Electronic Filing: The End of Bike Messengers?*, RECORDER, Oct. 13, 1998, at 4.

2. Steven P. Daitch & Philip B. Ytterberg, *Electronic Filing: Divine Intervention Needed?*, LAW TECH. PROD. NEWS, Dec. 1998, at 97.

3. *See id.*

4. *See id.*

5. *See id.*

6. *See* Wendy R. Leibowitz, *Electronic Filing Looks Easy, But Chaotic Approach Slows Progress*, NAT'L L. J., Jan. 13, 1997, at B20.

and forms, pay filing fees, and receive court notices.[7] In the United States, approximately 200 million filings are made each year.[8] Implementation of electronic filing systems will make these filings quicker, easier, and cheaper.[9]

We live in an "information society" where information is a valuable commodity.[10] The Internet continues to be a substantial source of information.[11] Current technology allows us to store more information for longer periods of time.[12] Given the efficiency of the Internet, the benefits of electronic filing are substantial. Internet use, however, generates growing concerns about possible privacy invasions.[13]

Court documents have traditionally been public documents. Now, because Internet information is more readily accessible and easier to manipulate than traditional paper documents, we need to consider new safeguards to protect individual privacy interests. This note presents two means of addressing the problems inherent in Internet filing. First, this note discusses possible legislative solutions to the privacy problems associated with electronic filing of court documents. Second, this note considers recognition of a new constitutional right to informational privacy.

I. Benefits of Electronic Filing and Particular Privacy Problems

Electronic filing allows attorneys to file court documents without ever making a trip to the courthouse.[14] Attorneys can file court documents from their home or office computers. Clerks will then receive the documents on their computers in the courtroom.[15] Many courts have already implemented electronic filing pilot projects.[16]

---

7. *See* Daitch & Ytterberg, *supra* note 2, at 97.

8. *See id.*

9. *See id.*

10. *See* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1162 (1997) (footnotes omitted).

11. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 6-7 (1997).

12. *See* ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY 324 (1995).

13. *See* Rocco Cammarere, *Electronic Access: Privacy Invasion?*, N.J. LAWYER, June 30, 1997, at 1.

14. *See* Daitch & Ytterberg, *supra* note 2, at 97.

15. *See* Albert L. Wells & Michael Winger, *Now in Development: The Courthouse on the Web*, LEGAL TECH, March 1998, at 1.

16. *See, e.g.*, Fried, *supra* note 1, at 4 (discussing San Francisco Superior Court's electronic filing implementation in October, 1998 for their asbestos cases). *See also* Peter

Since there are no technological barriers to electronic filing,[17] the system is projected to become widespread in the near future.[18] In fact, many judges and court administrators are so enthusiastic about the system that they are attending sold-out electronic filing seminars, sponsored by The National Center For State Courts.[19] Further, in some jurisdictions, attorneys are already able to electronically serve documents on each other.[20]

The goal of electronic filing is to "improv[e] accessibility and quality of justice."[21] Attorneys and judges seem to agree that the new system accomplishes both goals.[22] Attorneys like electronic filing because it saves time and money.[23] Since they do not have to hire messengers or worry about getting to the courthouse before the building closes, attorneys are able to spend more time preparing the substance of their filings.[24] Also, electronic filing is especially helpful for filing in out-of-state courts.[25] Another advantage of the electronic system is that multiple viewers can simultaneously access filed documents.[26] Attorneys are able to scrutinize documents filed in either their own cases or related cases without having to track down tangible copies.[27] Attorneys can also access court filings from a home or office computer.[28]

Electronic filing also makes the judicial system more accessible to those who cannot hire lawyers. For example, Maricopa County in Arizona has Arizona QuickCourt workstations, which "allow members of the public to fill out forms in English and Spanish; people can educate themselves on the basics of . . .family law matters and file

---

J. Ausili, *Using the EDNY Electronic Filing System*, N.Y.L.J., Jan. 12, 1999, at 5 (discussing implementation of electronic filing in the Eastern District of New York).

17. *See* Tom Little, *Electronic Filing: Why Aren't More Courts Offering It?*, LEGAL TECH, Nov. 1998, at 1 (describing a technology survey completed by the West Group).

18. *See* Daitch & Ytterberg, *supra* note 2, at 97.

19. *See id.*

20. However, currently, there are no universal standards for electronic serving of documents, and some attorneys are worried about the expense of this technology. *See, e.g.*, Fried, *supra* note 1, at 4.

21. Little, *supra* note 17, at 1.

22. *See, e.g.*, Daitch & Ytterberg, *supra* note 2, at 97.

23. *See id.*

24. *See* Albert L. Wells & Michael Winger, *Now in Development: The Courthouse on the Web*, LEGAL TECH, March 1998, at 1.

