DIGITAL SIGNATURES: WILL GOVERNMENT REGISTRATION OF USERS MEAN THAT ANONYMITY IN TRANSACTIONS ON THE INTERNET IS FOREVER LOST?

DEBORAH L. MORGAN*

Internet consumers have long taken anonymity for granted. Increases in commerce in cyberspace have created a need for consumer protection measures on the Internet. Digital signatures seek to meet this need in two important ways. First, they provide validation of data and identity to ensure that information has not changed between origin and reception. Second, they validate identity if pseudonyms or other anonymous processes are not used. This note argues that digital signature laws must be carefully crafted with consumer protection in mind. Problems may arise as governments, both state and federal, opt to serve as both authentication agencies and parties to electronic transactions. Depending on how digital certificates are issued, governments could have the capability to connect actual consumer identity information with digital signatures, thereby defeating the signatures' intended purpose. In addition, this note compares legislation from several states, as well as European legislation, and suggests that consumers and legislators need to make consumer privacy central to any viable digital signature legislation.

I. INTRODUCTION

Americans take anonymity for granted in their daily lives—though each knows they might be followed any time they browse from store to store in the mall or that information might be copied from a credit card handed over at dinner, or even that information might be gleaned from marketing surveys submitted to companies over the phone. It is even easier to feel anonymous while browsing the Internet from the seeming privacy of one's own home,[1] and for this reason, Internet anonymity has perhaps been taken for granted more than any other form. From a user's

* *I thank Douglas Hahn and Professor Bruce Smith for inspiring and tweaking this topic, and I am especially indebted to Mark Anderson, of the State of Illinois, for his technical expertise and input throughout the revision process and to Deb Kelley for all of her help. Also, I am grateful to my family for supporting and encouraging me when I have needed it most.*

1. *See* Marsha Cope Huie, Stephen F. Laribee, & Stephen D. Hogan, *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 463 (2002).

perspective, it appears that one can see the items in the online stores, but that he or she cannot be seen in return. However, the likelihood of being followed and identified is far greater when shopping online than in a local mall.[2] For instance, consider an example offered by Professor Jerry Kang:

> [I]magine the following two visits to a mall, one in real space, the other in cyberspace. In real space, you drive [there] . . . and stroll through corridors of inviting stores. Along the way, you buy an ice cream cone with cash. You walk into a bookstore and flip through magazines . . . buy a friend a silk scarf with a credit card . . . . [N]umerous people interact with you and collect information along the way . . . . [F]ellow visitors visually collect information about you, if for no other reason than to avoid bumping into you. But such information is general—e.g., it does not pinpoint the geographical location and time of the sighting—is not in a format that can be processed by a computer, is not indexed to your name or another unique identifier, and is impermanent, residing in short-term human memory. You remain a . . . stranger. One important exception exists: The scarf purchase generates data that are detailed, computer-processable, indexed by name, and potentially permanent.[3]

Unlike this real world example, Internet transactions allow a more detailed record of the sites you browse.[4] In cyberspace, "you are invisibly stamped with a bar code as soon as you venture outside your home."[5] Even without making a purchase, the fact that you glanced at, browsed through, or looked at a page long enough to thoroughly examine it can be recorded.

It is likely that, as Americans gain knowledge about this stealthy surveillance by commercial companies, a feeling of helplessness will also arise.[6] It is easy to imagine that nothing can be done to halt the masses

2. According to one study, ninety-two percent of online companies collect personal identifiable information from site visitors. *See* Karl D. Belgum, *Who Leads at Half-Time?: Three Conflicting Visions of Internet Privacy Policy*, 6 RICH. J.L. & TECH. 1, ¶ 11 (1999) (citing a Federal Trade Commission study from 1998), *at* http://law.richmond.edu/jolt/v6i1/belgum.html.

3. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198 (1998).

4. *See id.* at 1199. *But see* Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 97 (2002) (noting that the sharp distinction Kang suggests between real world and online observation may be blurring, due to the increased use of video cameras but stating that video cameras still provide less personally identifiable information than can be obtained by watchers online).

5. Kang, *supra* note 3, at 1198.

6. *See, e.g.,* Christopher F. Carlton, *The Right to Privacy in Internet Commerce: A Call for New Guidelines and the Creation of an Independent Privacy Commission*, 16 ST. JOHN'S J. LEGAL COMMENT. 393, 394 (2002) (stating that "an overwhelming number of Americans have reported that they have lost the ability to control the collection and dissemination of their personal information and that the current laws do not do enough to protect their right of privacy") (citing *Business Week/Harris Poll: Online Insecurity*, BUS. WK., Mar. 16, 1998, *available at* http://www.businessweek.com/1998/11/b3569107.htm).

of "watching" companies. As commerce becomes more and more prevalent on the Internet, the need for secure methods of communication grows, as well.[7] Though features such as digital signatures might seem to be a protection for consumers, they will not necessarily benefit consumers unless laws are carefully drafted with consumer anonymity and privacy in mind. Many digital, or electronic, signature laws have focused more on benefiting companies hoping to do an increasing amount of business on the Internet and less on protecting consumer privacy. Government agencies also play an increasing role in Internet surveillance. The government may be attempting to prevent crime, such as fraud or child pornography, but a growing number of agencies are simply attempting to make it easier for Internet users to do business with the government and with each other.[8] Though many welcome this advance in government agency technology because of the convenience of doing business on the Internet, there are reasons for the public to fear the government's involvement as a potential avenue for further losses of privacy and anonymity in Internet communications.

This note argues that digital signature legislation, as currently drafted by both the states and the federal government, does not protect the anonymity of users to the extent necessary for projected uses of digital signatures, including voting[9] and expression of political and other viewpoints, to become a reality. A user uses a digital certificate, along with an accompanying digital signature, to assure an end user, such as a commercial entity, that the sender is, in fact, who she claims to be and that she has the necessary authority to do the action attempted.[10] The user chooses to digitally sign the page, while the certificate allows the end user to verify the signature's credentials. Use of a digital signature requires the sender to register with an entity that verifies initial information, much like driver's license facilities verify identity for the first time, and that entity then provides the user with a password to use for digital signatures. The verification entity also ensures that the user's information is correct and still valid whenever the user uses her digital signature on the Internet.[11] Part II analyzes the scope of anonymity protection before the Internet and the anonymity offered by the Internet. Part III discusses digital signatures, including the components necessary for digital

7. *See, e.g.,* Eugene Yannon, *Protecting Consumer Rights*, MD. B.J., Mar./Apr. 2002, at 40, 43 (citing the Information and Security Committee of the A.B.A. Section of Science and Technology Law public key infrastructure assessment guidelines, portions of which were used to solicit comments in late 2001).

8. *See, e.g.,* Sarah L. Roberts-Witt, *Solving the PKI Dilemma*, STATETECH, Apr. 2002, at 17–19 (discussing the services the states of Washington and Illinois plan to offer users).

9. It is important to note that, while one's vote should be anonymous, the act of voting itself must necessarily be tracked to protect against voting fraud. In the case of voting, encryption would also be required.

10. *See infra* notes 69–104 and accompanying text. The digital certificate could contain the authorization information, if necessary.

11. *See infra* notes 81–87 and accompanying text.

signatures to work. Part IV identifies a difference between European and American legislation and suggests that some further steps may be needed to assure that American laws are adequately protecting consumers, rather than the commercial and governmental entities that are pushing the digital signature laws and capabilities forward. Part V first discusses the federal law regarding digital and electronic signatures that is currently in place and examples of state statutes based on that law. It then highlights and discusses the policy, and procedural, differences between state statutes that may lead to lower anonymity protection for residents of some states than others. Part V also includes a discussion of the considerations that must be taken into account when protecting citizens' anonymity on the Internet. Part VI argues that consumers and citizens need to be aware of the importance of digital signature legislation and that legislation needs to be drafted to protect and secure the rights of anonymity and privacy on the Internet for the future.

II. THE PAST PROTECTION OF ANONYMITY, FREE SPEECH, AND THE POTENTIAL FOR FREE SPEECH AND ANONYMITY ON THE INTERNET

Many have spoken of the "right to privacy" citizens expect from their governments (and even private businesses) in recent years. Privacy has been called "the right to be let alone"[12] and has been loosely classified under the First Amendment.[13] Many people are unconcerned that their telephone numbers are readily available (and indeed, they list them in phone books), but they do not want certain individuals, such as telemarketers, to call them.[14] Consumers also may not mind the profiling that is done to increase the likelihood that advertisements they see will actually feature products that interest them. There are times, however, when people may wish to not have those profiles linked with their names. Records that may be available include "health records; credit history; banking transactions; local and long-distance telephone calls; pay-per-view, VCR rental, cable, and other video records; records of an Internet service provider; and purchases made through direct mail or telephone ordering."[15] There may also be times when one wishes to speak without providing a name, or through the use of a pseudonym. For example,

12. Olmstead v. United States, 277 U.S. 438, 478 (1928).

13. *See, e.g.*, JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW § 14.26 (4th ed. 1991) ("The first amendment has been held to protect some rights to privacy in speech or association.").

