

PRIORITIZING PRIVACY: A CONSTITUTIONAL RESPONSE TO THE INTERNET

By Elbert Lin[†]

ABSTRACT

Beginning with the well-established notion that the Internet threatens informational privacy, this Article takes several uncharted steps toward the conclusions that the Internet calls for a constitutional right to informational privacy and that that right should first be sought in the state constitutions. As a foundation, this Article departs from the traditional conception of informational privacy as control over the disclosure of personal information. Rather, informational privacy is discussed as more strongly concerned with the use and dissemination of personal information.

Ultimately, this Article determines that the intersection of the Internet and informational privacy must be addressed at a constitutional level. A statute or some other solution might address the Internet as a technology alone. However, beyond its unprecedented information gathering and other capabilities, the Internet pervades all facets of life. As such, it has made informational privacy more than an infrequent concern of, say, financial or medical records. Informational privacy is now a universal and generalized interest. It requires a legal commitment that can only be accomplished through constitutional protection. This Article finds, however, not only the well-known fact that the federal constitutional right to informational privacy is weak, but also that the state constitutional right is weak. An unprecedented examination of the ten states whose constitutions contain explicit rights to privacy reveals that they offer little protection for informational privacy.

Given the need for a constitutional right, though, this Article focuses on the states. A few states have taken the first step toward greater protections by applying their constitutional rights of informational privacy to private actors. Moreover, the state constitutions have historically been the laboratories for federal constitutional interpretation, thus they provide an ideal place for privacy rights to develop and evolve.

© 2002 Elbert Lin

[†] J.D. Candidate, 2003, Yale Law School; B.A., 1999, Yale College; 2003-2004 law clerk to the Honorable Robert E. Keeton, Judge, U.S. District Court, District of Massachusetts. Thank you to Anita Allen-Castellito for her comments and encouragement.

I. INTRODUCTION

It is hardly novel to say that the Internet poses a severe threat to informational privacy. For years, academics and commentators have been foretelling the advent of “Big Brother,” warning that the worst of George Orwell’s fictional *Nineteen Eighty-Four* surveillance state¹ had become, or was approaching, reality.² Some have brought the metaphor closer to the privacy problem that the Internet truly poses—the collection and dissemination of information by private companies—in referring to it as the threat of “Little Brother.”³ Still others have applied wholly different metaphors.⁴

1. See generally GEORGE ORWELL, *NINETEEN EIGHTY-FOUR* (1949). Orwell’s book foretells a future where Big Brother is the omnipresent and omniscient government. Big Brother re-wrote history (“Doublethink”), fashioned and implemented its own language (“Newspeak”), and burned books. Big Brother maintains its grip on the minds of its population through a stifling use of surveillance technology. There are cameras and hidden microphones everywhere—even a telescreen in one’s private home. Perhaps the single most recognizable, and chilling, phrase from *Nineteen Eighty-Four* is “Big Brother Is Watching You.”

2. See, e.g., Matthew D. Bunker et al., *Access to Government-Held Information in the Computer Age: Applying Legal Doctrine to Emerging Technology*, 20 FLA. ST. U. L. REV. 543, 582 (1993); Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 293 (2001); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1395 (2001); George B. Trubow, *Protecting Informational Privacy in the Information Society*, 10 N. ILL. U. L. REV. 521, 522 (1990). Daniel Solove labels Orwell’s Big Brother “[t]he most widely discussed metaphor in the discourse of information privacy.” Solove, *supra*, at 1413.

3. See, e.g., The Honorable Ben F. Overton & Katherine E. Giddings, *The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection from Private and Commercial Intrusion*, 25 FLA. ST. U. L. REV. 25, 27 (1997) (“Today, we are cautioned to look out for ‘little brother’ and ‘little sister.’”); Solove, *supra* note 2, at 1396 (“Commentators have adapted the Big Brother metaphor to describe the threat to privacy caused by private sector databases, often referring to private sector entities as ‘Little Brothers.’”). This is not to say Big Brother does not pose a threat on the Internet. One noteworthy concern is the effect government surveillance will have on online political discussion. See, e.g., Helms, *supra* note 2, at 293 (“Anonymity and fear of ‘Big Brother’ tracking one’s every move on the Internet have received significant attention from scholars”).

4. See, e.g., Solove, *supra* note 2, at 1413-19. Solove dismisses the Big Brother metaphor as an improper characterization of the threat to information privacy. *Id.* at 1417-22 (arguing the more proper metaphor to characterize the threat is how information is collected and distributed, “with little intelligent control or limitation” by the faceless uncaring bureaucracy portrayed in FRANZ KAFKA, *THE TRIAL* (Willa & Edwin Muir trans., Knopf 1937)); see also Helms, *supra* note 2, at 291-93 (commenting on the use of another version of Big Brother—Jeremy Bentham’s Panopticon).

PRIORITIZING PRIVACY

Indeed, privacy concerns have led one commentator to compare the Internet to a fascist state that rivals those of Hitler and Stalin.⁵

Metaphors notwithstanding, the threat is very real. What one does on the Internet is far from private. The dean of the Harvard Divinity School was forced to resign after it was discovered he had downloaded pornography on his home computer.⁶ Meanwhile, a 1998 case involving a Navy man who was discharged for his Internet activities demonstrated how Internet Service Providers could be weak links in the chain of privacy.⁷ In fact, the Internet Service Provider NetZero actually boasts: “What we offer our advertisers [is] . . . an audience that we know intimately because they allow us to follow them wherever they roam on the Internet.”⁸ As Scott McNealy, the Chief Executive Officer of Sun Microsystems, Inc., has been famously quoted as saying: “You have zero privacy. Get over it.”⁹

The public is well aware of the Internet’s threat to informational privacy. According to the Federal Trade Commission (“FTC”), a recent survey indicated that ninety-two percent of Americans are “concerned about threats to their personal privacy when they use the Internet” and seventy-two percent are “very concerned.”¹⁰ The market has responded to the public’s growing concern by developing privacy enhancing technologies (“PETs”), programs that purport to allow consumers to “surf in secrecy,”¹¹ advertised ubiquitously in pop-up and banner advertisements on the Inter-

5. Margaret Ann Irving, *Reorganization of the Internal Revenue Service: Managing Information Privacy in the Information Age*, 53 ADMIN. L. REV. 659 (2001) (quoting Robert Scheer, *Nowhere to Hide*, YAHOO! Internet Life, Oct. 2000, at 100) (“[Anyone] on the Internet can find out more about what you read, think, and learn than Joseph Stalin or Adolf Hitler, with their fearsome secret police, could ever have learned about the inhabitants of their totalitarian states”).

6. See JEFFERY ROSEN, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA* 159-61 (Vintage Books 2001) (2000) (“The real lesson of the Divinity School scandal wasn’t legal but technological: the dean’s downfall reminds us how much of our reading habits on the Internet are exposed to public view”).

7. In *McVeigh v. Cohen*, 983 F. Supp. 215 (D.D.C. 1998), McVeigh sued America On-Line (AOL) and the United States Navy for the unauthorized disclosure and receipt of stored electronic communications service records. AOL allegedly provided the Navy the real-life identity behind McVeigh’s AOL Internet alias. *Id.* at 217.

8. Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1283 (2000).

9. A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1462 (2000).

10. *Federal Trade Commission Materials*, 1241 PRACTISING L. INST./CORP. 731, 762 (2001) [hereinafter *FTC Materials*].

11. HistoryKill Affiliate Ads, <http://www.historykillcash.com/banners> (last visited July 18, 2002).

net. Although the Internet came into popular use no more than ten years ago, it is not uncommon today to proclaim that the Internet is a threat to informational privacy.¹²

What remains novel, however, is the argument for a federal constitutional right to informational privacy on the Internet. Only a handful of scholars¹³ have suggested that the United States Supreme Court will strengthen its lukewarm hint at a constitutional right to informational privacy in *Whalen v. Roe*, in 1977.¹⁴ Moreover, only a few of those scholars call for the right with regard to the Internet. Similarly, only a small number of commentators have recommended a *state* constitutional right to informational privacy.¹⁵ Most commentators have eschewed federal and state constitutional rights as possible solutions to the increasing technological threat to informational privacy, either dismissing them as weak

12. Froomkin points out, however, that the fact “[t]hat surveillance technologies threaten privacy may not be breaking news, but the extent to which these technologies will soon allow watchers to permeate modern life still has the power to shock.” Froomkin, *supra* note 9, at 1465.