25. *See id.*

26. *See id.*

27. *See id.*

28. *See* Leibowitz, *supra* note 6.

the papers themselves."[29]

Judges like electronic filing because the system presents an efficient way to manage the numerous documents involved in litigation.[30] Electronic filing is especially useful in complex litigation cases—where cumbersome, voluminous filings are common.[31] In addition, the electronic filing system saves courts money.[32] A Kansas court compared the cost of filing documents electronically rather than by means of the traditional paper method.[33] "To file 100 documents traditionally took more than 10 hours to process and roughly $220 in staff time. But to file the same documents electronically took 9 minutes and cost a mere $2.80."[34] Electronic filing also saves clients money.[35] In the United States, clients pay their attorneys approximately $35.00 per delivery event, which does not include the cost of "rush" deliveries.[36] Electronic filing could eliminate these delivery charges.[37]

Although there are clear benefits to the electronic filing system, problems still frustrate certain aspects of the electronic process.[38] For example, there are no universal guidelines for electronic filing.[39] Further, it is unclear how courts will fund the system.[40] As a practical matter, some attorneys worry that their documents will not actually reach their destinations.[41] These attorneys will feel assured only after they receive a faxed confirmation from a court clerk or secretary.[42] The most serious concerns are the access and privacy problems that arise whenever information is available on-line.[43] The easy accessibility of information increases the potential for its misuse.[44]

---

29. *Id.*

30. *See* Fried, *supra* note 1, at 4.

31. *See id.*

32. *See* Daitch & Ytterberg, *supra* note 2, at 97.

33. *See id.*

34. *Id.*

35. *See id.*

36. *See id.*

37. *See id.*

38. *See* Daitch & Ytterberg, *supra* note 2, at 97; Cammarere, *supra* note 13, at 1; Little, *supra* note 17, at 1.

39. *See* Little, *supra* note 17, at 1.

40. *See id.*

41. *See* Liebowitz, *supra* note 6, at B20.

42. *See id.*

43. *See id.*

44. *See* CATE, *supra* note 11, at 3.

Corporations and individuals are taking advantage of current technology, using personal information to profit.[45] For example, "AOL, the nation's largest private online service, confirmed that it was compiling both the names and addresses of its subscribers and packaging lists with demographic information to sell to marketing companies and manufacturers."[46] In addition, criminals are using personal information in order to commit "identity theft":

> A clever swindler starts by using just a few bits of personal information, perhaps your full name and SSN, to access Internet databases and thereby obtain your address, telephone number, driver's license number, and so on. The swindler can then apply for credit using your good name, run up bills, take over bank accounts, rent apartments, buy cars, and at times even take out mortgages .... The important legal point about identity theft is that, unlike the accused in criminal cases, who have "reasonable doubt" on their side, victims of credit fraud bear the burden of proving they are not the individuals who incurred the debts and rang up the purchases in question.[47]

People are becoming more and more concerned about their confidentiality,[48] and rightly so. Criminals and profit-seeking organizations can access personal information on-line with astounding ease.[49] As information becomes easier to access, the privacy concerns of individuals and corporations become even more significant of an issue.[50]

Electronic filing presents particular privacy concerns. People are involved in lawsuits that cover a wide spectrum of issues. Potentially, a litigant's work history, medical information, marital history, family problems, and financial dealings could be disclosed in on-line pleadings. Litigants, unlike average e-mail or Internet users, do not have access to the same privacy protections. Generally, when using the Internet, there are certain safeguards that one can use to protect him or herself.[51] For example, a person can refrain from disclosing certain information, such as credit card numbers and addresses, over the Internet. Litigants, however, may not be able to withhold

45. *See* DAVID BRIN, THE TRANSPARENT SOCIETY 57 (1998).

46. *Id.*

47. *Id.* at 59-60.

48. *See id.* at 25.

49. *See id.* at 58.

50. *See, e.g.*, Matt Beer, *Another ID Number Flap Hits Intel*, S.F. EXAMINER, March 11, 1999, at B1 (describing how Intel is facing criticism for their computer chip that identifies users when they use the Internet).

51. *See* Gindin, *supra* note 10, at 1174-79.

information, as inclusion of the information in pleadings may be necessary to the lawsuit. Inclusion of this information is thus publicly available and may be subject to manipulation on-line. Electronic filing, therefore, poses particular privacy problems that extend beyond those inherent in the general Internet context.

II. Public Access to Courts

There is a common law right of public access to court records.[52] This common law right "exists to enhance popular trust in the fairness of the justice system, to promote public participation in the workings of government, and to protect constitutional guarantees."[53] However, the scope of this common law right is not clearly defined and the right is not absolute.[54] Thus, individual courts have taken it upon themselves to weigh competing interests in determining the reach of the common law right of public access.[55] Often, courts consider "whether public access is necessary to promote trustworthiness and respect in the judicial system."[56]

Generally, courts have upheld the presumption of public access to court records, including settlement agreements and documents filed in conjunction with summary judgment motions.[57] Courts "decided that settlement agreements are an important aspect of the civil judicial system, and therefore, public access to these documents is necessary to promote trustworthiness in the judicial system and enhance public understanding of the system."[58] For similar reasons, some courts have also concluded that the right of access applies to documents filed in conjunction with summary judgment motions.[59] However, courts are less likely to allow public access to documents filed in conjunction with discovery motions because public access would be contrary to the goals of discovery and would not further the

52. *See* Nixon v. Warner Communications, Inc., 435 U.S. 589, 597 (1978).