14. *See, e.g.,* Hal R. Varian, *Economic Aspects of Personal Privacy, in* THEORY OF MARKETS AND PRIVACY, http://www.ntia.doc.gov/reports/privacy/selfreg1.htm (last visited Apr. 20, 2004). This article suggests that in the case of telemarketing, it is really the attention of the recipient of the phone call that is guarded, not the information (the telephone number) itself. *Id.* at *2. Telephone numbers are therefore contrasted with personal information that one simply does not want revealed, such as health or financial information. *Id.*

15. Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in* THEORY OF MARKETS AND PRIVACY, *supra* note 14.

people calling talk-radio programs to complain about local politicians might not want to give their real names. They may want their viewpoints known, but not linked to their names. They may wish either to be anonymous or use an assumed name. People might be less willing to speak at all, if unable to protect their identities in this way. Similar examples, and concerns, exist for Internet speech.

A. Origins of the Right to Anonymity Within the First Amendment

Because of the wishes to be left alone and to speak without providing true identity, anonymity, pseudonymity, and privacy in general have been topics of much debate in both recent and more distant years. The Supreme Court has protected anonymity, as a necessary part of the First Amendment's free speech guarantee, for such activities as distributing[16] and receiving[17] political literature, and for distributing anonymous literature.[18] In these situations, the Court has cited the history of anonymity in connection with free speech, noting that the famed and influential Federalist Papers were anonymous documents.[19] Even the freedom of association has been afforded anonymity rights, protecting the ability to secretly belong to political and social organizations.[20] As many organizations establish an online presence and increasingly depend on the Internet for recruitment and newsletter purposes, their members' ability to remain anonymous in their online activities becomes important, especially for political groups.

However, the Court has not only afforded protection to anonymous political and social activities, but it has also afforded the same protection for literature in general, such as an author's right to use a nom de plume.[21] The Court has noted that "fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much as one's privacy as possible" may motivate one to publish anonymously and that, "[w]hatever that motivation may be, [for literary

16. *See* Buckley v. ACLU, 525 U.S. 182 (1999) (holding a Colorado statute requiring initiative petition circulators to wear identification badges unconstitutional); *see also* Talley v. California, 362 U.S. 60 (1960) (finding a California ordinance forbidding distribution of anonymous handbills unconstitutional).

17. *See* Lamont v. Postmaster Gen., 381 U.S. 301 (1965) (holding the requirement that those receiving communist information notify the post office that they intend to receive such material unconstitutional).

18. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) (finding Ohio's statute banning distribution of anonymous campaign literature unconstitutional); *see also* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150 (2002).

19. *See, e.g., McIntyre*, 514 U.S. at 343 n.6.

20. *See* Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539, 543–44 (1963) (holding a demand by the state for the NAACP to turn over documents stating whether suspected communists were also NAACP members unconstitutional and noting the chilling effect exposure to the community might have on members of NAACP); Shelton v. Tucker, 364 U.S. 479, 488 (1960) (finding an Arkansas statute requiring teachers at state-supported schools to file a list of all organizations to which they belonged or which they supported during the last five years unconstitutional).

21. *McIntyre*, 514 U.S. at 341 n.4.

works], the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry."[22] The Court also stated that anonymity may be the best way for unpopular authors to reach an audience with their points of view.[23] Other courts have been confronted with the question of whether anonymity should be protected when information is sought from a third party.[24] Thus, courts have sought to protect anonymity in connection with speech in the real world for a variety of reasons.

B. Application of Anonymity Protection to Internet Communications

These rationales for protecting anonymity in connection with real world speech are no less important for Internet communications. "Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders and newsgroups, the same individual can become a pamphleteer."[25] Online entities have touted the benefits of the level of anonymity that is possible online. Many contend that "[i]ndividuals should be able to conduct certain types of transactions online without identifying themselves."[26] In fact, one online organization has stated that "[a]nonymity is essential to protect free speech."[27] The Internet has provided a new sort of anonymity—allowing users to travel and speak without indicating even such basic features as race, gender, age, economic status, or physical ability that are often clearly apparent in the real world.[28] The Internet thus offered a more true sense of anonymity than that often possible in the real physical world.

Professor Lawrence Lessig stated that the anonymity initially present on the Internet was due to the fact that the Internet was originally made "for research, not commerce."[29] Still, growth and user-friendly changes to the Internet are likely due to the intervention of private and

22. *Id.* at 341–42.

23. *Id.* at 342.

24. *See* Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1047 (Colo. 2002), *as modified on denial of reh'g* (Apr. 29, 2002) (holding that a search warrant for information about an individual's book purchases from a bookseller could not be enforced without meeting a higher standard than that generally used for search warrants—a heightened need for the purchase records). *But see* Pappas v. Giuliani, 290 F.3d 143, 151 (2d Cir. 2002) (holding that police officer's free speech rights were not violated when city terminated him after he used envelopes—which the city used to trace his identity—originally sent to him with charitable solicitations to distribute antiblack and anti-Semitic materials).

25. Reno v. ACLU, 521 U.S. 844, 870 (1997).

26. Hahn & Layne-Farrar, *supra* note 4, at 88.

27. The World Wide Web Consortium consists of companies developing procedures and standards for practices on the world wide web. *See* World Wide Web Consortium, *About the World Wide Web Consortium*, *at* http://www.w3.org/Consortium. The consortium has stated that anonymity may protect one's life or harmony, such as for political disagreements, controversial publications, reporting human rights violations, etc. *Id.*

28. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 65 (1999).

29. *Id.* at 39.

commercial actors, who strove to reach more and more viewers and potential consumers.[30] Lessig notes that as commerce on the web has developed, much of the ability to remain anonymous has been eroded.[31] Commercial entities cannot afford to deal with complete unknowns; they need to ask not only for identity, but also authenticate the identities of the individuals with whom they transact.[32] Lessig has stated that because of these commercial needs, anonymity on the Internet is shrinking.[33] Companies are using "cookies" to track consumer movement on the Internet.[34] Cookies may reside on the computer of a user and save and send information, for example the user's name, personal information, purchases on the Internet, and sites visited, to the cookies' originator. Most of this information transmission occurs without the user's knowledge.[35]

In the real world, of course, such copying of your personal information could occur—your name and address could be stolen when you use your credit card, and you could be followed from store to store to see where you shop, even if you have not purchased anything.[36] It is clear, however, that on the Internet this information can be tracked with ease and with much less cost than in the real world.[37] Because much of privacy and anonymity law appears to be based on what people have become accustomed to,[38] it appears to be a real danger that anonymity may

30. Bradford L. Smith, *The Third Industrial Revolution: Policymaking for the Internet*, 3 COLUM. SCI. & TECH. L. REV. 1, 13 (2001), *at* http://www.stlr.org/cite.cgi?volume=3&article=1; *see also* Ari Lanin, *Who Controls the Internet? States' Rights and the Reawakening of the Dormant Commerce Clause*, 73 S. CAL. L. REV. 1423, 1423 (2000).

31. LESSIG, *supra* note 28, at 39.

32. Lessig defines "authentication" as "the process by which aspects of your identity become known." *Id.* at 31. He states that some can be learned only through communication with the person, while others can be determined from "credentials" provided by an outside institution, which provides validity for the document. *Id.* These include drivers' licenses, transcripts, deeds, etc. *Id.*

33. *Id*. at 30–31.

34. *See* Belgum, *supra* note 2, ¶ 8.

35. *See, e.g.,* Hahn & Layne-Farrar, *supra* note 4, at 135–36. While a simple function allows cookies to be turned off, few Internet users use this function, choosing the convenience of freely surfing the web over the inconvenience of being denied access to certain sites if they choose not to accept cookies.

36. *See supra* text accompanying note 3.

37. *See* Carlton, *supra* note 6, at 403–05; Hahn & Layne-Farrar, *supra* note 4, at 86.

38. *See* Katz v. United States, 389 U.S. 347, 351–53 (1967) (holding that the Fourth Amendment's protection extends to situations in which one has an expectation of privacy if that expectation is reasonable). The Supreme Court's holding in *Kyllo v. United States*, 533 U.S. 27 (2001), went further than *Katz*, with Justice Scalia stating that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Id.* at 40 (holding the use of thermal imaging devices to detect heat sources used for growing marijuana unconstitutional because of the information provided about the inside of the home). Businesses do not face the same limitations as government criminal investigators. "The United States Constitution does not protect a person's right to privacy with respect to intrusions by private parties." Richard A. Mann & Barry S. Roberts, *Cyber Law: A Brave New World*, 106 DICK. L. REV. 305, 347 (2001). The use of digital signatures may increasingly involve the government playing a role in consumer transactions, meaning information may be gained in that context, rather than in criminal investigations.

not be well-protected on the Internet if consumers are not able to effectively curtail such information gathering activities on the Internet.

While you might willingly share your identity with some, it is an aspect of yourself that you may prefer to keep private from others.[39] Issues of anonymity on the Internet are frequently reaching the courts.[40] Because many Internet user names are pseudonyms, Internet Service Providers (ISPs) are inundated with requests for the true identities of users the seekers claim have wronged them in one way or another.[41] Both civil litigants and government entities are seeking identities of users and attempting to investigate cybercrimes.[42] The Supreme Court has noted the various types of communication and ease of dissemination of information that is possible on the Internet and mentioned that there is "no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium."[43] Other courts have noted that statutes requiring identification of users on the Internet are invalid due to the protections of anonymity afforded in the offline world.[44] Of course, as in the real world, others may be harmed by users who are anonymous or pseudonymous, and there have been claims of defamation and other complaints resulting from Internet conduct of unidentifiable members.[45]

39. *See* Kang, *supra* note 3, at 1203–05.