13. See David H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 CASE W. RES. L. REV. 831, 852 (1991) (“The ultimate protection for the individual must lie in the constitutional entrenchment of rights to privacy, data protection, and informational self-determination”); Francis S. Chlapowski, Note, *The Constitutional Right to Informational Privacy*, 71 B.U. L. REV. 133, 135 (1991) (“[T]his Note argues that the interest in informational privacy is a right that the Constitution protects [and] . . . that a new level of scrutiny . . . should be recognized”); Thomas B. Kearns, Note, *Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns*, 7 WM. & MARY BILL RTS. J. 975, 1003 (1999) (calling for a “change in constitutional interpretation” to “align privacy interests and privacy rights”). Richard Turkington has argued that the right, which he calls the “unencumbered constitutional right to informational privacy,” already exists. Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479, 496-502 (1990). In addition, while neither advocating nor dismissing the constitutional right, Susan Gindin has proclaimed, “[I]t seems likely the Supreme Court will hold that the Constitution protects a right of informational privacy.” Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1185 (1997); see also Kyla Kitajima, Note, *Electronic Filing and Informational Privacy*, 27 HASTINGS CONST. L.Q. 563, 581 (2000) (“Because Internet growth and increased access to information will persist, the Supreme Court may soon have to decide whether an informational privacy right actually exists”).

14. 429 U.S. 589 (1977). See also discussion *infra* Part III.A on the opinion in *Whalen* and the current status of the federal constitutional right to informational privacy.

15. See Overton & Giddings, *supra* note 3, at 53 (advocating a constitutional amendment to make Florida’s right to informational privacy applicable to private parties); see also Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1431 (“[O]ne of the significant features of privacy in the next few decades will be that new technology . . . will push more and more cutting-edge issues into the states”).

PRIORITIZING PRIVACY

(and presumably incapable of change)¹⁶ or contending that a constitution is ill-equipped to protect against privacy-destroying technologies.¹⁷ Rather, the debate over informational privacy—on the Internet, in particular—oscillates between industry self-regulation and government legislation, though support increases for other solutions, such as casting privacy as a property right or expanding the privacy torts.¹⁸

This Article will argue that a constitutional right to informational privacy is necessary and appropriate for protecting privacy on the Internet. Moreover, given the progress they have already made, and their receptiveness to experimentation, the state constitutions are and should continue to be the testing grounds for an eventual federal constitutional right to informational privacy on the Internet. Part II lays out the threat posed by the Internet and computers to informational privacy, defining the contours of “informational privacy,” the computer technology that threatens informational privacy, and the threat itself, and focusing less on the disclosure aspect and more on the dissemination and use of personal information. In closing, Part II notes that online privacy is the most significant informational privacy concern. Part III argues that the Internet has created the need for a constitutional right by elevating informational privacy to a generalized concern. Part III also examines the failure of the current, nonconstitutional legal regime to address the threat of the Internet. Part IV discusses the current state of the constitutional right to informational privacy, considering both the federal and state constitutions, and surveying in detail the constitutional rights in the eleven most noteworthy states, ten of which have explicit constitutional provisions for privacy. The right has not been utilized in Internet litigation and offers the lack of a generalized interest in privacy as a reason for the current weakness in both the federal and state constitutional rights. Part V determines that the constitutional right can best be developed in the states. The leading states have already developed robust constitutional rights, and constitutional experimentation is an ac-

16. See, e.g., FRED H. CATE, *PRIVACY IN THE INFORMATION AGE* (1997). Information law scholar Fred Cate concluded that “[t]he U.S. Constitution . . . offers little support for information privacy.” *Id.* at 66. “Even the most protective state constitutional provisions . . . have yielded little protection for information privacy.” *Id.* at 68.

17. See, e.g., CATE, *supra* note 16; Froomkin, *supra* note 9. Froomkin argues that “the United States Constitution is unlikely to be the source of a great expansion in informational privacy rights” because “privacy-destroying technologies do not line up particularly well” with what the Constitution is designed to protect. *Id.* at 1540-41. With regard to state constitutions, Cate, among others, points out that “in the context of global information networks and national and multinational information users, state protection is of limited significance.” CATE, *supra* note 16, at 68.

18. See Litman, *supra* note 8, at 1283.

cepted premise at the state level. Part VI concludes the Internet has altered the interest in informational privacy such that constitutional protection is necessary and, furthermore, it is best sought first through the state constitutions.

II. THE THREAT TO INFORMATIONAL PRIVACY

While the Internet has been in popular use for less than ten years, the notion that computers in general might cause unwanted losses of informational privacy has been well established.¹⁹ Recently, rapidly improving technology has vaulted us into an “information age” where information is “the lifeblood that sustains political, social, and business decisions.”²⁰ For instance, in 1997, over 550 companies had “information” as their product.²¹ In a sort of chicken-and-egg debate, some commentators contend that technology has transformed the very nature of information and made it more valuable,²² while others believe that technology has simply made

19. As early as 1973, the United States Department of Health, Education, and Welfare released a study that documented “threats to individual privacy” caused by computerized federal databases. Trubow, *supra* note 2, at 523. In fact, since the 1970s, European and North American legislatures implemented numerous laws regulating particular effects of computers. Flaherty, *supra* note 13, at 834. The earliest arguably “Internet related” legislation was the United States’ Electronic Communications Privacy Act of 1986 (the ECPA). 18 U.S.C. §§ 2510-2520, 2701-2709 (1997). The ECPA adapted the federal regulation of electronic surveillance to new technologies. It was designed with e-mail specifically in mind. RICHARD C. TURKINGTON & ANITA L. ALLEN, *PRIVACY LAW: CASES AND MATERIALS* 229-30 (1999). The leading United States Supreme Court case on the constitutional right to informational privacy also dates from the 1970s and regarded a computerized medical database. *See Whalen v. Roe*, 429 U.S. 589 (1977). The Court specifically noted that they were “not unaware of the threat to privacy implicit in . . . computerized data banks or other massive government files.” *Id.* at 605. According to George Trubow, “The notion of ‘informational privacy,’ a development of the 1970s, was spawned by the remarkably constant improvement and growing pervasiveness of the digital computer and electronic data banks.” Trubow, *supra* note 2, at 521; *see also* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 *STAN. L. REV.* 1193, 1199 (1998) (“[F]or the past three decades, many have warned about the privacy dangers posed specifically by the computer.”); Solove, *supra* note 2, at 1394 (“Since their creation, computer databases have been viewed as problematic—a fear typically raised under the mantra of ‘privacy’”).

20. CATE, *supra* note 16, at 5 (quoting Anne W. Branscomb, *Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition*, 36 *VAND. L. REV.* 985, 987 (1983)) (quotation marks omitted).

21. Gindin, *supra* note 13, at 1162.

22. *See id.* (“Information has taken on a new character . . . [and] passed from being an instrument through which we acquire and manage other assets to being a primary asset itself.”) (quoting ANNE WELLS BRANSCOMB, *WHO OWNS INFORMATION? FROM PRIVACY TO PUBLIC ACCESS* 1 (1994)).