53. Arthur R. Miller, *Confidentiality, Protective Orders, and Public Access to the Courts*, 105 HARV. L. REV. 427, 429 (1991).

54. *See* Diane Apa, *Common Law Right of Public Access – The Third Circuit Limits its Expansive Approach to the Common-Law Right of Public Access to Judicial Records*, 39 VILL. L. REV. 981, 982-86 (1994).

55. *See id.* at 985.

56. *Id.* at 992.

57. *See id.* at 986-89.

58. *Id.* at 988.

59. *See id.* at 989.

objectives of the common law right of public access.[60] In general though, courts adhere to a strong presumption of public access for most court documents, absent a showing of exceptional circumstances.[61] In the electronic filing context, this right to public access must be reconciled with litigants' privacy rights.

III. Electronic Documents vs. Paper Documents: Equal Treatment?

With the advent of electronic filing and the Internet availability of court documents, public documents have become easier to access, compile, and manipulate.[62] Both the ease of access and danger of manipulation prompt another question: should electronic documents be treated the same as paper documents?[63] Those who advocate equal treatment of electronic and paper documents argue that paper documents that are considered "public" should likewise be treated as "public," regardless of medium.[64] A New Jersey subcommittee "concluded that 'drawing artificial distinctions between paper and electronic records for the sake of privacy expectations which are not realistic in today's information society is not an appropriate policy response.'"[65] Other commentators, however, including New Jersey Supreme Court Justice Marie L. Garibaldi, are concerned that "the computer's speed and agility to analyze public records may somehow impinge on a person's privacy rights."[66] The American Civil Liberties Union of New Jersey also expressed their concern, stating that they were:

> [T]roubled by the accessibility of entire data bases to inspection and copying, and by the possibility that such information could be manipulated. For example, corporations or individuals could create lists that would be used by employers and landlords to determine individuals' qualifications or eligibility based on

---

60. *See* Anderson v. Cryovac, Inc., 805 F.2d 1, 11-12 (1st Cir. 1986).

61. *See* Ronald D. May, *Public Access to Civil Court Records: A Common Law Approach,* 39 VAND. L. REV. 1465, 1478-1490 (1986).

62. *See* CATE, *supra* note 11, at 1-2.

63. *See, e.g.*, Cammarere, *supra* note 13, at 1.

64. *See id. See also* Henry H. Perritt, Jr., *Federal Electronic Information Policy*, 63 TEMP. L. REV. 201, 224 (1990) (stating that the prevailing view under the Freedom of Information Act is that electronic documents should be treated the same as paper documents).

65. Anna Snider, *Public Domain Dismissing Privacy Concerns, Court Panel Urges Electronic Access to Computerized Records*, 147 N.J.L.J. 1 (1997).

66. Cammarere, *supra* note 13, at 1.

litigation history in wrongful discharge or landlord-tenant actions.[67]

Justice Garibaldi also distinguished electronic documents from paper documents, stating that "[u]nlike paper records, computerized records can be rapidly retrieved, searched, and reassembled in novel and unique ways."[68]

There is truth to this distinction. Paper documents are less likely to be misused because they are more difficult to actually obtain and copy. In order for a person to retrieve a document, he or she would need to make a trip to the courthouse during business hours, wait in line, wait for an employee to find the file, and then wait for copies (or make copies him or herself). In contrast, electronic documents can be retrieved, copied, and manipulated without ever having to leave your desk. The public access characteristics of electronic documents indicate that, at least in the electronic filing context, electronic documents should be treated with more care than their paper counterparts.[69]

It is presently unclear whether the advent of electronic court documents will lead to increased misuse of information. Privacy concerns, however, are likely to grow once court pleadings become universally available on the Internet. Although the benefits of electronic filing and access are substantial, as a precaution, courts and legislators should consider and formulate guidelines to prevent misuse of information.

IV. Legislative Solutions to Electronic Filing Privacy Concerns

Federal privacy legislation governing the use of personal information is generally very specific, usually addressing a particular industry or area.[70] For instance, separate privacy legislation has been directed at privacy in the workplace and the protection of both educational and financial records.[71] Another piece of legislation is the

---

67. Snider, *supra* note 65, at 1.

68. Cammarere, *supra* note 13, at 1.

69. Despite these concerns, it appears that the prevailing view is in favor of equal treatment of electronic and paper documents. *See* Snider, *supra* note 65. Furthermore, states are currently enacting legislation that "provides that contracts entered into by electronic means have the same legal force and effect as paper contracts." George Raine, *New Way to Sign Papers*, S.F. EXAMINER, Jan. 2, 2000, at B1. For example, California recently enacted the Uniform Electronic Transactions Act, "which validates all transactions formed, transmitted and recorded electronically." *Id.*

70. *See* CATE, *supra* note 11, at 80.