40. *See, e.g.,* Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (W.D. Wash. 2001); *In re* Am. Online, Inc., 52 Va. Cir. 26 (2000), No. 40570, 2000 WL 1210372, at *1 (Jan. 31, 2000).

41. *See* McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998) (granting an injunction against the government using information it obtained about a Navy officer from an online service provider without identifying that it was a government entity, in violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2701). "In these days of 'big brother,' where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights be strictly observed." *Id.* at 220; *see also In re Am. Online, Inc.*, 52 Va. Cir. 26, 2000 WL 1210372, at *1 (involving a civil suit by a company wanting to learn the identity of AOL subscribers it wished to name in a suit).

42. *See* David L. Sobel, *The Process That "John Doe" Is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 VA. J.L. & TECH. 3, ¶ 2 (2000) (commenting that the discovery process is being used to "pierce the veil of online anonymity"), *at* http://www.vjolt.net/vol5/symposium/v5i1a3-Sobel.html; *see also Doe*, 140 F. Supp. 2d 1088 (allowing a civil defendant to proceed under a pseudonym when identity was not central to the plaintiff's claim); *McVeigh*, 983 F. Supp. at 219–20 (finding it likely that there had been a violation of the Electronic Communications Privacy Act when the government asked for, and received, an AOL user's true identity and used it to discharge McVeigh for his sexual orientation); *In re Am. Online, Inc.*, 52 Va. Cir. 26, 2000 WL 1210372, at *7 (finding that for a civil litigant to receive the identity of a user, the court must be satisfied (1) of the pleadings or evidence, (2) that the party wanting the subpoena has a legitimate good faith basis to state that the conduct is actionable in that jurisdiction, and (3) that the identity is centrally needed to advance the claim).

43. Reno v. ACLU, 521 U.S. 844, 870 (1997).

44. ACLU v. Miller, 977 F. Supp. 1228, 1232–35 (N.D. Ga. 1997) (invalidating a Georgia statute that prohibited falsely identifying oneself in setting up a home page, electronic mailbox, or other electronic information storage bank, despite the state's argument that the statute was limited to prevention of fraud). The court determined that, "[o]n its face, the act prohibits such protected speech as the use of false identification to avoid social ostracism, to prevent discrimination and harassment, and to protect privacy." *Id.* at 1233.

45. See *In re Am. Online, Inc.*, 52 Va. Cir. 26, 2000 WL 1210372, at *1, in which a plaintiff company allegedly harmed by the speech of anonymous Internet users requested the identity of the users and simultaneously requested to remain anonymous in the proceedings to protect itself from reputation or economic harm as a result of the suit.

Users may maintain multiple Internet identities and accounts as a method to keep anonymity or at least pseudonymity. Though anonymity in purchasing capabilities has largely been lost on the Internet, it is still possible to send anonymous communications. Presently, parties wishing to communicate anonymously may use remailers, which mask the original sender of the message.[46] This allows a user to communicate without being identified as the speaker.

C. Privacy and Anonymity Concerns on the Internet

Differentiating between privacy and anonymity concerns is difficult because both are largely intertwined on the Internet. Keeping your identity secret, and thus remaining anonymous, protects information that you may have an interest in keeping private or secret. Professor Jerry Kang differentiates between several types of privacy.[47] First, he identifies privacy involving "physical space," noting that it is important to most people to keep their territory free from invasion, as is protected by the Fourth Amendment idea of curtilage around a dwelling.[48] Next, Kang describes the privacy of being able to "make certain significant decisions without [state] interference."[49] Finally, Kang identifies privacy regarding the flow of personal information, including the processing of information that is identifiable to the individual.[50] Kang notes that these three types of privacy overlap, such as when one has decisional privacy, it will keep her from having to justify a choice she made, keeping her informational privacy intact.[51] Anonymity may be important in each of these types of privacy, as identity disclosure may be a source of concern for certain transactions or discussions.

Kang also identifies two types of anonymity relevant to his privacy discussions.[52] He first discusses anonymous communications, which are those that result when anonymous remailers are used.[53] The use of remailers is likely to protect the anonymity of communications of a political nature because, at the moment, the use of digital signatures for such communications has not yet been contemplated.[54] As identity becomes

46. Gia B. Lee, *Addressing Anonymous Messages in Cyberspace,* 2 J. COMPUTER-MEDIATED COMM. 1 (June 1996), *at* http://www.ascusc.org/jcmc/vol2/issue1/anon.html.

47. Kang, *supra* note 3, at 1202–05.

48. *Id.* at 1202.

49. *Id.* at 1202–03. Kang states that this includes one's ability to make a decision about abortion without interference. *Id.*

50. *Id.* at 1203.

51. *Id.* at 1203–04. Kang notes that the reverse is also true—that keeping a fact such as pregnancy private (informational privacy) can allow one to have decisional privacy. *Id.* at 1203.

52. *Id.* at 1242.

53. *Id.* at 1242–43.

54. It appears this will remain the case at least so long as liability for slanderous statements belongs to the person posting the statements. The Communications Decency Act, 47 U.S.C. § 230(c)(1) (2000), provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." This has

more and more important in protecting businesses from losses due to unverified identity in transactions, it will become easier for more entities to require digital certificates or signatures to verify the source of postings and information. Businesses not worried about ensuring receipt of payment may be temporarily prohibited from using digital signature technology due to the cost of implementation, but this may not be an issue if government provides digital signature capability to its citizens.[55] Next, Kang discusses the possibility of anonymous payment systems with public key encryption.[56] These systems allow payments to remain anonymous through a system using "blind" digital signatures, which provide no more personally identifiable information than a cash transaction does.[57]

Congress has dealt with the issue of an ISP having to release information to the government, but carefully left ISPs free to release the information to private entities.[58] Though much of the Supreme Court's focus in anonymity cases appeared to involve the government's regulation of identity, the Court recognized the importance of anonymity for reaching one's audience in literary or other creative works.[59]

Many have identified problems associated with Internet anonymity. Lessig noted that anonymity may also allow a speaker, under the cloak of a pseudonym, to attack others without fear of reprisal, whereas in real life his identity would have been known and social norms would likely have softened the effect of a disagreement.[60] Ku Klux Klan members have also spoken out freely on the Internet, due to the anonymity afforded them, allowing retribution-free communication and possibilities for targeted or broad harassment.[61] The Supreme Court also has noted that anonymity brings with it the potential of abuse, but stated that "our

been interpreted to mean that Internet service providers are not liable for content posted by their users. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997).

55. *See infra* Part V.G.

56. Kang, *supra* note 3, at 1243–44.

57. *Id.*

58. Under the Electronic Communications Privacy Act of 1986 (ECPA), "a provider of electronic communication service . . . may disclose a record or other information pertaining to a subscriber or customer of such service (not including the contents of the communications covered by subsection (a) or (b) of this section) to any person other than a governmental entity." 18 U.S.C. § 2703(c)(1)(A) (2000). Thus, the identity of a subscriber, as included in a record, is not protected from private disclosure. For the government to receive the information, however, a warrant, court order, or consent is required. *Id.* § 2703(c)(1)(B)(i)–(iii). A violation of this part of the act may lead to exclusion of the evidence in a government case. *See* McVeigh v. Cohen, 983 F. Supp. 215, 220 (D.D.C. 1998). There are no similar remedies when private parties are the recipients of such disclosures, as they are not forbidden by the statute.

59. *See supra* notes 121–23 and accompanying text.

60. *See* LESSIG, *supra* note 28, at 80–82; *see also* Kang, *supra* note 3, at 1218–20; Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 1, ¶ 69-82 (Dec. 2000), *at* http://stlt.stanford.edu/STLR/Articles/00_STLR_2/index.htm.

61. Lee, *supra* note 46, at *3. "[A]s a former Ku Klux Klan leader has admitted, 'The access is anonymous and there is unlimited ability to communicate with others of a like mind.' Anonymity facilitates not only the general spread of messages of hatred, but also targeted forms of personal harassment." *Id.*

society affords greater weight to the value of free speech than to the dangers of misuse."[62]

It seems unlikely that the Court would have supported the regulations noted above if it had simply required revealing identity to a third party rather than the government.[63] The Court did not seem to protect individuals solely from government intrusion or knowledge of their acts, but rather from community knowledge as well due to the possibilities of censorship only indirectly sanctioned by the government.[64] The Court claimed to protect the anonymity rights of the individuals who engaged in political or creative speech.[65]

Commentators have already noted that because of the lack of privacy on the Internet, users' activities are already being curtailed.[66] "Unlike the casual observation that people encounter from passers-by each day . . . the constant surveillance engendered by Internet technologies 'leads to self-censorship.' Knowing we are watched, we behave differently."[67] Perhaps users fail to click on web sites with topics that they would like to learn more about for fear of having that topic added to an interest profile a company is creating for that individual. Even this curtailing is an undesirable effect of the feeling that privacy is incomplete on the Internet. Most authors, including the one quoted above, however, complain of commercial entities as the source of the privacy violations.[68] Few speculate on the effects, or likely effects, of government surveillance or even the government's mere ability to easily survey citizen activities, transactions, or speech on the Internet. The chilling vision inspired by these capabilities is that of "Big Brother,"[69] a government able to see more and more into citizens' personal interactions. Worse still, digital certificates and signatures, which are heralded as protective devices for

62. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (citing Abrams v. United States, 250 U.S. 616, 630–31 (1919) (Holmes, J., dissenting)). There have also been suggestions that post-September 11, 2001, the protections of privacy that would allow terrorists to mask their identities on the Internet are undesirable. *See* Peter Lewis, *The Tools of Freedom and Security*, FORTUNE, Oct. 29, 2001, at 195. Lewis argues that the tools that allow monitoring merely hurt personal privacy and do not actually prevent terrorists from acting. *Id.*

63. *See, e.g., In re* Am. Online, Inc., 52 Va. Cir. 26 (2000), No. 40570, 2000 WL 1210372, at *6 (Jan. 31, 2000) ("To fail to recognize that the First Amendment right to speak anonymously should be extended to communications on the Internet would require this Court to ignore either United States Supreme Court precedent or the realities of speech in the twenty-first century.") (citing Reno v. ACLU, 521 U.S. 844, 870 (1997); *McIntyre*, 514 U.S. at 342).