PRIORITIZING PRIVACY

previously valuable information easier to trade.²³ Regardless, it is clear that information, including personal information, is in higher demand than ever before.²⁴ However, computer technology, digitalization in particular, has decreased the cost of, reduced the space necessary for, and increased the speed of, information storage and transfers, resulting in the widespread collection and trading of information.²⁵

The Internet lies at the crossroads of the concern about the effect of computers on informational privacy and the exponential need for information. It is simultaneously the largest computer in the world²⁶ and the most efficient trading ground for information.²⁷ The fact that the Internet poses a threat to informational privacy should be beyond dispute.²⁸ However, many “seek reassurance in the notion that, as unimportant peons with no public profile, [their] personal information is not of sufficient interest to anyone to collect, compile or correlate.”²⁹ This Part attempts to define informational privacy and spell out the threat posed by computers and the

23. See Leslie A. Kurtz, *The Invisible Becomes Manifest: Information Privacy in a Digital Age*, 38 WASHBURN L.J. 151, 152 (“Information has long been a commodity, and mailing lists have been bought and sold. But today, it is far easier to generate, organize and deliver this information”).

24. Chlapowski, *supra* note 13, at 133 (“The advent of the Information Age has precipitated the commodification of virtually all types of personal information.”); see also CATE, *supra* note 16, at 2 (“[O]thers know more about you—even things you may not know about yourself—than ever before”).

25. E.g., Bunker et al., *supra* note 2, at 582 (“This information explosion is due partly to the drastic reduction of space needed for record-keeping”); Kurtz, *supra* note 23, at 152 (noting that “today, it is far easier to generate, organize and deliver . . . information”). Cate proclaims that “[t]he practical ability to create, manipulate, store, transmit, and link digital information is the single most influential innovation of the twentieth century.” CATE, *supra* note 16, at 5.

26. See Jay Krasovec, *Cyberspace: The Final Frontier, for Regulation?*, 31 AKRON L. REV. 101, 103 (1997) (“The Internet . . . is ‘a loose collection of millions of computers at sites throughout the world sharing information and files.’ . . . Thousands upon thousands of local networks then connect, with communication software managing the communications between them”).

27. See Kang, *supra* note 19, at 1223 (“The networked personal computer will become the one-stop information appliance for all types of transactions that now take place in the physical world”); see also Elizabeth deGrazia Blumenfeld, *Privacy Please: Will the Internet Industry Act to Protect Consumer Privacy Before the Government Steps In?*, 54 BUS. LAW. 349, 350 (1998) (noting that “the information superhighway’s inherent potential to become the next commercial marketplace”).

28. Internet and computer databases have obvious benefits, of course, but weighing the benefits of computer technology against the costs of informational privacy is beyond the scope of this Article. I will assume, as do most commentators, that the costs are sufficiently significant to warrant discussion.

29. Litman, *supra* note 8, at 1285.

Internet for those who take comfort in such perceived anonymity, thereby also providing the necessary foundation for an intelligent discussion of a potential constitutional solution to the threat to informational privacy.³⁰

A. Informational Privacy

Defining informational privacy is a dizzying endeavor. As information law scholar Fred Cate noted, “for all of the passion that surrounds discussion about privacy, and the recent attention devoted to electronic privacy, surprisingly little consensus exists regarding what ‘privacy’ means”³¹ In the five years that have passed since Cate wrote this, the definitions have done everything but converge. The underlying problem appears to be that “privacy” is an extremely broad concept³² and that informational privacy is but one segment of “privacy.” This raises two distinct issues.

First, there is no consensus on the interests that comprise privacy.³³ For instance, Jerry Kang describes three “clusters”—privacy concerns with regard to (1) physical space (“spatial privacy”), (2) choice, and (3) the flow of personal information.³⁴ However, Anita Allen-Castellitto divides

30. See Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 816 (2000) (“I turn to the development of a substantive concept of information privacy. This task is inescapable; the merits of different regulatory regimes are only understandable in reference to a sought after outcome”).

31. CATE, *supra* note 16, at 3; see also Flaherty, *supra* note 13, at 834 (“The essential distinction between privacy protection and data protection, or informational privacy, is not commonly understood”).

32. See Kang, *supra* note 19, at 1200 (noting that there are “equivocations latent in the term ‘privacy’”).

33. By “interests,” I mean simply the aspects of life in which one *can have* or might expect privacy. For instance, it is possible to be private “physically” by being alone. This seems intuitively different in some way from being private “decisionally.” My point is that there is little consensus on the *categorizations* of how one can be private. At a more fundamental level and outside the scope of this Article is the question of why certain privacy interests should or should not be valued. See generally ANITA L. ALLEN, *UNEASY ACCESS* 35-52 (1988); PATRICIA BOLING, *PRIVACY AND THE POLITICS OF INTIMATE LIFE* (1996); JULIE INNESS, *PRIVACY, INTIMACY, AND ISOLATION* (1992); PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY (Ferdinand Schoeman ed., 1984). On the contrary, there does appear to be consensus on this broader normative “definition.” “The idea that moral respect for persons demands broad protection for privacy appears in many of the most influential accounts of the value of privacy.” TURKINGTON & ALLEN, *supra* note 19, at 28.

34. Kang, *supra* note 19, at 1202-03; see also William C. Heffernan, *Privacy Rights*, 29 SUFFOLK L. REV. 737, 745 (1995) (denoting the “three constituent parts” of privacy as “the privacy of autonomous personal life, privacy-as-seclusion, and privacy-as-informational-control”). Heffernan adds a higher level of distinction by labeling “privacy-as-seclusion” and “privacy-as-informational-control” as “mechanisms of privacy” and “the privacy of autonomous personal life” as a “conduct component.” *Id.* at 745-46.

PRIORITIZING PRIVACY

privacy into “at least four basic types”: (1) informational privacy, (2) physical privacy, (3) decisional privacy, and (4) proprietary privacy.³⁵ Meanwhile, the fathers of privacy law, Samuel Warren and Justice Louis Brandeis, described a “general right to privacy for thoughts, emotions, and sensations [that] should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression.”³⁶

Second, the segmenting of one or a portion of those interests into the sub-title “informational privacy” is difficult because the interests all interconnect.³⁷ Any definition of informational privacy thus seems, at best, debatable and, at worst, arbitrary. This Article will try to find either the middle ground or the least common denominator on the theory that that will encompass the least disputed, and therefore most essential, elements of informational privacy.

In seeking a definition for informational privacy, it is useful to begin with the United States Supreme Court’s leading case on the issue, *Whalen v. Roe*.³⁸ In *Whalen*, the Court separated the constitutional right to privacy into at least two interests: “the individual interest in avoiding disclosure of personal matters, and . . . the interest in independence in making certain kinds of important decisions.”³⁹ The former—avoiding disclosure of personal matters—has been widely acknowledged as the Court’s definition of

35. Anita L. Allen-Castellitto, *The Origins and Growth of U.S. Privacy Law*, 632 PRACTISING L. INST./PATENTS 9, 16 (2001). Allen-Castellitto has separated out the interest in propriety privacy, the “issue in cases about publicity rights, identity, and the ownership of the body.” *Id.* at 17; *see also* Gormley, *supra* note 15, at 1337-38. Gormley finds four definitional clusters in the scholarship: (1) privacy as personhood; (2) privacy as autonomy; (3) privacy as the “ability to regulate information about [oneself];” and (4) privacy as several “essential components,” such as “secrecy, anonymity and solitude.” *Id.* (quotation marks omitted).

36. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 206 (1890).

37. *See* CATE, *supra* note 16, at 19 (“The fear of compulsory disclosure may very well influence [the] freedom to engage in independent action.”); *see also* Kang, *supra* note 19, at 1203-04 (acknowledging that the clusters are “functionally interconnected” and recognizing that “a serious argument can be made that all three and additional privacy clusters can be integrated into a single, abstract cluster”). Kang points out that in focusing on informational privacy, he takes no position on the ultimate definition of privacy in general. *Id.* at 1204-05. I make the same claim.

38. 429 U.S. 589 (1977) (determining the constitutionality of a New York statute that required all prescriptions for a certain class of drugs be reported to the state Department of Health, the computerized records of which contained the names and addresses of the drug recipients).