71. *See id.* at 81-85.

Electronic Communications Privacy Act (ECPA), which contains some protections for Internet users.[72] However, this protection is limited by many exceptions.[73] For example, the Act does not protect against interceptions of communications made to a system that is "readily accessible to the general public."[74] Thus, "the ECPA is not violated when postings to Usenet groups, listservs [sic], bulletin board systems, and chat rooms are read and archived."[75] There are many criticisms of existing privacy legislation, namely that "most of these statutes contain exceptions that gut the protection."[76]

Privacy laws targeted at specific problem areas create a patchwork of federal privacy legislation. Currently, there is no comprehensive federal body of law to govern informational privacy as a whole. Until such a body of law exists, the most practical way to protect informational privacy is to implement state legislation directed at specified targets. Thus, an effective way to protect individual privacy interests within the judicial system is to enact state legislation to govern electronic filing.

A. Proposed Uniform State Legislation

Uniform state legislation should accomplish two goals. First, state law should provide a cause of action against individuals or businesses that manipulate data for fraudulent purposes. Second, state law should establish a commission, consisting of judges, practicing attorneys, computer experts, and members of the public, to establish uniform standards and guidelines for attorneys, courts, and the public. In crafting guidelines, the commission must acknowledge that the right to privacy conflicts with many other interests, including "society's interest in free expression, preventing and punishing crime, protection of private property, and the efficient operation of government."[77] Thus, suggested guidelines and standards must be flexible enough to accommodate these competing interests, while simultaneously protecting the individual's interest in nondisclosure of personal information. For example, the commission may consider adopting a categorical approach to help determine when to prohibit electronic filing. In particular, the commission may create special

72. *See* 18 U.S.C. §§ 2510-2520, 2701-2709 (1997).

73. *See* 18 U.S.C. § 2511(2)(g) (1994).

74. 18 U.S.C. § 2511(2)(g)(i) (1994).

75. Gindin, *supra* note 10, at 1198.

76. ALDERMAN & KENNEDY, *supra* note 12, at 330.

77. *Id.* at 102.

guidelines to govern family law and juvenile cases. In such situations, where the privacy stakes are high, the judge would have discretion to decide whether electronic filing is appropriate. In so deciding, the judge should consider whether the privacy interests at stake are greater than the need for on-line availability of court pleadings. Although this would give judges a great deal of discretion, this approach would at least provide some flexibility in deciding whether electronic filing would be appropriate in a particular case.

Courts should also be required to employ certain security measures to minimize manipulation of information. Courts should consider restricting access to computer-generated lists from court dockets, such as compilations of landlord-tenant claims in a given county.[78] Such lists are dangerous because they provide succinct lists of similar cases, which can then be used in a fraudulent or discriminatory manner. For example, landlords could obtain and use compilations of landlord-tenant cases in their county to discriminate against prospective tenants who have sued prior landlords. Courts should also employ security measures, so that they are able to detect tampering with documents. The San Francisco Superior Court has hired "Dallas-based LAWPlus Inc. . . . [to] creat[e] a secure audit so that any changes – including alterations to the content or backdating – can be detected and traced."[79]

Some citizens, attorneys included, lack the requisite technology to effectively utilize electronic filing. The process, therefore, should be voluntary – at least for the time being. One possible exception is in complex litigation cases, where there are voluminous filings and multiple parties. (In such cases, the benefits of electronic filing would be great – it would eliminate the stacks of paper and reduce the amount of paperwork for judges. However, it may be impractical to get all parties to agree to electronic filing. Thus, it may be sensible to require electronic filing in complex litigation cases.) It must be noted that while electronic filing may increase the efficiency, it would be unfair to penalize some individuals based on their lack of computer access. Voluntary participation, however, will allow those who can afford it to electronically file without penalizing those who lack the requisite technology.

---

78. However, courts should not bar access to these lists altogether. Instead, courts should employ methods to deter fraudulent activity. For example, individuals can apply for passwords, which will allow them to gain access to the lists. The passwords enable courts to know something about the individuals who are accessing the information.

79. Fried, *supra* note 1, at 4.

By following these guidelines, litigants will become aware of the privacy risks inherent in electronic access, and the invasion of privacy risks will be minimized by the imposed restrictions. Although it is impossible to prevent all misuse of information, state legislation and guidelines are essential in order to protect individual privacy in the electronic court system.