64. *See McIntyre*, 514 U.S. at 357; *see also supra* note 19 and accompanying text.

65. *See McIntyre*, 514 U.S. at 342–43; *supra* text accompanying notes 15–17, 20.

66. Hahn & Layne-Farrar, *supra* note 4, at 88 (referring generally to GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949)).

67. *Id.; see also* Kang, *supra* note 3, at 1216.

68. *See* Hahn & Layne-Farrar, *supra* note 4, at 87; Kang, *supra* note 3, at 1201 ("An important limit to my project is that it does not examine how privacy may be violated by the state in the course of, for example, doling out public benefits, collecting taxes, or deterring crime in and through cyberspace—although these, too, present critical social issues.").

69. *See* Hahn & Layne-Farrar, *supra* note 4, at 94.

consumers in online transactions,[70] may better enable governments to be aware of citizens' online activities.

III. DIGITAL SIGNATURES—REQUIREMENTS AND USES FOR INTERNET COMMERCE AND COMMUNICATION

Digital signatures[71] could help consumers and citizens protect their anonymity. The usefulness of digital signatures may depend, however, on whether the laws creating them are crafted with consumers' or businesses' desires in mind, and whether the legislature has considered how those laws relate to the provision of government services through online media. Digital signatures provide businesses with a method of authenticating a user based on verification through other entities. Digital signatures became a viable option with the encryption capabilities provided by asymmetric cryptography.[72] This encryption technique provides each user with a key pair, including both public and private encryption keys.[73] In contrast, symmetric cryptography uses only one key to both encrypt and decrypt the message.[74] Unlike symmetric key encryption, which poses a risk that the single key will be lost or intercepted,[75] asymmetric encryption allows for only the user's public key to be used for encryption.[76] The private encryption key remains secure with the user.

This encryption, however, does not provide all that is necessary for a recipient to be assured of the sender's identity. A digital signature is "an item of data accompanying a communication used to authenticate its sender and to ensure its integrity."[77] The "hash function," which is the mathematical processing of a message or content, puts out "a relatively small piece of data [called the message digest] that is unique to the mes-

70. *See, e.g.,* LESSIG, *supra* note 28, at 42.

71. A "digital signature" is an authentication method involving hashing. Stephen S. Wu, *Digital Signatures, Authentication, and Secure E-Commerce*, ILL. INST. FOR CONTINUING LEGAL EDUC. § 10.6 (2002). Other electronic signature methods involve biometric devices or smart cards, but those methods will not be dealt with in this note despite the anonymity concerns that they may present. *See id.* § 10.3. Because a digital signature is a subset of electronic signatures, both terms will be used throughout this note.

72. *Id*. § 10.5.

73. A key pair is made up of mathematically related numbers. *Id.* The private key is composed in part by two large prime numbers. *Id.* These numbers are multiplied to produce a number that comprises part of the public key. *Id.* It is extremely difficult to work backward from this large number to determine the original two prime numbers. *Id.*

74. The noted "Caesar Cipher," in which a message was encoded by changing the intended letter to the letter three letters ahead in the alphabet, as in switching *A* to *D*, was an example of symmetric cryptography, because the end user knows the single key (that he must move each letter three spaces back to decode the message). *Id.* Anyone who then stumbles across the key can decrypt that message. *Id.* The key is then intended to be a shared secret between only the message sender and recipient. *Id.*

75. Because it is not feasible to meet in person and in relative secrecy, as Caesar might have met with his generals to give them the decryption key he devised, the key must often be sent to the recipient, and the likelihood of interception is greater. *Id.* § 10.9.

76. *Id.*

77. *Id.* § 10.10.

sage."[78] Therefore, if any changes are made to the message, the output—or message digest—of the hash function will be different.[79] Digital signature software creates the digital signature by using the hash function to generate its output and then encrypting that output with the sender's private key.[80] That data becomes the digital signature. The recipient then uses the same hash function to get the message digest and uses the sender's public key to decrypt the message.[81] Now the recipient can verify that the proper sender sent the message, but still needs to authenticate that the sender has an acceptable real-world identity.[82]

Just as individuals receive credentials from accepted and trusted authorities, such as obtaining a Driver's License from the State of Illinois, an accepted and trusted online authority can authenticate a user's credentials. This is accomplished through the use of a certificate, a digitally signed "electronic passport," to assure that the sender is the proper user.[83] To do this, the recipient uses the public key of the entity that issued the certificate to verify that the certificate is valid.[84] The recipient will only accept certificates from entities that it trusts to have properly checked the identity and credentials of a user before issuing the digital signature capability to that user.[85]

Because trust is important, widespread use of digital signatures depends on an infrastructure of trusted entities upon whose certificates recipients can rely. This infrastructure is known as Public Key Infrastructure (PKI).[86] Entities may cross-certify, agreeing to accept each other's certificates, as an effort to increase the number of users who may be authenticated.[87] This is useful for electronic commerce and for the government as well—offering electronic service delivery to provide confidence for government agencies in dealing with employees, other agencies, and recipients of services.[88] A trusted digital certificate, with the proper underlying certification, can communicate information such as credit rating,

78. *Id.*
79. *Id.*
80. *Id.*
81. The fact that the public key works assures the recipient that the sender sent the data. *Id.*
82. *Id.*
83. *Id.* § 10.7. The term "electronic passport" was suggested to the author by Mark Anderson. Telephone interview with Mark Anderson, Data Sec. Manager, Ill. Dep't of Cent. Mgmt. Servs., Bureau of Communications and Computer Servs. (Jan. 20, 2004) (transcript on file with the University of Illinois Law Review).
84. Wu, *supra* note 71, § 10.7.
85. *Id.* The entity that issues certificates is a "Certificate Authority" (CA), which may be a either a private company or government entity. *Id.* Usually, the CA will be trusted if the procedure used to verify identity is deemed adequate by the recipient, with procedures ranging from online registration using only a credit card to in-person registration. *Id.* The decision of whether to accept the third party's certifications must be made by the recipient personally, while the other functions are performed after this decision is made and communications are received. *Id.*
86. *Id.*
87. *Id.*
88. Roger Clarke, Position Statement, *at* http://www.anu.edu.au/people/Roger.Clarke/DV/PKIPosn.html (last revised May 6, 1998).

name, address, employment, voting status, age, or any type of information that a certificate (CA) requires or a sender wishes to have verified.[89]

So far, most commentators have assumed that certificates will need to consist of features of identity that may include the user's real name, rather than just the person's "clearance"—things such as credit limit, voting rights, and citizenship.[90] This may be due to Lessig's suggestion that e-commerce is fueling the drive toward digital signatures on the Internet.[91] It would seem intuitive that commercial enterprises would seek to have a digital signature function exactly like a credit card, quickly and securely transmitting information needed to verify the identity of a purchaser.[92]

This, however, does not consider the potential for electronic signatures to be used for online voting in political elections, political and other forms of speech, or artistic expressions.[93] There are two main types of certification. The first has been referred to as "eligibility authentication," which means giving "assurance that people claiming a particular capability actually have it," such as the authority to sign contracts, receive discounts, and vote.[94] The other is known as "person authentication" or "user authentication," which ensures that a person is who he or she claims to be when it is needed, such as to access one's own personal data from a medical source or to establish ongoing relationships with entities.[95]

The current uses of digital certificates appear to combine person authentication and eligibility authentication. For example, a certificate might say that Jane Jones of 15 XYZ Street, is authorized to purchase up to $16,000 of merchandise for her employer, Jones Enterprises. Both the name of the individual and the authorization level are often included in the settings for certification and authentication. Thus, it is likely that the digital certificate capabilities will provide businesses with the security and authentication they need to transact business online.[96] Still, even when it is impossible to remain completely anonymous in transactions, it

89. Roger Clarke, Public Interests on the Electronic Frontier, Address to I.T. Security '97, IIR Conferences (Aug. 14–15, 1998), *available at* http://www.anu.edu.au/people/Roger.Clarke/II/IIRSecy97.html.

90. *Id.*

91. *See* LESSIG, *supra* note 28, at 39.

92. It should be possible, however, for online transactions to proceed anonymously. *See* Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 467 (1999) (noting that, though such anonymous transactions are possible, "law enforcement officials have lobbied aggressively against anonymity.").