39. *Id.* at 599-600.

informational privacy.⁴⁰ The vast majority of commentators have adopted a very similar definition,⁴¹ conceptualizing informational privacy as a right to control the flow of personal information.⁴²

However, a relatively new camp has begun to criticize the privacy-as-control definition of informational privacy.⁴³ Absolute control over one's personal information seems logically to include the unilateral ability to relinquish control. As a result, the privacy-as-control definition of informational privacy is frequently interpreted as a property right in one's personal information.⁴⁴ The critics argue that this property view of informa-

40. See, e.g., Bunker et al., *supra* note 2, at 587 (noting that the *Whalen* Court recognized an "informational privacy 'interest'"); Jonathan P. Cody, Comment, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183, 1195 (1999) (noting that the Court "touch[ed] upon [informational privacy]" in *Whalen*).

41. See Bunker et al., *supra* note 2, at 585 (supporting the definition of "controlling the flow of information about him- or herself" with a citation to *Whalen*).

42. Kang, *supra* note 19, at 1205 (noting that a privacy as control definition is "consistent with a broad swath of academic and policy thinking"); Schwartz, *supra* note 30, at 820 ("The weight of the consensus about the centrality of privacy-control is staggering"). One example is Alan Westin's early definition from his book *Privacy and Freedom*: "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others." CATE, *supra* note 16, at 22 (quoting ALAN F. WESTIN, *PRIVACY AND FREEDOM* (1967)); see also Flaherty, *supra* note 13, at 832 ("Westin provides the most useful identification of the interests at stake in . . . informational privacy"). President Clinton's Information Infrastructure Task Force adopted a nearly identical definition. Kang, *supra* note 19, at 1205. The running theme is that of control over personal information. See, e.g., CATE, *supra* note 16, at 22 ("[A] key element[] of this definition [is] its focus on control of information"); Froomkin, *supra* note 9, at 1463 ("[I]nformational privacy' [is] shorthand for the ability to control the acquisition or release of information about oneself"); Irving, *supra* note 5, at 661 ("An individual has the right to control the conditions under which information pertaining to him is collected, used, and disseminated"); Kang, *supra* note 19, at 1205 ("Information privacy is 'an individual's claim to control the terms under which personal information . . . is acquired, disclosed, and used'"); Turkington, *supra* note 13, at 487 ("[T]he right's major principle the claim of a person to a right to decide who shall have access to personal or intimate information about her"); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1050 (defining information privacy as "my right to control your communication of personally identifiable information about me").

43. Schwartz argues that "the . . . debate about Internet privacy has employed a deeply flawed rhetoric." Schwartz, *supra* note 30, at 815.

44. See *id.* at 820 ("Privacy-control . . . encourages a property approach to personal information that transforms data into a commodity."); Solove, *supra* note 2, at 1446 ("Theorists who view privacy as control over information frequently understand it within the framework of property and contract concepts").

PRIORITIZING PRIVACY

tional privacy fails to protect privacy both by creating improper incentives⁴⁵ and by misplacing the threat to informational privacy.⁴⁶ More fundamentally, allowing “individual stewardship”⁴⁷ of personal information on the Internet does not take into account the high transaction costs, information asymmetries, or bounded rationality facing consumers.⁴⁸

Among others, Paul Schwartz and Daniel Solove offer competing theories of informational privacy. Instead of privacy-as-control, Schwartz conceives of informational privacy as a “constitutive value.”⁴⁹ Solove also eschews the conception of informational privacy as strictly a right to individual control. Rather, he sees informational privacy as a right to have one’s information “treated thoughtfully,” to understand the disclosures of one’s personal data, and to participate meaningfully in the use of that data.⁵⁰

45. Allen, for instance, points to the numerous webcam sites on the Internet as fuel for her concern that people with control over their own privacy may simply choose to surrender it. *See* Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 867-69 (2000).

46. *See* Schwartz, *supra* note 30, at 828-30. Solove argues that this vision misses the real problem with databases—“the uses and practices associated with our information.” Solove, *supra* note 2, at 1439. The “ownership model” is caught up in the immediate transaction—whether the information is disclosed or not—and fails to recognize the long-term consequences. *Id.* at 1452.

47. Schwartz, *supra* note 30, at 820.

48. *Id.* at 821-28; Solove, *supra* note 2, at 1452-53. For instance, Solove observes that individual consumers are not only unable to adequately assess the future value of specific pieces of personal information, but they are also unable to appropriately internalize the ultimate effect of the aggregation of seemingly innocuous bits of information. *Id.* at 1452. Moreover, “the process of information collection in America is clandestine, duplicitous, and unfair. The choices given to people over their information are hardly choices at all.” *Id.* at 1426. This problem with the property view of informational privacy is so insidious that some commentators who favor a strong element of individual control of personal information (but not a property regime) have added their criticism. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject As Object*, 52 STAN. L. REV. 1373, 1396-1401 (2000) (debunking the illusion of consumer empowerment); Froomkin, *supra* note 9, at 1501-05 (describing the individual’s “myopia” when it comes to the alienation of personal information); Litman, *supra* note 8, at 1301 (“Market solutions based on a property rights model won’t cure [the informational privacy problem], they’ll only legitimize it”).

49. Schwartz, *supra* note 30, at 834. Schwartz proposes creating boundaries—“information territories”—to “stimulate or discourage different kinds of social expression and action,” but not to serve as “data fortress[es].” *Id.*

50. *See* Solove, *supra* note 2, at 1461.

The easy common thread here is that informational privacy concerns “personal information.”⁵¹ In general, this encompasses any information that is identifiable to an individual.⁵² This includes both assigned information, such as a name, address, or social security number, and generated information, such as financial or credit card records, medical records, and phone logs.⁵³ For the purposes of this Article, personal information will be defined as any information, no matter how trivial, that can be traced or linked to an identifiable individual.⁵⁴

In addition to this component of personal information, the foregoing conceptions of informational privacy share a concern with the *consequences*—both real and perceived—of disclosure. That is, not merely that information has been revealed, but that the information will be used in many undesired and unexpected ways. For instance, an essential part of the privacy-as-control definition is that absolute control grants informational autonomy—the ability to determine one’s data self.⁵⁵ “Privacy-control seeks to achieve informational self-determination through individual stewardship of personal data, and by keeping information isolated from access.”⁵⁶ Meanwhile, Solove’s noncontrol, right to be treated

51. Kang, *supra* note 19, at 1206 (“[The] central component of . . . nearly all definitions of information privacy is the term ‘personal information’”).

52. See James T. Sunosky, *Privacy Online: A Primer on the European Union’s Directive and United States’ Safe Harbor Privacy Principles*, 9 CURRENTS: INT’L TRADE L.J. 80, 81; Trubow, *supra* note 2, at 521.

53. Kearns, *supra* note 13, at 976-77. There is some debate over how intimate or sensitive personal information must be, perhaps reflecting the judiciary’s reluctance to protect a wide expanse of information. See Kang, *supra* note 19, at 1206-07 (“[P]ersonal’ does not mean especially sensitive private, or embarrassing”). *But see* Sunosky, *supra* note 52, at 81 (“Personal information refers to . . . information that is likely to be the most intimate details of an individual’s life”). Discussion *infra* Part III on the judiciary’s protection of personal information..

54. After quickly adopting the privacy-as-control definition for informational privacy, Kang notes that the term “personal information” is the “least self-explanatory” element of informational privacy. Kang, *supra* note 19, at 1205-06. For an in-depth analysis of personal and non-personal information, see *id.* at 1206-11.

55. See Chlapowski, *supra* note 13, at 154 (“Informational privacy should be protected under the right to privacy because it is an element of personhood, integral to an individual’s identity . . . [It is] the freedom from being coerced into a definitive identity”); Kearns, *supra* note 13, at 983 (“Information privacy is based on an autonomist view of individuals in which personal data are included as part of the ‘self.’ In this view, the right to privacy protects the information that comprises a person’s ‘data image.’” (citation omitted)).