B. Possible Federal Legislation to Govern Electronic Filing

Federal legislation is another possible solution to potential electronic filing problems. Congress may be able to use its Commerce Clause power to regulate the sale and use of information obtained from state court electronic filing databases. In general, Congress can regulate three categories of interstate commerce: channels of interstate commerce, instrumentalities of interstate commerce, and activities that "substantially affect" interstate commerce.[80]

In *United States v. Lopez*, the Court struck down the Gun Free School Zones Act, which made possession of a firearm in or near schools a federal offense, as an improper use of the federal commerce power.[81] A student, who was convicted under the Act for possession of a gun in school, challenged the federal law on the grounds that Congress lacked the power to enact the law.[82] The Court, agreeing with the student, found that the Gun Free School Zones Act did not "substantially affect" interstate commerce. Although Congress is not required to adduce evidence of "substantial effect" on interstate commerce for every piece of legislation it enacts under the Commerce Clause, the Court stated that it would not defer to Congressional judgment if Congress produces no evidence to support a "substantial effect" on interstate commerce.[83] Because Congress had not accumulated evidence as to the impact that possession of guns in schools had on interstate commerce, the Court did not defer to the judgment of Congress. Instead, the Court conducted its own inquiry: Did the regulation of firearm possession in or near school zones substantially affect interstate commerce? In support of "substantial

80. *See* United States v. Darby, 312 U.S. 100 (1941) (discussing channels of interstate commerce); NLRB v. Jones & Laughlin Steel Corp., 301 U.S. 1 (1937) (discussing "substantial effect" on interstate commerce); Shreveport Rate Cases, 234 U.S. 342 (1914) (discussing instrumentalities).

81. 514 U.S. 549, 551 (1995).

82. *See id.* at 552-53.

83. *See id.* at 562-63.

effect" on interstate commerce, the Government put forth three arguments: "First, the costs of violent crime are substantial, and, through the mechanism of insurance, those costs are spread throughout the population. Second, violent crime reduces the willingness of individuals to travel to areas within the country that are perceived to be unsafe."[84] Third, the Government argued that the presence of guns in schools posed "a substantial threat to the educational process by threatening the learning environment."[85] The Court rejected all of these arguments, reasoning that, if accepted, Congress could effectively regulate *any* activity that might lead to violent crime or reduced national productivity.[86] Congress, therefore, would have unlimited authority to regulate anything and everything, as long as it somehow decreased violent crime or national productivity. Thus, the Court refused to uphold the constitutionality of the Act.

In *United States v. Darby,* the Court held that Congress could use its commerce power to regulate channels of interstate commerce.[87] There, the Court upheld the Fair Labor Standards Act, which prevented the interstate shipment of certain goods that did not meet the Act's minimum wage and labor standards. In upholding the Act, the Court stated: "While manufacture is not of itself interstate commerce the shipment of manufactured goods interstate is such commerce and the prohibition of such shipment by Congress is indubitably a regulation of the commerce."[88]

Although the federal commerce power appears broad, it is not without limits.[89] Federal legislation, although a proper exercise of the Congress' commerce power, may nevertheless be invalid as an improper intrusion on state autonomy.[90] The Court revisited Commerce Clause and state autonomy issues in *Reno v. Condon*,

84. *Id.* at 563-64.

85. *Id.* at 564.

86. *See id.*

87. 312 U.S. 100, 115 (1941).

88. *Id.* at 113.

89. *See* U.S. CONST. amend. X ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.").

90. *See* Printz v. United States, 521 U.S. 898, 935 (1997) (holding that Congress cannot command the States' officers directly); New York v. United States, 505 U.S. 144, 149 (1992) (holding that Congress cannot force the States to enact or enforce a federal regulatory program); South Carolina v. Baker, 485 U.S. 505, 514 (1988) (Congress can regulate state activities but cannot "seek to control or influence the manner in which States regulate private parties.").

which involved a federal statute regulating the use and resale of information from state Department of Motor Vehicle (DMV) databases.[91]

In *Reno v. Condon*, the Supreme Court upheld the constitutionality of the Driver's Privacy Protection Act (DPPA).[92] The DPPA regulated the state's disclosure and resale of personal information contained in the records of state DMVs.[93] The State of South Carolina and its Attorney General challenged the constitutionality of the DPPA. The Court found that the DPPA was a proper exercise of Congress' power to regulate under the Commerce Clause and did not violate South Carolina's state autonomy. The Court stated that drivers' information constituted an instrumentality of commerce because "its sale or release into the interstate stream of business is sufficient to support congressional regulation."[94]

The Court then addressed South Carolina's argument that the DPPA violated the Tenth Amendment because it required state employees to learn and apply the Act's restrictions. Although the Court acknowledged that "the DPPA's provisions will require time and effort on the part of state employees,"[95] the Court nonetheless concluded that the DPPA did not violate states' rights. The Court analogized the case to *South Carolina v. Baker*, emphasizing that although some state action may be necessary to comply with federal regulation, such state involvement is inevitable and presents no constitutional defect.[96] The Court concluded:

> "[T]he DPPA does not require the States in their sovereign capacity to regulate their own citizens. The DPPA regulates the States as the owners of databases. It does not require the South Carolina legislature to enact any laws or regulations, and it does not require state officials to assist in the enforcement of federal statutes regulating private individuals."[97]

Thus, in order for federal electronic filing legislation to survive constitutional scrutiny, Congress should first show that it seeks to regulate a channel of interstate commerce, an instrumentality of interstate commerce, or an activity that *substantially affects* interstate

91. 528 U.S. 141 (2000).
92. *See id.* at 150.
93. *See id.* at 146.
94. *Id.* at 148.
95. *Id.* at 150.
96. *See id.* at 151.
97. *Id.*

commerce. Second, Congress must be careful to craft legislation that comports with state autonomy limits on the federal commerce power.