93. *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶¶ 56–57 (2001), *at* http://stlr.stanford.edu/SLTR/Articles/01_STLR_1/index.htm.

94. Clarke, *supra* note 89.

95. *Id.*

96. *See* Geoffrey Gordon, *Breaking the Code: What Encryption Means for the First Amendment and Human Rights*, 32 COLUM. HUM. RTS. L. REV. 477, 481–82 (2001) (noting that digital signatures provide the recipient to assure that the purported sender actually sent the message and that the message has not been altered in any way since it was sent).

may be possible to remain pseudonymous—using just the chosen username to conduct transactions, rather than using one's real name.[97]

Roger Clarke, a Visiting Fellow at Australian National University, has commented that "[a]ll forms of PKI necessarily involve some degree of intrusiveness, in order that sufficient quality can be achieved."[98] Part of the concern arises when government entities request authentication of individuals and ask for both identity and access authority or rights to be combined.[99] The government is then requesting both the access rights of the individual and the identity. Both may not always be necessary, however. Because, especially in the case of voting, the government possessing both may actually chill exercise of constitutional rights of citizens, it is important to examine the implications of such requests.

Currently, many state governments authorize CAs to operate in their states, thus certifying that the procedures used by those CAs are adequate for government and business needs.[100] In Illinois, at least, the government itself is steadily working at creating its own CA, and it plans to offer basic government services to all citizens, such as driver's license renewal and receipt of state aid, online in the hope of eventually providing many of the state's services, such as business registration and payment of taxes, through the Internet.[101] Though full implementation of these plans will likely take years, government employees are currently being authenticated and assigned digital signature and encryption capabilities.[102] If the State of Illinois is successful, then the state itself would collect the information about the individual, and it would have the tools necessary to connect the online identity with that person's real world identity, providing no buffer between the government and the information.

The federal government has already noted the problem of the loss of consumer privacy online. Laws have been put in place to protect the privacy of certain information on the Internet. The Children's Online Privacy Protection Act prevents solicitation of personal information from children on the Internet without parental consent.[103] The Health Insurance Portability and Accountability Act of 1996 protects the privacy of medical information.[104] The Financial Services Modernization Act of

97. Clarke, *supra* note 89, at *1.

98. *Id*. at *2.

99. *Id.*

100. *See* Lanin, *supra* note 30, at 1452.

101. *See* G. Kreizman, *State of Illinois Moves Public-Key Infrastructure Forward*, Gartner Research Case Studies, CS-16-1191 (Apr. 19, 2002).

102. *Id*. (noting that Illinois had registered 3500 users as of April 2002). As of January 2004, Illinois has registered 23,000 users. Telephone interview with Mark Anderson, *supra* note 83.

103. *See* The Children's Online Privacy Protection Act, 15 U.S.C.A. §§ 6501–6506 (West Supp. 2003). For an account of its effect on businesses and consumers, see Rachael Malkin, Note, *How the Children's Online Privacy Protection Act Affects Online Businesses and Consumers of Today and Tomorrow*, 14 LOY. CONSUMER L. REV. 153 (2002).

104. *See* The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996). For an analysis of the privacy protection afforded by HIPAA and

1990, or the Gramm-Leach-Bliley Act, applies to financial institutions and protects against the release of information allowing individuals to be personally identified.[105] Thus, the federal government has provided limited protections for information becoming freely available online, but it has been strictly limited by subject matter.

Despite these protections, it may be important for anonymity, or at least pseudonymity, to be addressed as an issue separate from privacy and in conjunction with electronic and digital signatures. When dealing with government agencies, it may be necessary for the government to know your name—as in the receipt of government benefits. After all, the beneficiaries are availing themselves of these government benefits. Still, it is then easy for the government to find out other uses of your certificate and digital signatures, if the certificate has multiple uses and is simply cross-certified by other agencies or businesses. Some users may choose to join or participate in certain online groups or activities only if they can do so without fear of being identified.[106]

Actual anonymity may not be realistic or desirable in all cases, however. "Where candor is valued above all, perfectly consequence-free anonymity may be most appropriate. Where there's a concern about flaming or disruptive behavior, pseudonymity may be best."[107] To achieve this objective, while recognizing that anonymity may not be possible in all cases, it may be extremely important for any certificates issued directly by government entities to be carefully monitored. It may be important for such certificates to have uses limited to governmental services only, that the same certificate not be used for services for which the real identity of the user is important and for services when it might chill speech for the true identity to be known, such as voting, and for it to be difficult for the government to obtain the real identify of users.[108] Due to the cost of certificates, however, such limits may not be desirable. An additional possibility is for a private entity to register users, thus insulating the users from direct governmental involvement.[109] It is unclear whether the current legislation provides these protections for users or whether legislators or citizens recognize the potential for abuse.

whether it is sufficient, see Peter D. Jacobson, *Medical Records and HIPAA: Is It Too Late to Protect Privacy?*, 86 MINN. L. REV. 1497 (2002).

105. Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act), Pub. L. No. 106-102, 113 Stat. 1338 (1999).

106. *See supra* note 19 and accompanying text. Anonymous organization and speech in the real world is analogous to that necessary for Internet communications.

107. Walker, *supra* note 60, ¶ 61. Walker suggests that it is thus important for carefully crafting Internet laws and that it might be impossible to create "one-size-fits-all" legislation. *See id.* ¶¶ 104–105.

108. *See supra* note 93 and accompanying text.

109. *See infra* Part VI.

IV. COMPARISON OF THE REQUIREMENTS OF THE EUROPEAN UNION, GERMANY'S DIGITAL SIGNATURE STATUTE, AND ILLINOIS'S DIGITAL SIGNATURE LEGISLATION

A. European Union Directive

The United States and European countries have not always agreed on the amount of privacy to afford to their respective citizens. For example, while the United States has allowed personal information collected by companies to be resold and has not yet legislated to require Internet information collectors to disclose their privacy policies, the European Union has taken a different stance.[110] The EU requires that companies gathering information about its citizens operate from countries that have satisfactory privacy-protection legislation in place.[111] The United States had no such legislation, so U.S. companies would have faced an inability to engage in the data collection business in Europe.[112]

The United States, however, was able to enter an agreement with the European Union.[113] The so-called Safe Harbor Agreement allowed transfer of information to individual companies that agreed to abide by the European policies, thus allowing continued business.[114] Thus, a contractual way around the problem was developed for U.S. companies wanting to participate in the European market. This highlights a difference between the privacies provided freely in Europe but not afforded to U.S. citizens. Also, European citizens are granted the right to view information being compiled about them, while that is not freely available in the United States.[115] There are also differences in the expectations of anonymity, as can be seen in the following directives and statutes.

In 1999, the European Parliament and Council enacted legislation intended to govern the enactment of statutes for controlling digital signatures and other electronic signature devices on the Internet.[116] The Directive prohibits "any kind of interception or surveillance of [confidential communications governed by Article 5 Directive 97/66/EC] by others

110. *See* Huie, *supra* note 1, at 396.

111. *See* Council Directive on Data Privacy, 95/46/EC, 1995 O.J. (L 281) 31–50. This directive prohibits any transfer of personal data to nations not in the European Union if they are not "adequate" under the European Union standards. *See* Huie, *supra* note 1, at 469 n.14.

112. *See* Huie, *supra* note 1, at 396. "The EU's data-privacy efforts for e-commerce could cause 'imposition of one of the largest free trade barriers ever seen.'" *Id.* at 392 (quoting Representative Billy Tauzin, Chair of U.S. House of Representatives Comm. on Energy and Commerce, *in* Peronet Despeignes & Deborah Hargreaves, *The Americas: U.S. Criticises EU on Data Privacy*, FIN. TIMES (London), Mar. 9, 2001, at 12).

113. Huie, *supra* note 1, at 397.

114. *Id.*

115. *Id.* at 396. European citizens also enjoy the right to alter the information, expunge it when it is no longer necessary, and to affirmatively "opt-in" to the data being collected at all. *Id.*

116. Council Directive on a Community Framework for Electronic Signatures, 1999/93/EC, 1999 O.J. (L 13) 12.

than the senders and receivers."[117] The Directive notes that it "is not intended to affect national fundamental rules and principles relating to freedom of expression."[118] The Directive states that protection for individuals for "the processing of personal data is solely governed by" other law, as is the "free movement" of such data. Just six months after passing its first Directive, the Council adopted another Directive, designed to aid electronic commerce in the internal European Market.[119]

The second Directive notes the importance of "balanc[ing] . . . consumer and business needs."[120] Also, in its findings portion, the Directive states that electronic signatures will be used for "public procurement, taxation, social security, health and justice systems," and that it is important for the signatures to be allowed in legal proceedings to confirm identity.[121] Under Article 8: Data Protection, the Directive states that "[w]ithout prejudice to the legal effect given to pseudonyms under national law Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name."[122] The Directive also provides that the data collected for the purpose of issuing a certificate for a user shall be collected only from the subject and used only for certificate purposes without direct consent by the subject.[123]

B. Germany's Statute Regulating Digital Signatures[124]

Passed in 1997, Germany's multimedia law includes issuance of certificates and provides guidelines and expectations of privacy similar to those in the European Union Directives. One ordinance authorizes the government to license CAs for operation, and if performed by public agencies, it allows the services to be charged to recipients of the licenses.[125] For documentation, the ordinance provides that the CA shall keep certain records, including pseudonyms issued, proof of required notifications of applicants and third parties, and issued certificates, including validity dates.[126] This ordinance works in congruence with Germany's multimedia law, which states, "[t]he provider shall offer the user anonymous use and payment of teleservices or use and payment under a pseu-

117. *Id.* ¶ 15.