56. Schwartz, *supra* note 30, at 820; see also Heffernan, *supra* note 34, at 746 n.67 (“The key to privacy-as-informational-control is that it allows for mobility of one’s person”). Cohen, for instance, argues that to “value[] the individual as an agent of self-determination and community-building,” one must “take seriously a conception of data

PRIORITIZING PRIVACY

thoughtfully springs from a concern about “the uses and practices associated with our information.”⁵⁷ Finally, Schwartz’s constitutive value also rises from the recognition that “access to personal information and limits on it help . . . shape our individual identities.”⁵⁸

The various definitions differ primarily in the *way* in which they cope with the consequences of disclosure. At some level, though, they all seem to aim at Solove’s complaint, that computer technologies resemble Kafka’s *The Trial*—once information is disclosed, it is used and abused with no sense of purpose or reason.⁵⁹ The privacy-as-control advocates want to return control to the individual; Solove seeks to restore the sense that one’s information is “treated thoughtfully”⁶⁰; and Schwartz hopes to corral the use of information into directed norm-building by defining clear

privacy that returns control over much personal data to the individual.” Cohen, *supra* note 48, at 1377.

Indeed, even in *Whalen*, the Supreme Court’s imprimatur on privacy-as-control, the undercurrents are about the perceived *consequences* of disclosure. The plaintiffs argued that “[t]he mere existence in readily available form of the information . . . creates a genuine concern that the information will become publicly known and that it will adversely affect their reputations.” *Whalen v. Roe*, 429 U.S. 589, 600 (1977). Furthermore, this concern will cause patients to avoid getting medication, effectively restraining the “making of decisions about matters vital to the care of their health.” *Id.* Solove actually believes the Court wholly missed these undercurrents about the consequences of disclosure (specifically, the possibility of further use), affecting the outcome of *Whalen*.

The plaintiffs’ argument, however, was not that disclosure was the real privacy problem. Rather, the plaintiffs were concerned that the collection of and greater access to their information made them lose control over their information. A part of themselves—a very important part of their lives—was placed in the distant hands of the state and completely outside of their control.

Solove, *supra* note 2, at 1436. Solove’s argument is particularly interesting in that he may be challenging the Court’s division of informational privacy from the more accepted concept of privacy based on decisional autonomy. I would stand by the proposition that informational privacy is in fact also grounded in decisional autonomy, but that is a topic for another forum.

57. Solove, *supra* note 2, at 1439.

58. Schwartz, *supra* note 30, at 834. *But see* Volokh, *supra* note 42, at 1056. Volokh, who is concerned about the First Amendment ramifications of restrictions based on informational privacy, believes that protection against secondary disclosures is not out of concern for the consequences. He argues that “[t]he felt injury . . . is the perceived indignity or intrusion flowing from the very fact that people are talking about you or learning about you, and not the embarrassment flowing from the fact that people are learning things that reflect badly on you.” *Id.* Volokh’s error is that embarrassment is the only consequence against which he can envision protection.

59. *See generally* KAFKA, *supra* note 4.

60. *See supra* text accompanying note 50.

“information territories.”⁶¹ The least common denominator is a desire to have one’s information treated with an understandable purpose.

Superficially, this can begin to sound a lot like privacy-as-control. Even Solove says, “Perhaps the most appropriate notion of privacy for databases is that of ‘control of personal information.’”⁶² He goes on to say, however, that “[though] [t]heorists who view privacy as control over information frequently understand it within the framework of property and contract concepts . . . [t]his is not the only way control can be understood.”⁶³ This is a control of personal information, insofar as somebody defines the consequences of disclosure, but it is certainly not the “right of control” that Schwartz, Solove, and others adamantly reject.⁶⁴ It is grounded in a sense of decisional autonomy that is much less literal than the simple ability to regulate the on-off valve for one’s personal information. It is not control, *per se*; rather, it is not a lack of control. An individual is not necessarily in direct control of her personal information, but she is at least on notice as to the bounds and parameters within which her information, once disclosed, may be used.

Informational privacy is a right to understand the real and perceived consequences of the disclosure of personal information.⁶⁵

B. Big Brother, Little Brother, the Whole Darn Family Is Watching

Like a multi-fronted assault, the threat to informational privacy posed by the technological weapons available from computers and on the Internet seems as broad as the definition of informational privacy.⁶⁶ Much of

61. Schwartz, *supra* note 30, at 834.

62. Solove, *supra* note 2, at 1445.

63. *Id.* at 1446.

64. Schwartz, *supra* note 30, at 834.

65. I would be remiss if I concluded a discussion on the definition of informational privacy without mentioning those who would not protect informational privacy. While advocates argue that informational privacy is instrumental to personhood, *see* Chlapowski, *supra* note 13, at 160, critics, such as Judge Richard Posner, argue that it is instrumental to economically inefficient deception and lying. *See* Richard A. Posner, *An Economic Theory of Privacy*, in TURKINGTON & ALLEN, *supra* note 19, at 244. Indeed, some commentators have acknowledged Posner’s concern (though they lack his distaste for economic inefficiency). *See* CATE, *supra* note 16, at 23 (recognizing the “inherent neutrality” in informational privacy and that therefore “[t]he information that individuals, groups, or institutions choose to communicate . . . may be true or false, significant or trivial, meaningful or misleading”).

66. For a much more thorough analysis of privacy-invading technologies and their impacts, *see* generally Froomkin, *supra* note 9, at 1468-1501; Gindin, *supra* note 13, at 1156-74; and Kang, *supra* note 19, at 1220-45.

PRIORITIZING PRIVACY

the technology, however, is information-gathering and as such is, strictly speaking, a direct threat only of unwarranted disclosures. As this Article has defined it, informational privacy is not concerned with unwarranted disclosures. The real threat to informational privacy arises from the technologies that come into use once the information has been collected.⁶⁷ This narrows the technological threat to one major source: computer databases. Digitalized information is easier to manipulate, analyze and synthesize, transmit, and store; it is easier to use and abuse without a sense of purpose or reason.

1. *Computer Databases*

Computer databases store, sort, and process information in such a way that they transcend both temporal and spatial restrictions. Stored in a database, information once valuable only in real time can be compiled to reconstruct the past, decipher patterns, and serve as evidence.⁶⁸ As Froomkin has said, “Databases multiply the effects of [real time] sensors.”⁶⁹ Now, the advent of the Internet has multiplied the effects of databases, linking hundreds and thousands of databases into one giant database.

Perhaps the most significant threat posed by computer databases is the destruction of “practical obscurity,”⁷⁰ sometimes referred to as “anonymity through obscurity.”⁷¹ Previously, the physical restraints of time and space prevented gross violations of informational privacy. For instance, paper records are often filed in numerous locations, are easy to misplace or permanently destroy, and require a great deal of effort to gather and sort.⁷² Furthermore, even the best efforts at thorough collection of paper records are likely to remain incomplete. Computer databases changed this

67. Of course, information gathering, especially that which is done surreptitiously and on a large scale, contributes to and aggravates the threat to informational privacy. Indeed, most of the data gathered on the Internet is collected in such a way as to facilitate secondary transfers and uses—to increase the potential for consequences of disclosure. See Kang, *supra* note 19, at 1199 (“All these data generated in cyberspace are detailed, computer-processable, indexed to the individual, and permanent”). As Froomkin aptly put, “Once created or collected, data is easily shared and hard to eradicate; the data genie does not go willingly, if ever, back into the bottle.” Froomkin, *supra* note 9, at 1469. Recognizing these facts, a brief survey of computer- and Internet-based information-gathering technologies will be conducted later in this Part. For an interesting list of the “many dangers” created by the “collection and collation of large amounts of personal data,” see *id.* at 1471-72.

68. See Froomkin, *supra* note 9, at 1480.

69. *Id.* at 1468.