Because it is not acceptable practice for courts to compile and sell court information, electronic filing legislation would not regulate an instrumentality of interstate commerce. It is possible for the Government to argue that the regulation of electronic filing involves a channel of interstate commerce (namely, the Internet). The Internet is a "channel" of interstate commerce because goods are sold and transferred via the Internet. Thus, because electronic filing requires Internet use, regulation of electronic filing constitutes regulation of a channel of interstate commerce. However, it is unclear whether this argument would succeed because the courts have not yet addressed this issue.

Perhaps the best way Congress can demonstrate its power to regulate under the Commerce Clause is to present evidence that the sale and exchange of court information by private parties substantially affects interstate commerce. Currently, such evidence does not exist. Because relatively few courts have adopted electronic filing, speculation about the potential impact on interstate commerce may be too tenuous to withstand constitutional scrutiny. However, if, in a few years, Congress were to hold hearings in order to adduce evidence of substantial impact on interstate commerce, such evidence could arguably satisfy this part of the inquiry.

If Congress adduces adequate evidence of substantial effect on interstate commerce or can show that it is regulating a channel of interstate commerce, it must then craft federal legislation that complies with state autonomy limits on the federal commerce power. Like the DPPA in *Reno v. Condon*, electronic filing legislation should restrict the ability of states and private individuals to sell or exchange certain court information. However, such legislation must not require "the States in their sovereign capacity to regulate their own citizens" or to enact legislation.[98]

V. The Constitutional Right to Informational Privacy

Although it appears that legislation is the most likely solution to electronic filing privacy problems, there may also be a judicial solution to Internet privacy problems – constitutional protection for informational privacy rights. Although the Supreme Court has not officially recognized such a right, the increasing wealth, speed, and

98. *Id.* at 142.

prevalence of the Internet may force the Court to address privacy concerns and, ultimately, to decide whether or not a privacy right in personal information actually exists.

The right to privacy is not expressly recognized in the Constitution. However, courts do recognize a right to privacy, described over a century ago by Louis Brandeis and Samuel Warren as the "right to be let alone."[99] Although the Supreme Court has made clear that there is no general right to privacy,[100] the Court has recognized a right to privacy in making certain kinds of decisions.[101] For instance, the landmark decision of *Roe v. Wade* established that a woman's right of privacy included the right to terminate her pregnancy.[102] *Roe* also limited the right to privacy to issues involving marriage, procreation, contraception, family relationships, child rearing, and education.[103]

The privacy right implicated in the Internet and electronic filing context is the right to informational privacy: an individual's interest in avoiding disclosure of personal matters.[104] Although the Supreme Court has never explicitly recognized an informational privacy right, the growth of the Internet and increasing privacy concerns will likely prompt the Supreme Court to consider the informational privacy issue. If and when the issue arises, the Court should recognize a limited right to informational privacy. (A limited right to informational privacy would more effectively balance an individual's privacy rights against the public's right to information than would an absolute privacy right, which may run afoul of First Amendment free speech rights.)

Despite the Supreme Court's silence on the subject, some circuit courts have used Justice Stevens' majority opinion in *Whalen v. Roe* to create a right to informational privacy.[105] In *Whalen*, the Court discussed two kinds of privacy interests: "the interest in independence in making certain kinds of important decisions" and "the individual

99. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193 (Dec. 1890).

100. *See* Katz v. United States, 389 U.S. 347, 350 (1967) (stating that there is no "general constitutional 'right to privacy'").

101. *See* GERALD GUNTHER & KATHLEEN M. SULLIVAN, CONSTITUTIONAL LAW 538 (13th ed. 1997).

102. 410 U.S. 113, 153 (1973).

103. *See id.* at 152-53.

104. *See* Whalen v. Roe, 429 U.S. 589, 599 (1977).

105. *Id.* at 599-600

interest in avoiding disclosure of personal matters."[106] It is the latter interest from which some circuit courts have derived the right to informational privacy.[107]

At issue in *Whalen* was a New York law that required physicians to identify patients who took certain kinds of prescription drugs,[108] so that their names and addresses could be recorded in a central computerized database.[109] The Court upheld the statute because the risk of public disclosure of information was minimal: the state statute required stringent security precautions on behalf of the Health Department and imposed criminal liability on anyone who publicly disclosed the information.[110] The Court did not decide whether a broad informational privacy right existed: "We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional or by a system that did not contain comparable security provisions."[111]

Although the Court did not find a violation of an informational privacy right in *Whalen*, the Court acknowledged the privacy dangers inherent in our technologically advanced society.[112] The Supreme Court has never decided a case in which it found that a government regulation violated the constitutional informational privacy right discussed in *Whalen*. However, a number of circuit courts have used *Whalen* to recognize a right to informational privacy.[113] Although it has not happened yet, it is possible that other courts may use a similar analysis to recognize a right to informational privacy in the Internet context.