118. *Id.* ¶ 9 (noting that "[t]he free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression").

119. Council Directive on Electronic Commerce, 2000/31/EC, 2000 O.J. (L 178) 1.

120. *Id.* ¶ 14.

121. *Id.* ¶¶ 19–21.

122. *Id.* art. 8, ¶ 3.

123. *Id.* art. 8, ¶ 2.

124. *See* THE PRIVACY LAW SOURCEBOOK 2001: UNITED STATES LAW, INTERNATIONAL LAW, AND RECENT DEVELOPMENTS 351–61 (Marc Rotenberg ed., 2001); *see also* Signaturverordnung [Digital Signature Ordinance], *translated in* 37 I.L.M. 579 (1998).

125. Signaturverordnung, *supra* note 124, at 579–80, §§ 1–2.

126. *Id.* at 583, § 13.

donym to the extent technically feasible and reasonable."[127] Though the multimedia statute applies to providers of consumer service, the ordinance applies to the government as a CA, as well. Germany thus protects both consumers and citizens. The security measures require that the recipient of a document that is digitally signed be able to "reliably establish the identity of the signature key holder."[128]

C. Illinois's Statute Governing the Use of Digital Signatures[129]

The Illinois Electronic Commerce Security Act lists requirements for a certificate, including that each:

> (a) identif[y] the certification authority issuing it; (b) name[] or otherwise identif[y] its subscriber or a device or electronic agent under the control of the subscriber; (c) contain[] a public key that corresponds to a private key under the control of the subscriber; (d) specif[y] its operational period; and (e) [be] digitally signed by the certification authority issuing it.[130]

A digital signature is then defined as:

> a type of electronic signature created by transforming an electronic record using a message digest function and encrypting the resulting transformation with an asymmetric cryptosystem . . . such that any person having the initial untransformed electronic record, the encrypted transformation, and the signer's corresponding public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial electronic record has been altered since the transformation was made.[131]

The statute provides for the Secretary of State to issue rules as to when a certificate is trustworthy and to ensure that there will be uniformity with the laws of other jurisdictions.[132] A digital signature may be used to identify the signatory while the certificate is still valid and trustworthy, according to the regulations issued by the Secretary of State.[133]

Further, an electronic signature is attributable to the person to whom it is assigned, "whether or not authorized, if: (1) the electronic signature resulted from acts of a person that obtained the signature device or other information necessary to create the signature from a source un-

127. *See* Rotenberg, *supra* note 93, at 68 (citing PRIVACY LAW SOURCEBOOK 305–13 (Marc Rotenberg ed., 1999)).

128. Signaturverordnung, *supra* note 124, at 579, § 16, ¶ 3.

129. 5 ILL. COMP. STAT. ANN. 175/1-101 to 175/99-1 (West 2003).

130. *Id.* 175/5-105.

131. *Id*.

132. *Id.* 175/15-115. The Secretary of State may develop standards for registering CAs and may charge fees for doing so, as well as provide a way to recognize foreign certificates, both from other states, the United States, and international issuers. *Id.* For a view that such regulations being set by the states may cause dormant Commerce Clause issues, see Lanin, *supra* note 30, at 1423.

133. 5 ILL. COMP. STAT. ANN. 175/15-105.

der the control of the alleged signer, creating the appearance that it came from that party;" (2) the party didn't use reasonable care; and (3) the recipient relied on the "apparent source." However, this does not apply to personal, household, family, or consumer transactions.[134]

D. Discussion of Various Digital Signature Statutes

The Illinois regulation lacks any mention of a possibility for users to remain either anonymous or pseudonymous. It does not provide a way for the user's identity not to be connected with the digital signature itself. While identity is likely to be important for transactions between a consumer and the government, involving tax payment or disability payments, other transactions would be better served through anonymity.[135] Although political groups do not currently require the use of electronic signatures, as more functions are performed online they may wish to identify members more clearly, requiring electronic signatures as the cost of technology decreases.

The Illinois law does not appear to make a distinction between the government functioning as a CA and external nongovernment CAs. Because the Illinois plan is to issue certificates to all citizens for uses both with the state and with external entities, the lack of the possibility to have a pseudonym for certain activities may be pivotal. Having an external provider as a CA requires the government to go through proper channels to get the information about identity, as it must do now to get the identity of users from ISPs. If, however, the government itself registers users, then the information is freely provided by the users to the government.[136] This may make a difference in a court's analysis of what level of privacy the user should expect in the transactions conducted using the electronic certificate provided and authenticated by the government. While it is unlikely that the government could use the electronic certificates to track every web page a person views, as has been feared,[137] the government would be authenticating every web transaction signed with the certificate the government provided. This is in stark contrast to the requirements in Europe. Not only do European laws protect consumers from unknown data collection, but European laws also provide the capability to remain anonymous or pseudonymous in transactions.

Finally, the fact that the Illinois statute specifically exempts consumer uses of the digital signatures from certain liabilities is an important indicator of the law's focus, as currently drafted. While the European statutes clearly contemplate a government role in the regulation of digital and electronic signatures for consumer protection,[138] the Illinois stat-

134. *Id.* 175/10-130.
135. *See* Clarke, *supra* note 89.
136. *See infra* notes 190–91 and accompanying text.
137. *See* Swire, *supra* note 92, at 474.
138. *See supra* notes 118–23 and accompanying text.

ute seems to be driven more from the point of view of businesses—wanting to legitimate the use of such signatures for large commercial transactions, but without fully considering the amount of protections that may be necessary for consumers and citizens. Although businesses have wanted the ability to identify purchasers and thus be able to enforce contracts,[139] this focus has meant that consumers' and citizens' privacy rights have not fully been considered in enacting such laws.[140]

V. AMERICAN ELECTRONIC AND DIGITAL SIGNATURE STATUTES—DIFFERENT GOALS AND APPROACHES

Legislation was needed to legitimize the use of electronic signatures in the formation of contracts to give effect to those contracts made either between businesses, or between consumers and businesses, online.[141] In other words, electronic signatures needed to have the same effect as ink signatures applied to paper. Businesses needed to be able to trust contracts made in this fashion, and the resulting legislation reflected the need for secure digital contracts. Even before the U.S. federal government passed legislation permitting the use of digital and electronic signatures, some states, including Utah[142] and California,[143] had already passed legislation governing the use of such identification and verification techniques. Utah and California chose two different approaches to legitimizing electronic verification devices—technology-specific and technology-neutral.

A. Utah's Technology-Specific Approach

Utah chose technology-specific legislation, requiring the use of "digital signatures as a means of executing an electronic document."[144] Although Utah has since adopted different legislation, the original act had strict requirements that a CA had to meet to be certified within the state.[145] Once a CA met the requirements, it received limited liability.[146]

139. *See* Lanin, *supra* note 30, at 1449.

140. It is not only Illinois's laws that suffer from this lack of foresight into the privacy losses that may accompany the use of digital signatures. There do not appear to be any statutes within the United States that mention anonymity or pseudonymity in conjunction with the use of digital or electronic signatures. While, of course, certain functions will require identification of the user, as in when one is actually doing business with the state, it is the functions for which the state should not need to know one's identity that the laws may present a problem.

141. *See, e.g.,* Lanin, *supra* note 30, at 1449.

142. UTAH CODE ANN. §§ 46-3-101 to -504 (1998).

143. CAL. GOV'T CODE § 16.5 (West Supp. 2003).

144. Ian A. Rambarran, *I Accept, but Do They? . . . The Need for Electronic Signature Legislation on Mainland China*, 15 TRANSNAT'L LAW. 405, 415 (2002) (stating that, to be equal to an ink signature, the document requires a digital signature, along with a "digital certificate, issued by a state-licensed certification authority that verified the owner of the public key").

145. *See id.* at 419–20; *infra* note 156 and accompanying text; *see also* UTAH CODE ANN. §§ 46-3-201, -301 (1998). To get a license, and each CA needed a license, required posting a guarantee and

Utah also established procedural requirements for CAs.[147] Many other states modeled their statutes after Utah's technology-specific approach, though the statutes varied in either addressing electronic signatures or digital signatures, without examining both.[148]

B. California's Technology-Neutral Approach

California's first round of legislation gave digital signatures the effect of ink signatures, but the act applied only to transactions with an agency of the government.[149] California later enacted legislation intended to apply to consumer transactions.[150] California's legislation applied to electronic signatures as a whole, rather than to just digital signatures.[151] This is the technology-neutral approach to legislation regarding electronic signatures. This approach allows different types of electronic signatures to be used to authenticate Internet transmissions and documents.[152]

C. The Need for a Uniform Approach in State Legislation on Electronic Signatures

Utah's and California's differing approaches to electronic signatures and the question of whether legislation should be technology-neutral or technology-specific influenced the other states, which could then choose between the two approaches. Federal legislation seemed necessary to help with commercial certainty because businesses wishing to do business online and in multiple jurisdictions faced the dilemma of which technology to develop and determining which sets of laws and regulations it would need to comply.[153]

meeting personnel requirements meant to ensure reliability and honesty of the CA's staff. *See* Rambarran, *supra* note 144, at 415.