70. Bunker et al., *supra* note 2, at 583 (quotation marks omitted).

71. Kearns, *supra* note 13, at 993 (quotation marks omitted).

72. See Irving, *supra* note 5, at 662.

with their ability to store, search, and sort large volumes of information in short amounts of time.⁷³ And while the scattering of information throughout numerous computer databases had preserved some practical obscurity, the Internet has all but eliminated those remnants of isolation.⁷⁴

A corollary to the destruction of practical obscurity is the use of databases to manufacture identity profiles. Databases can easily be searched and cross-referenced to gather large quantities of information over time about a particular individual.⁷⁵ The resulting profile is probably far more comprehensive and telling than the owner of the information ever intended anyone to know. This has been dubbed the “Mosaic Theory”: the sum of a number of bits of information is exponentially more valuable than each bit individually.⁷⁶ Indeed, one commentator has noted, “once the persona is recorded it achieves more credence than the individual.”⁷⁷ The problem is aggravated by the fact that these databases containing both raw data and sophisticated consumer profiles are increasingly sold,⁷⁸ usually without the consumers' knowledge of their synthesis.⁷⁹ It has been shown that “an individual's personal information may be transferred to over five computers in a single day.”⁸⁰

As a result, computer databases and the Internet have significantly increased access and ease of access to information. Many government agencies have computerized databases, which recently have been both linked to

73. See Bunker et al., *supra* note 2, at 581 (“Before computers dominated government record-keeping, the best protections for personal privacy were practical barriers.”); Kurtz, *supra* note 23, at 156 (noting that “an electronic compilation in searchable form and records that can only be found by a diligent search through scattered files” differ in that the former “presents a far greater threat to privacy”).

74. Bunker et al., *supra* note 2, at 583.

75. See Froomkin, *supra* note 9, at 1469 (“databases make it possible to create new information by combining existing data in new and interesting ways”); *FTC Materials*, *supra* note 10, at 753 (noting that consumer data is “analyzed and combined”); Litman, *supra* note 8, at 1284 (“Anyone with reason to do so can correlate the information stored on one computer with the information stored on another, and another, and another”); Overton & Giddings, *supra* note 3, at 28 (discussing “data matching”).

76. Kearns, *supra* note 13, at 991; see also Sunosky, *supra* note 52, at 81.

77. Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 25 (1996).

78. See, e.g., Kang, *supra* note 19, at 1239-40 (describing the industry of database marketing); Solove, *supra* note 2, at 1407-08 (discussing the new database industry).

79. According to the FTC, the lack of consumer knowledge was the “most consistent and significant concern” about online profiling. *FTC Materials*, *supra* note 10, at 758.

80. Anna E. Shimanek, Note, *Do You Want Milk with Those Cookies?: Complying with the Safe Harbor Privacy Principles*, 26 J. CORP. L. 455, 459 (2001).

PRIORITIZING PRIVACY

the Internet and to each other.⁸¹ Like private companies, some government agencies have begun to cross-reference other databases to create limited citizen profiles.⁸² Giant private databases have also arisen and are often published on the Internet.⁸³ Internet searches can now reveal a smattering of information with relatively little time and effort.⁸⁴

The storage capabilities of computer databases, as well as their questionable accuracy and security, generate additional privacy concerns. Digital information has a veritably infinite lifespan.⁸⁵ As a result, it can resurface at any time, even though one's life may have changed and that particular information may no longer be valid.⁸⁶ Compound this both by the fact that inaccurate information can be stored just as easily as accurate information,⁸⁷ and by the fact that security breaches—either inadvertent or by hackers—are very real concerns.⁸⁸

81. Solove, *supra* note 2, at 1403. According to Solove, the federal government maintains almost 2000 databases. *Id.*

82. Trubow, *supra* note 2, at 524.

83. *See, e.g.,* Gindin, *supra* note 13, at 1156-61. Solove notes that “[t]he most powerful database builders construct information empires, sometimes with information on more than half of the American population.” Solove, *supra* note 2, at 1408.

84. Two commentators were able to obtain from the Internet the following information about one of them in less than ten minutes:

his full name; his telephone number; the address of his Tallahassee residence; date of birth; and his social security number; the same information for his wife; the median income of his neighborhood; the median value of the homes in his neighborhood; the names of ten of his closest neighbors (including their addresses and telephone numbers); and similar information on his condominium in another city.

Overton & Giddings, *supra* note 3, at 29. All the information was correct. Indeed, today all manner of information can be found on the Internet, including court pleadings, motor vehicle records, credit information, and vehicle registrations, to name a few. *See* Gindin, *supra* note 13, at 1156-57; Kurtz, *supra* note 23, at 154; Kitajima, *supra* note 13; *see* Overton & Giddings, *supra* note 3, at 28-29.

85. Kurtz, *supra* note 23, at 153. Cate reminds us that computers regularly generate back-ups, as well as multiple copies of documents and e-mails. *See* CATE, *supra* note 16, at 15-16. Even the Internet is being archived. Solove, *supra* note 2, at 1412.

86. One commentator has compared such surplus information to atomic waste. *See* Bunker et al., *supra* note 2, at 582.

87. Inaccurate information can have disastrous consequences. For example, in one case, a credit report erroneously reported that a Missouri couple had filed for bankruptcy. Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 535 (1998).

88. In April 2000, the DeBeers website exposed to the public the personal information of 35,000 customers. John B. Kennedy & Matthew H. Meade, *Privacy Policies and Fair Information Practices: A Look at Current Issues Regarding Online Consumer Pri-*

2. *Information-Gathering Technologies*

Though information-gathering technologies are not a direct threat to informational privacy, they deserve brief consideration because they provide the foundation for databases. If there is no disclosure, there can be no threat to informational privacy.⁸⁹ In fact, the more insidious and widespread the information-gathering technologies are, the greater the threat can be to informational privacy.⁹⁰ These technologies are therefore worth discussing—if only to understand how pervasive the threat really is.

Information gathered on the Internet can be grouped into two categories: that which is disclosed voluntarily and that which is disclosed involuntarily.⁹¹ Both types of information can contribute to an informational privacy problem. However, voluntary disclosures often lead to the more insidious violations of informational privacy because the information is usually submitted with the erroneous belief that it will be confined to the

vacy and Business Practices, 632A PRACTISING L. INST./PATENTS 321, 323 (2001). The computer systems of the Central Intelligence Agency, the Justice Department, and the National Aeronautics and Space Administration have all previously been hacked. Gindin, *supra* note 13, at 1174. In 1998 alone, losses due to Internet security breaches exceeded \$100 million. Major R. Ken Pippin, *Consumer Privacy on the Internet: It's "Surfer Beware"*, 47 A.F. L. REV. 125, 130 (1999).

89. Froomkin grounds his solution on this idea in his article, *The Death of Privacy?*. Froomkin, *supra* note 9, at 1163. "If information never gets collected in the first place, database issues need never arise." *Id.* at 1164. This may seem to confuse the issue somewhat, so it is important to note that disclosure (information gathering) is necessary, but not sufficient for a threat to informational privacy. If information is disclosed, then there naturally arises a threat of unknown and undesired uses. However, just because information is disclosed, there are not necessarily any real or perceived consequences.

90. Cate argues that "[n]o form of communication other than face-to-face conversation and handwritten, hand-delivered messages escapes the reach of electronic information technologies." CATE, *supra* note 16, at 6. This assertion is almost certainly true with regard to the Internet. As well, the academic literature is rife with analogies that compare a real-life shopping mall to the Internet. *E.g.*, Kang, *supra* note 19, at 1198-99; Sunosky, *supra* note 52, at 80-81. Everything is the same, except for the fact that on the Internet, one's every move—every book browsed, every purchase made, every window shopped—is recorded in excruciating detail. Kurtz, *supra* note 23, at 151 ("The tracks we leave [in real life] are difficult and time consuming to follow. When we do the same things using the Internet, they become much easier to see"). Indeed, the structure of the Internet makes the Internet one giant information-gathering technology. *See* Helms, *supra* note 2, at 295 ("While using the Internet, a number of technical realities conspire to associate an individual's Internet actions with their biological identity."); Kurtz, *supra* note 23, at 153 (noting that the Internet is structured such that "[i]nformation does not travel directly from sender to receiver," thus "allow[ing] data to be captured at various locations using diverse means").

91. *See* Blumenfeld, *supra* note 27, at 352 (distinguishing between overt and clandestine collection).