The Third Circuit in *United States v. Westinghouse* recognized the

---

106. *Id.*

107. *See, e.g.*, U.S. v. Westinghouse, 638 F.2d 570, 580-82 (3d Cir. 1980); Plante v. Gonzales, 575 F.2d 1119, 1132 (5th Cir. 1978).

108. The law sought to prevent overuse and over-prescribing of certain kinds of prescription drugs, which were labeled as "Schedule II" drugs. Schedule II drugs included types of drugs that are dangerous, but prescribed by some physicians for legitimate medical purposes. *See Whalen*, 429 U.S. at 592-93.

109. *Id.* at 593

110. *See id.* at 594-95

111. *Id.* at 605-606.

112. *Id.* at 605.

113. *See, e.g.*, In re Crawford, 194 F.3d 954, 958 (9th Cir. 1999); Doe v. City of New York, 15 F.3d 264, 267 (2d Cir. 1994); United States v. Westinghouse, 638 F.2d 570, 577 (3d Cir. 1980); Plante v. Gonzales, 575 F.2d 1119, 1127-28 (5th Cir. 1978).

individual's right to prevent disclosure of personal information.[114] There, an employer refused to release his employees' medical records to the National Institute for Occupational Safety and Health (NIOSH).[115] The court stated: "There can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection."[116] The court found that such privacy could only be invaded if the "societal interest in disclosure outweighs the privacy interest on the specific facts of the case."[117] The court listed factors to be considered in this balancing test:

> The factors which should be considered in deciding whether an intrusion into an individual's privacy is justified are the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.[118]

Applying the factors, the court found that the societal interest in the occupational safety and health of employees was substantial in relation to the "minimal intrusion into the privacy which surrounds the employees' medical records."[119] However, the court also held that NIOSH should give notice to employees whose medical records it wants to examine.[120] Furthermore, individual employees should be allowed to raise his or her own privacy claim, since it is improper to "assume that an employee's claim of privacy as to particular sensitive data in that employee's file will always be outweighed by NIOSH's need for such material."[121]

Likewise, the Fifth Circuit in *Plante v. Gonzales* recognized the right to informational privacy and applied a similar balancing test to determine when the public dissemination of personal information is

---

114. 638 F.2d 570 (3d Cir. 1980).

115. *See id.* at 572-73.

116. *Id.* at 577.

117. *Id.* at 578.

118. *Id.*

119. *Id.* at 580.

120. *See id.* at 581.

121. *Id.* at 581.

warranted.[122] In *Plante*, five state senators challenged the financial disclosure provisions of Florida's Sunshine Amendment on the grounds that it violated their right to privacy.[123] The court recognized the importance of financial privacy,[124] but found that "[t]he public interests supporting public disclosure for these elected officials are even stronger."[125]

The Fourth Circuit in *Walls v. City of Petersburg* also recognized the right to informational privacy.[126] The court, however, severely limited the right by holding that there could be no violation of an informational privacy right, unless the information itself implicated a fundamental right.[127] In *Walls*, a government employee declined to answer four questions on a questionnaire, including the following: "Have you ever had sexual relations with a person of the same sex?"[128] The court found that the employee did not have a right to keep that information private because there is no recognized right to homosexual conduct: "The Court [in *Bowers v. Hardwick*] explicitly rejected the proposition that any kind of private sexual conduct between consenting adults is constitutionally insulated from state proscription."[129] However, the court also acknowledged the privacy problems associated with technological advances:

> In the past few decades, technological advances have provided society with the ability to collect, store, organize, and recall vast amounts of information about individuals in sophisticated computer files. This database capability is already being extensively used by the government, financial institutions, and marketing research firms to track our travels, interests, preferences, habits, and associates. Although some of this information can be useful and even necessary to maintain order and provide communication and convenience in a complex society, we need to be ever diligent to guard against misuse. Some information still needs to be private, disclosed to the public only if the person voluntarily chooses to disclose it.[130]

In contrast, the Sixth Circuit in *J.P. v. DeSanti* completely

---

122. 575 F.2d 1119, 1134-35 (5th Cir. 1978).

123. *Id.* at 1121-22.

124. *See id.* at 1135.

125. *Id.* at 1136.

126. 895 F.2d 188, 193 (4th Cir. 1990).