146. *See* Rambarran, *supra* note 144, at 415.

147. *See* Andrew B. Berman, *International Divergence: The "Keys" to Signing on the Digital Line—The Cross-Border Recognition of Electronic Contracts and Digital Signatures*, 28 SYRACUSE J. INT'L L. & COM. 125, 141 (2001).

148. *See* Thomas J. Smedinghoff, *Analyzing State Digital Signature Legislation*, Aug. 1997, *at* http://www.mbc.com/ds_rev.html (Aug. 1997) (website no longer accessible; information on file with University of Illinois Law Review) (noting that Illinois's then-proposed legislation was the only exception, seeking to address both types of signatures). Smedinghoff also noted that while a few states would allow most electronic marks to be used as electronic signatures, states such as California had specific requirements for acceptability. *Id.*

149. *See* Rambarran, *supra* note 144, at 416–17 (citing CAL. GOV'T CODE § 16.5 (West Supp. 1995)).

150. *See id.* (citing CAL. GOV'T CODE §§ 1633.1–.17 (West Supp. 2001)).

151. *See* CAL. GOV'T CODE § 16.5 (West 2003).

152. *See* Rambarran, *supra* note 144, at 417. Rambarran noted that a problem with California's legislation is that it applies to such a narrow set of transactions between the government and private parties. *Id.*

153. *See id.* at 418 (noting that businesses were having to adopt multiple technologies to meet the requirements of different states, leading to consumer uncertainty).

The National Conference of Commissioners on Uniform State Laws (NCCUSL) suggested that a uniform law used as a guideline for all states would be helpful in solving many of these problems.[154] They composed the Uniform Electronic Transaction Act (UETA)[155] as a model for state adoption. NCCUSL designed UETA to correct problems that had developed with both Utah's[156] and California's[157] previously enacted legislation. Not all states were convinced, however, and by the middle of 2000, not even half of the states had adopted UETA, as suggested or with modification.[158] Because the proposed legislation had not yet caught on with the states, and there was a heavy push for uniform laws, the call for federal legislation began.[159]

D. Federal Legislation Began to Seek a Uniform Approach Among the States

President Clinton responded to the increasing Internet market with legislation called Electronic Signatures in Global and National Commerce Act, commonly known as E-SIGN.[160] E-SIGN was designed to increase consumer willingness to engage in electronic transactions and create uniformity in the previously confusing laws.[161] The Act treats electronic signatures as the equivalent of ink and paper signatures, thus creating certainty for consumers and businesses alike.[162] Like California's legislation, E-SIGN takes a technology-neutral approach to regulating electronic signatures.[163] Additionally, E-SIGN allows parties to remain autonomous, so that they may choose the best method of electronic signature for their particular transactions.[164] The Act allows states to enact legislation to replace E-SIGN as long as they do not give preference to one form of electronic signature over another.[165] This would preempt

154. *See id.* (citing Amilia H. Boss, *Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reformation*, 72 TUL. L. REV. 1931, 1963 (1998)).

155. *See id*.

156. Utah has since adopted UETA. *See id.* at 419–20.

157. California had adopted a version of UETA, but made many exceptions and has since considered replacing its version to match the version produced by NCCUSL. *Id.* at 420.

158. *Id.*

159. More and more businesses pushed for the possibility of online transactions, and the federal government responded. *Id.*

160. Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 U.S.C.A. §§ 7001–7031 (West Supp. 2003). For an overview of the history, purpose, and effect of E-Sign, see Robert A. Wittie & Jane K. Winn, *Electronic Records and Signatures Under the Federal E-Sign Legislation and the UETA*, 56 BUS. LAW. 293 (2000).

161. Rambarran, *supra* note 144, at 420.

162. *Id.* at 420–21.

163. *See id.* (noting that "an e-mail message, a digital signature, or a biometric signature can be used to execute a document, as long as it is intended to be substituted for an ink signature").

164. *See id.* at 421.

165. 15 U.S.C.A. §§ 7001–70031. The relevant portion states that states may give "legal effect" to types of technologies as long as "such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating,

legislation that favors digital signatures over other forms of electronic signatures, such as Utah's original legislation. As of August 2003, forty-two states and the District of Columbia had enacted some form of UETA, helping to achieve the goal of encouraging online transactions through uniform laws among the states.[166]

E. Amount of State Involvement in the Regulation of Electronic Signatures

Since the creation of more uniform state laws, other differences between the states' laws have come to the forefront. The states do not agree on methods of implementing the new laws they have adopted. The regulation of electronic signatures has caused legislatures and state agencies to contemplate important policy issues regarding the amount of state involvement that is advisable or necessary.[167] Washington and Illinois illustrate two differing approaches in PKI legislation, with Washington choosing to outsource much of the work, and Illinois choosing to itself become the CA for users in the state.[168]

F. Washington State's Approach

Washington passed the Washington Electronic Authentication Act in 1996, modeling its law on Utah's Digital Signature Act.[169] It began its project, Transact Washington, in late 2000.[170] Washington designed its project to allow businesses to interact with the state for services, such as filing workers' compensation claims and affidavits, as well as other forms of electronic filing.[171] The state is selling electronic signatures to users, and by early 2002, had distributed approximately 3000 certificates.[172] In 1998, Washington decided to try to use its Act to make government activities more efficient.[173]

Implementation proved more complex than was originally anticipated, however, so the state began with a pilot project using digital signa-

or authenticating electronic records or electronic signatures." *Id.*; *see* Wittie & Winn, *supra* note 160, at 334 (stating that Congress did not want states to be able to help or harm certain forms of technology through their legislation).

166. *See* Nat'l Conf. of State Legislatures, Uniform Electronic Transactions Act, *at* http://www.ncsl.org/programs/lis/cip/ueta.htm (last visited May 3, 2004).

167. *See generally* Roberts-Witt, *supra* note 8, at 17, 19. The article discusses Washington and Illinois as "PKI Innovators" in legislating the issues and highlights their differing approaches. *Id*.

168. *Id.* at 19.

169. *Id.* at 17.

170. *Id.*

171. *Id.* To make it easy for users, the only system requirements are a Windows-based operating system, either Internet Explorer or Netscape Navigator to browse the Internet, encryption capability, and a digital certificate. *Id.*

172. *Id.*

173. *Id.* at 18.

tures and serving as its own CA.[174] The state thus checked identities of applicants, issued certificates, and managed the certificates over time—including expiration dates and other management issues.[175] Through its pilot project, Washington was dissatisfied with being its own CA because of the cost of background checks and necessary technology and of the liability that the state incurred by operating as the CA.[176] Because Washington was the CA, the state itself answered requests for authentication of digital certificates, and it thus assumed responsibility for the identity of the individual and the authenticity of the digital certificate, even for transactions between individuals.[177] The state was unwilling to bear the risk.[178] Through a PKI team, the state began to look for outside entities that could provide the needed CA and PKI services, the state team chose Digital Signature Trust as the provider.[179] Washington continues to outsource its CA services due to its findings during its pilot project.

Washington also chose to allow businesses to participate in the policy creation for its pilot project, but chose not to allow this for the final Transact Washington project, instead requesting that the agencies make suggestions regarding already written policies.[180] The team felt that this would prevent the agencies or businesses from having too much control over the legislation, allowing the team to instead devise the best prototype and limit the scope of suggestions.[181]

G. Illinois's Approach—Acting as Its Own Certificate Authority for Electronic Signatures

Illinois has chosen an ambitious scope for its project, choosing to become its own CA and intending to issue certificates both to businesses (as Washington has done) and directly to individuals to enable them to collect disability benefits and interact directly with both other state agencies and private entities, online.[182] Then-Governor George Ryan, show-

174. *Id.* Serving as its own CA required the state to "issue[] and maintain[] digital certificates and ensur[e] that those who applied for them were who they said they were." *Id.*

175. *Id.*

176. *Id.*

177. *Id.* "'Being responsible for the entire transaction conducted with a digital signature, especially if it is a high-dollar transaction or one that isn't even with a state agency, was just not a risk we were willing to take,' said Bream." *Id.* Bream is Program Manager of Washington's PKI initiative. *Id.* at 17.

178. *Id.* at 18; *see also* Shimshon Berkovits et al., Nat'l Inst. of Standards & Tech., Public Key Infrastructure Study: Final Report, *at* http://www.nap.edu/readingroom/books/crisis/H.txt (last revised Apr. 1994) (noting, while freedom from liability might be possible for government entities acting as CAs, that would be undesirable, as the point of having such CAs is to verify identities to reduce liability of the parties to the transaction).

179. Roberts-Witt, *supra* note 8, at 18.

180. *Id.* at 20–21. Washington's policy can be found *at* http://www.digsigtrust.com/state/wa/swa-policies-main.html.