PRIORITIZING PRIVACY

purposes for which it is being given. For instance, many voluntary disclosures occur through registration pages, contest sign-ups, and application or order forms.⁹² In these cases, users will often give crucial personal information, such as their name and address, believing that the information is being collected only for a specific purpose, such as the shipment of their purchase. This is frequently untrue.⁹³ Newsgroup postings are another source of voluntary disclosures.⁹⁴ These users likely do not believe or truly realize that their postings will be preserved and can be distributed.⁹⁵ Creators of web pages fall into this same category.⁹⁶

Involuntary Internet disclosures usually entail some sort of surreptitious tracking. The two most discussed methods are the gathering of clickstream data and the use of cookies. Clickstream data is the generic name given to the information a website can know about a user simply because the user has browsed the site.⁹⁷ Accessing a website discloses the user's TCP/IP address, the types of computer and browser used, and limited information about browsing activity (notably the time and date of access, and the referring website's Internet address).⁹⁸ With slight effort, the website can record the user's clickstream, which will reveal more detailed browsing activity, such as the order of the webpages visited and the time spent at each one.⁹⁹ This information can threaten informational privacy because there are several ways it can be traced to an identifiable individual. First, a site may require registration to log-in.¹⁰⁰ Second, the TCP/IP address can be used to trace a user's personal information.¹⁰¹ Third, a

92. Pippin, *supra* note 88, at 129.

93. *See* Kurtz, *supra* note 23, at 160.

94. *See* Gindin, *supra* note 13, at 1169 (explaining how search engines can result in postings achieving "Internet-wide distribution"). Newsgroup postings can also result in involuntary disclosures for the user and third parties. With regard to the user, the postings often identify the actual e-mail address, place of origin, and sender. Krasovec, *supra* note 26, at 109-10. As to third parties, the concern is that anyone can post anything about anyone else. Kurtz, *supra* note 23, at 157.

95. *See* Kurtz, *supra* note 23, at 156 (noting how newsgroup users "may reach more people than [they] expect and leave tracks that are more permanent than [they] intend").

96. *See Id.* at 156-58.

97. Solove, *supra* note 2, at 1411; *see also* Kang, *supra* note 19, at 1227 (discussing "clicktrails" in particular).

98. Kang, *supra* note 19, at 1224-27; *see also* Froomkin, *supra* note 9, at 1486; Shimanek, *supra* note 80, at 460; Solove, *supra* note 2, at 1411.

99. Kang, *supra* note 19, at 1227; *see also* Pippin, *supra* note 88, at 129.

100. Solove, *supra* note 2, at 1411.

101. Malla Pollack, *Opt-in Government: Using the Internet to Empower Choice—Privacy Application*, 50 CATH. U. L. REV. 653, 665 (2001) ("An IP address, with variable effort, can be traced back to a specific computer, which itself may be strongly related to a specific person, or a small group of persons"). IP addresses are either static—associated

website can deposit a cookie on the user's hard drive, which will be used to identify the user on a return visit.¹⁰² Cookies are files in which websites record the information they have gathered from a user—information either voluntarily or involuntarily disclosed—and may be the most insidious form of information collection.¹⁰³

A number of other involuntary Internet disclosures bear mentioning. Digital watermarking allows intellectual property owners to track documents.¹⁰⁴ Similarly, Microsoft's Office 97 routinely tagged each document with an identification number.¹⁰⁵ One commentator claims that "the 'JavaScript' in the Netscape Web browser allows 'Web sites to collect real-time data on visitors' activities and to examine the directory of a visitor's hard drive.'"¹⁰⁶ Meanwhile, Intel has embedded each of its Pentium III chips with a unique identification number that, when functioning, can

with one computer—or dynamically assigned. The latter is usually the case for patrons of dial-up Internet Service Providers (ISP). Since IP addresses are centrally coordinated, a reverse DNS look-up of an IP address will return the identity of the ISP to which the address was assigned. From there, it is simply a matter of obtaining the user's personal information from the ISP. Static addresses are undoubtedly easier to trace, but ISPs generally log the assignments of their dynamic addresses. *See* Helms, *supra* note 2, 295-97; Pollack, *supra*, at 665-66.

102. Solove, *supra* note 2, at 1411 (identifying a cookie as a means of "secretly tag[ging] a user" to associate the user with clickstream data).

103. The cookies are placed on user's hard drives so that the website can recall the information when the user next visits. *E.g.*, Gindin, *supra* note 13, at 1170. In and of themselves, cookies do not pose an information-gathering or -disseminating threat. Rather, cookies resemble databases in that they facilitate intertemporal information gathering by other technologies, such as clickstream monitoring. In fact, some advertising companies have begun to use cookies (or sometimes transparent GIFs) as unique identifiers that allow them to track users from website to website. This entails a centralized advertisement provider that works with several companies. Every time an ad is clicked, a cookie is sent to the user by the advertisement provider, while the user is directed to the advertised company's website. Solove, *supra* note 2, at 1412. More insidiously, every time a user accesses a page that simply contains a banner advertisement, the advertisement provider places a cookie on the user's hard drive. *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 503-04 (S.D.N.Y. 2001); Kurtz, *supra* note 23, at 164. By accessing its cookies, the advertisement provider can literally track a user's movement from site to site and determine what sort of products or websites interest that particular user. Again, the cookies are facilitators, aiding interspatial information gathering. Recently, however, some websites have joined "cookie exchanges," making cookies themselves a direct threat to informational privacy. Shimanek, *supra* note 80, at 460; *see also* Kang, *supra* note 19, at 1228 (noting that "there is nothing to keep companies . . . from sharing with each other the browsing history of a given individual recorded through their respective cookies").

104. Froomkin, *supra* note 9, at 1489.

105. *Id.* at 1492.

106. Sunosky, *supra* note 52, at 81.

PRIORITIZING PRIVACY

be accessible to web browsers.¹⁰⁷ Finally, IPv6, the successor to the current IP address system, might permanently embed an IP address in every device that can connect to the Internet.¹⁰⁸

C. The Unique Problem of the Internet

Though informational privacy covers a wide range of issues,¹⁰⁹ this Article focuses on the Internet because it is the greatest threat to informational privacy. The Internet was essentially designed to collect information.¹¹⁰ Surveys have found that over ninety percent of websites collect some personal information.¹¹¹ Moreover, the use of the Internet as a tool for communicating, for educating, for shopping, for banking, and *for living*,¹¹² is growing and will continue to expand.¹¹³ In fact, Internet access will likely become unavoidable and indispensable.¹¹⁴ On top of it all, the Internet stores and is capable of processing all of the information it collects.¹¹⁵ Put simply, the Internet is the largest computer database ever, with

107. Froomkin, *supra* note 9, at 1490; Helms, *supra* note 2, at 298.

108. Froomkin, *supra* note 9, at 1491-92; Helms, *supra* note 2, at 299-300.

109. See Allen-Castellitto, *supra* note 35, at 17 (“Informational privacy is at issue in cases about access to medical records, employer access to email, online anonymity, data encryption, and executive privilege”).

110. Gindin, *supra* note 13, at 1164 (“The Internet has the capacity to be the most effective data-collector in existence”); Schwartz, *supra* note 30, at 815 (noting how the Internet’s “current technical configurations” allow daily activities on the Internet to generate “finely grained personal data”).

111. See Charles L. Kerr, *Online Privacy: Recent Developments*, 632A PRACTISING L. INST./PATENTS 51, 150-51 (mentioning two surveys, the first of which found that ninety-three percent of the sites surveyed collect personal information and the second of which found that ninety-nine percent of the sites surveyed collect personal information).

112. See Kang, *supra* note 19, at 1223 (“The networked personal computer will become the one-stop information appliance for all types of transactions that now take place in the physical world”).

113. According to Krasovec, in 1997 the Internet was gaining “roughly one million new users per month.” Krasovec, *supra* note 26, at 105; see also CATE, *supra* note 16, at 7 (giving a reliable benchmark for the growth of the Internet as “doubling in size every twelve to fifteen months”).

114. See CATE, *supra* note 16, at 1 (“Exponential increases in computing power and dramatic decreases in the physical size and price of computers have created a frenzied cycle in which both individuals and organizations increasingly use computers, spawning phenomenal growth in and dependence on computer-base services, and resulting in greater demand for and use of computers”).