127. *See id.*

128. *Id.*

129. *Id.*

130. *Id.* at 194-95.

rejected the right to informational privacy.[131] In that case, juveniles brought suit to prevent the compilation and dissemination of information by state probation authorities.[132] The court stated: "We do not view the discussion of confidentiality in *Whalen v. Roe* as . . . creating a constitutional right to have all government action weighed against the resulting breach of confidentiality."[133] The court concluded that the right to privacy is limited to fundamental rights.[134] Since no fundamental right was implicated in *J.P v. DeSanti*, there could be no corresponding right to privacy.[135] Furthermore, the court noted that "none [has] cite[d] a constitutional provision in support of [the existence of a constitutional right to nondisclosure of private information]."[136]

A. Recognition of a Limited Constitutional Informational Privacy Right

We live in an "information age," where people are more concerned than ever about access and misuse of their personal information.[137] Although the Supreme Court has not explicitly recognized a constitutional right to informational privacy, some circuit courts have already acknowledged such a right. Because Internet growth and increased access to information will persist, the Supreme Court may soon have to decide whether an informational privacy right actually exists. If the Supreme Court is faced with this issue, it should recognize a limited constitutional right to informational privacy right.

If the Court recognizes an informational privacy right, this right should exist narrowly and evolve slowly to accommodate changing societal and legal climates. A broad, blanket right would be both impractical and unlikely, given that the courts have generally recognized an informational privacy right only in cases where a government entity has required involuntary disclosure of personal information. Furthermore, applying an informational privacy right to disclosure of every instance where personal information is requested would be overbroad and contrary to other well-settled principles. For

---

131. 653 F.2d 1080, 1088-89 (6th Cir. 1981).

132. *See id.* at 1081-82.

133. *Id.* at 1088-89.

134. *See id.* at 1088-90.

135. *Id.*

136. *Id.* at 1090.

137. *See* Brin, *supra* note 45, at 25-26.

example, the public has an interest in government disclosure of information – the notion that the public has a right to know. Thus, the informational privacy right should be limited to situations where the government (or state actor) requires the involuntary disclosure of personal information. In such cases, the court should apply a balancing test to determine whether the invasion of privacy is warranted; if the government interest in disclosure outweighs the individual's privacy right, the disclosure is warranted. This approach is ideal because it properly weighs society's interest in the information against the individual's right to confidentiality, and does not undermine the current state of privacy jurisprudence.

B. Application of the Limited Right to Electronic Filing

Although a constitutional informational privacy right will be helpful in many Internet contexts and provide a useful constitutional foundation to privacy claims, it may not prove useful in the electronic filing context for two reasons. First, in order for the informational privacy right to apply, the individual's disclosure must be "involuntary." In the electronic filing context, it is debatable whether litigants provide information in court filings "involuntarily." It appears that plaintiffs provide their information voluntarily by initiating lawsuits. However, defendants must disclose information to respond to plaintiff's allegations and to avoid default judgment. Thus, one could argue that defendants involuntarily provide court information. Nevertheless, even if the "involuntary" prong is satisfied for defendants, it would be both impractical and inefficient to require courts to engage in a balancing inquiry at the outset of every lawsuit. Because of the difficulty in applying a constitutional informational privacy right to electronic filing, it appears that legislation would be a more practical solution to electronic filing problems.

Conclusion

Courts are moving toward a uniform electronic filing system that increases efficiency, cuts costs, and improves access to the judicial system.[138] In the past few years, Internet use has grown rapidly. New technology and increased access of information is making everyday tasks and transactions easier and more efficient. The Internet is

138. *See* Daitch & Ytterberg, *supra* note 2, at 97. *See also* Wells & Winger, *supra* note 24, at 1.

changing the way society thinks, interacts, and conducts business.

Uniform electronic filing is the first step to a more efficient judicial system. Once a uniform system is in place, on-line users will be able to access court documents freely. However, the efficiency of electronic filing has a price – with the ease and convenience of the Internet comes a loss of informational privacy. With this loss of informational privacy comes an increase in potential misuse of information. Thus, this "information age" has resulted in a need to curtail public access to confidential information.

Because we live in a society where information is valuable and plentiful, there is an increasing need to explore new ways of protecting personal information. Uniform state legislation is one way to create guidelines and standards for state court filings. Federal legislation of electronic filing is another possibility. In enacting federal legislation, Congress may use its Commerce Clause power to regulate the sale and use of information obtained from state court electronic filings. Such legislation would depend upon the Government's ability to demonstrate that electronic filing has a "substantial effect" on interstate commerce or that electronic filing on the Internet constitutes a "channel" of interstate commerce.

Although the Court has not yet explicitly recognized a constitutional right to informational privacy, the current nature and growth of the Internet may force the Court to consider whether such a right exists. Recognition of a limited informational privacy right may help individuals protect their personal information. Such a right should apply in situations where the government is requiring involuntary disclosure of personal information. It is presently unclear whether litigants "involuntarily" disclose their personal information. Whether applicable to electronic filing or not, a limited informational privacy right will provide a strong constitutional backdrop for the many Internet privacy claims that will undoubtedly come to light.