181. Roberts-Witt, *supra* note 8, at 21.

182. *Id.* at 19–20. "'We started this project thinking just of the state government, which consists of 60 agencies and 60,000 employees, as the enterprise,' Crossland said." *Id.* "'However, we realized

ing his commitment to using electronic signatures, signed his first administrative order of 2002 with a digital signature.[183] Illinois's Deputy Technology Officer, Brent Crossland, stated that Illinois was uncomfortable with outsourcing and preferred to create its own PKI infrastructure and issue certificates.[184] Illinois had initially planned to have each agency pay for the certificates it issued, but that proved difficult, due to the fact that the same certificate would later be used to interact with other agencies, meaning no agency would want to be the first to issue certificates.[185] Also, individuals might not be able to bear the cost. Illinois, therefore, chose a different funding approach from that of Washington and decided to centrally fund its project.[186]

Illinois's approach also differed from that of Washington in that it created a Joint Policy Board, which has control over drafting, reviewing, and updating the certificate policy necessary for a CA to operate.[187] Users view the certificate policy when attempting to ascertain the level of authenticity to afford a certificate issued by that CA, because the policy details the procedures used for issuing and revoking digital certificates by that entity. Illinois's policy is similar to that of the federal CAs, because there are four levels of certificates, each requiring a different degree of background check and proof of identification.[188]

The differing approaches that Illinois and Washington have taken may lead to different concerns for private citizens. While the residents of Washington will be able to choose whether they wish to have a digital certificate and from whom they will obtain it, the Illinois approach requires residents to register directly with the state and to provide varying degrees of identifying information to the state, depending on the type of certificate that is issued or required.[189] When outside entities request authentication of users who attempt to interact with them, such as a business wishing to form a contract with an Illinois resident, the state will issue the required authentication of the resident's identity. As a result of the authentication, the state will have knowledge of the entity requesting the level of authentication and of the identity of the individual for each transaction entered. Thus, whether or not the individual intends to in-

that the definition had to change to include municipal and local governments, public universities, basically any public institution that an individual might need to interact with.'" *Id.* at 20.

183. *See* Ill. Admin. Order, No. 1 (Feb. 14, 2002), *at* http://www.illinois.gov/tech/tech_administrative.cfm (last visited Apr. 21, 2004). The order required that PKI would be administered by the Department of Central Management Services and that agencies should procure equipment that would be compatible with the system set up by the Department of Central Management Services, to ensure that the agencies would be able to interoperate. *Id.*

184. Roberts-Witt, *supra* note 8, at 19. "'We just weren't comfortable trusting something of this magnitude and this level of security to a third party,' said Brent Crossland, Illinois's deputy technology officer." *Id.*

185. *Id.* at 20.

186. *Id.*

187. *Id.* at 21.

188. *Id.* Illinois's policy is available *at* http://www.illinois.gov/pki/cert_policy_contents.cfm.

189. *See* Clarke, *supra* note 89.

teract with the state, the state will have a record of the individual's transactions, or at least the entity with whom the individual interacts. This may be a matter of little concern to some, but it does represent a difference in the level of privacy and anonymity currently enjoyed by Illinois residents.

Not only does the state face additional liability for the authentication of all those to whom it issues certificates, but consumers and citizens to whom the certificates are issued face lost anonymity and the loss of privacy in their outside interactions. Each Illinois agency is required to have a Privacy Officer in place to monitor state *disclosure* of information, but the Governor's Administrative Order for E-Government does not mention state *collection* of personal information.[190] In addition, Illinois did not initially allow certificates to be issued with the possibility of using a pseudonym.[191] Each certificate is issued with the user's name attached. The State of Illinois has issued certificates to both state employees and citizens, but those currently issued are for use in state business. Currently, Illinois does not plan for these certificates to be used in private transactions, but this policy may change in the future. This change would present far greater privacy concerns.

VI. RESOLUTION

Just as individuals might expect their Internet speech to receive First Amendment protection, they also might expect their records to receive protection under the Fourth Amendment, when the concern is criminal prosecution. The Supreme Court has viewed financial records as banks' business records, and found that an individual had waived any possible expectation of privacy by choosing to do business with the bank in a way that revealed his financial activities to the bank and employees.[192] Congress later added protections,[193] but because the court found the voluntary interaction with the bank and voluntary provision of information a key factor, interactions made with knowledge that the state will be authenticating transactions using the electronic signature provided might cause the Supreme Court to rule that the individual has no expectation of privacy in the information freely provided.[194] The gov-

190. Ill. Admin. Order No. 1 (Feb. 14, 2002), *at* http://www.illinois.gov/tech/tech_administrative.cfm (last visited Apr. 21, 2004). Governor Ryan also required each agency to appoint a Security Officer to "safeguard[] the information technology assets of the agency." *Id.*

191. *Id*. Now, though a recipient's real name is required to register for the certificate itself, the login name may be a pseudonym.

192. Swire, *supra* note 92, at 482 (citing United States v. Miller, 425 U.S. 435 (1976)).

193. *Id.*

194. *See supra* note 190 and accompanying text. This voluntariness of information raises both First and Fourth Amendment concerns. Even if governmental knowledge of transactions does not violate either amendment because of the user's voluntarily providing the information, it challenges the underlying values of each amendment. If the Supreme Court does not see government knowledge of information as a violation, then it is important that citizens push for congressional recognition of the right to privacy (freedom from governmental intrusion) in information such as the records provided

ernment is restricted in its use of information, but the collection of information just as a function of authentication would be done as a service to citizens and might not be seen as harmful, despite citizens' wishes to have anonymous transactions. If businesses in Illinois choose to have the state provide the electronic signature capability (as seems likely, because the state would pay at least the bulk of the costs), then citizens may have little choice but to use the signatures provided by the state if they wish to conduct business online.[195] Because users often choose convenience over data protection,[196] it means that they may slowly waive their rights. Once what was formerly private is freely provided to the government, the Supreme Court may cease to recognize a privacy interest in the information at all; no constitutional violation can then occur, even if citizens later object to the loss of privacy.[197]

If users choose to use the system provided by the state, then all transactions requiring authentication would be done through state computers. Some suggest that certain Internet payment options allow a purchaser's bank to be "unable to link the transaction to the individual purchaser."[198] If external entities register users for digital signatures for the state and provide, at a minimum, pseudonym capabilities, then it should similarly be impossible for the end user to trace the transaction or for the government to get the records without going through proper channels to get the information. Having a private entity do all registration, even if the registration is done *for* the government, should provide greater protection of individuals' rights than if the government itself does the registration because of the insulation between the individual's transactions and the government actor.

If, however, citizens do not call for legislation recognizing the privacy interest in information freely provided, then the Supreme Court may still refuse to find constitutional implications, as it did for the information in bank records. Still, for law enforcement purposes, the government would at least be required to follow proper procedures to get

online. While the government may violate both amendments in its actions, a private entity cannot violate either.

195. The focus of this note is not on the interaction between different systems in different states. It appears likely that states will cross-certify with each other, agreeing to take the certificates each other state authenticates, as long as the processes used to register users meet the minimum requirements each state has set.

196. *See* Walker, *supra* note 60, ¶ 40 ("[M]ost people prefer to use a credit card rather than a debit card, trading confidentiality of purchases for the convenience of deferred payment.").

197. This should be true of both First and Fourth Amendment violations. Though the government may not be able to *require* use of digital signatures for certain activities, if businesses with whom users interact require them, and the user freely provides the information to the government, then the First Amendment would likely not be violated, despite the obvious connections to the concerns underlying the First Amendment. As for the Fourth Amendment, the government would already possess the information. It might require a warrant to access information in other departments if to be used for law enforcement purposes, but it would certainly be harder to prove a violation.

198. Swire, *supra* note 92, at 484.

the transactional or other information requested, rather than having the information in-hand due to providing the digital signature service itself.

"Individuals can no longer maintain a wait-and-see attitude if they wish to protect their privacy."[199] The concern is not purely about government crime control initiatives.[200] The freedom of association and speech currently enjoyed on the Internet cannot be fully used when government entities can trace and identify transactions or communications and associate those with the sender.[201] The fact that some entity will be able to trace certain communications or transactions may be unavoidable, but the entity does not have to be the government itself.

In a similar light, the problem is not that the technology to make our lives easier exists, but that laws need to be crafted with the interests of consumers and privacy in mind. Because Supreme Court precedent suggests that unless Congress creates a right to privacy in the information freely turned over for the privilege of using technology, it will be lost,[202] laws regarding digital signatures should be created with the interests of consumers in mind, to preserve the privacy still possible on the Internet. Individuals should be free to contract and communicate on the Internet without the possibility of government tracking, even if the government does not intend to use the technology in that way.

Citizens need to be aware of the differences in Internet laws and the implications that those differences have on their privacy and anonymity rights as they currently exist. Internet privacy is already on precarious grounds due to private companies, but it should not be eroded any further by government action. The convenience of Internet transactions with digital signatures does not have to result in a loss of privacy, but both citizens and government will have to act to ensure that anonymity, pseudonymity, and privacy continue to exist on the Internet.

199. Janice A. Alwin, Comment, *Privacy Planning: Putting the Privacy Statutes to Work for You*, 14 DEPAUL BUS. L.J. 353, 373 (2002).

200. Swire, *supra* note 92, at 473 (discussing harms of government surveillance of financial transactions and stating "[p]olitical opponents, disfavored minorities, and powerless people generally could be targeted for exploitation by government officials").

201. *Id.* at 474. "[C]onsumers who are concerned about the safety of transmitting their credit card numbers over the Internet will tend to avoid Internet purchases." *Id.*

202. *See supra* note 194 and accompanying text.