115. Solove quotes a marketer as saying, “The time will come . . . [when w]e will be classified, profiled, categorized, and our every click will be watched.” Solove, *supra* note 2, at 1412. Solove himself notes that “[a]s we live more of our lives on the Internet, we are also creating a permanent record of unparalleled pervasiveness and depth.” *Id.*; see also Sunosky, *supra* note 52, at 80 (noting the Internet’s “impressive ability to increase the speed and lower the cost of transferring and sharing information”).

a nearly infinite memory and access to arguably the largest possible (and a near endless) stream of information.¹¹⁶ The real and perceived consequences of the disclosure of personal information are mind-boggling.¹¹⁷

It has taken some time for this realization to dawn on the general masses,¹¹⁸ but people have begun to come around.¹¹⁹ Indeed, the issue of Internet privacy was a “hot button issue” in the recent presidential campaign.¹²⁰ There are signs, too, that the public has become aware of the specific threat that the Internet poses to informational privacy.¹²¹ Privacy concerns have been cited as the “primary reason” for avoiding the Internet.¹²² According to the Pew Internet & American Life Project, fifty-four percent of Americans consider online tracking a “harmful invasion of privacy.”¹²³ Most significantly, as of late, there has been increased judicial activity regarding online violations of informational privacy.¹²⁴

III. THE NEED FOR A CONSTITUTIONAL RIGHT

The Internet is creating a generalized interest in informational privacy and, consequently, the need for a constitutional right to informational privacy that will provide real protection against the Internet. Unlike earlier technologies, the Internet pervades all aspects of life.¹²⁵ Information *is* a

116. See Helms, *supra* note 2, at 293 (“[As] a worldwide network, [the Internet] can connect, coordinate and centrally aggregate all privacy invading technologies”).

117. Kang captures much of this sentiment in his concerns about “second generation” problems. For the first time ever, the power of computer databases is being applied to a set of information “about the average Jane” that it had “[n]ever before in human history [made] any economic sense to [collect].” Kang, *supra* note 19, at 1271.

118. For an interesting discussion on how people have kept their heads in the sand about the Internet and its threat to informational privacy, see Litman, *supra* note 8, at 1284-86.

119. The FTC cites a recent survey as finding that ninety-two percent of Americans say they are “concerned about threats to their personal privacy when they use the Internet” and seventy-two percent say they are “very concerned.” *FTC Materials*, *supra* note 10, at 762.

120. Kennedy & Meade, *supra* note 88, at 323.

121. See Blumenfeld, *supra* note 27, at 353 (“Although many Internet privacy concerns are present in the off-line world, the Internet’s ability to accumulate vast amounts of data has heightened consumer fear about the availability of personal information on the Internet”).

122. Cody, *supra* note 40, at 1184.

123. Pollack, *supra* note 101, at 698.

124. Kerr, *supra* note 111, at 64-114 (regarding the types of judicial activity).

125. See Blumenfeld, *supra* note 27, at 381 (“[T]he statutory protections are sectorial in nature and . . . the Internet industry increasingly cuts across nearly all industry sectors”); see also CATE, *supra* note 16, at 1 (referring to the “frenzied cycle” of computer and website dependence in both government and private companies); Kang, *supra* note

PRIORITIZING PRIVACY

currency, and as such, personal information will become an increasingly necessary gate key as more processes and services become purely automated, computerized, and online.¹²⁶

Patchwork protection for informational privacy will no longer suffice.¹²⁷ A generalized interest in informational privacy calls for generalized protection. This Part will expand on this argument and show that a constitutional right will best provide such generalized protection by establishing a firmly entrenched foundation that allows flexibility in scope. A constitutional right would also address many of the rationales for other methods of informational privacy protection, while avoiding those methods' more significant pitfalls.¹²⁸ As necessary groundwork, this Part will first demonstrate the inability of current nonconstitutional law to adequately address the threat posed by the Internet to informational privacy.

A. The Failure of Current Nonconstitutional Law

Since the inadequacy of the current legal regime with regard to Internet privacy is well recognized,¹²⁹ the following survey of current tort law

19, at 1223 (“The networked personal computer will become the one-stop information appliance for *all* types of transactions that now take place in the physical world.” (emphasis added)).

126. See Kearns, *supra* note 13, at 983 (“As society becomes ever more information-based, the need for individuals to distribute their personal information increases. An unwillingness to give personal information to others effectively would prevent an individual from functioning in society.” (internal citation omitted)).

127. See Schwartz, *supra* note 30, at 815 (“In the absence of effective limits, legal or otherwise, on the collection and use of personal information on the Internet, a new structure of power over individuals is emerging”).

128. At least two other commentators have argued that a changing interest in informational privacy will likely need a strengthened federal constitutional right to informational privacy. See Kearns, *supra* note 13, at 984 (“As personal information plays a greater role in the daily lives of individuals, and the interest in personal information privacy increase[s], the need to develop [the constitutional right to informational privacy] will increase as well”); Kitajima, *supra* note 13, at 581 (“We live in an ‘information age’ [and] . . . [b]ecause Internet growth and increased access to information will persist, the Supreme Court may soon have to decide whether an informational privacy right actually exists”).

129. See, e.g., Blumenfeld, *supra* note 27, at 381 (“Current constitutional, legislative, common law, and state law privacy protections fail to provide consumers with comprehensive privacy protections and, as such, offer little, if any privacy protections against information collection on the Internet”); Gindin, *supra* note 13, at 1210-17 (notably failing to mention basic online privacy concerns when suggesting “fertile ground for litigation”); Helms, *supra* note 2, at 313-14 (“[C]onstitutional claims, privacy torts, and federal statutes . . . have considerable weaknesses when applied to privacy on the Internet”); Cody, *supra* note 40, at 1231-32 (calling for legislation to “ensure that individual privacy is protected online”).

and federal and state statutes will be brief. This Part will also consider the success of fledgling online privacy litigation, however, adding empirical verification to the current scholarship.

1. *Tort law*

The privacy torts are generally considered the first stop for protection against privacy intrusions by *private* parties.¹³⁰ They are categorized into four related claims: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) misappropriation of name or likeness; and (4) publicity that places another in a false light.¹³¹ A few particularities make current tort law incapable of providing much protection for informational privacy on the Internet.¹³² To begin with, Internet-related torts are difficult to demonstrate since consent (which is typically provided in Internet transactions) is often a defense to tort claims.¹³³ For instance, a successful claim on the first three torts would require that the complainant neither was aware of nor could foresee data collection.¹³⁴ The average Internet user would be hard-pressed to make such a claim truthfully. In addition, the privacy torts tend to require meeting the high standard that an intrusion or disclosure be “highly offensive to a reasonable person.”¹³⁵ Finally, tort law protection advances slowly, but is retracted quickly.¹³⁶ This quality makes the privacy torts difficult to adapt to rapidly changing or developing technologies.

It is interesting to note that the failure of the current legal regime may be linked to the misunderstanding of informational privacy that this Article has identified. While I have defined informational privacy as being concerned with the real and perceived *consequences* of disclosure, privacy law developed with an eye toward disclosure and keeping secrets. Solove, *supra* note 2, at 1430-31 (noting privacy law’s tendency toward keeping information from being revealed).

130. See Marc Rotenberg, *Consumer Privacy in the E-Commerce Marketplace*, 632A PRACTISING L. INST./PATENTS 303, 308 (2001) (noting that the privacy tort established rights of privacy beyond a protection against the government).

131. Helms, *supra* note 2, at 309.

132. For the most part, commentators agree that none of the four privacy torts will provide much protection against Internet informational privacy concerns. See Kang, *supra* note 19, at 1231 n.159; Overton & Giddings, *supra* note 3, at 44. A significant minority, which will be discussed shortly, has indicated the misappropriation tort may provide limited relief.

133. See Froomkin, *supra* note 9, at 1536.

134. Helms, *supra* note 2, at 309-10.

135. *Id.* at 310.

136. Kearns, *supra* note 13, at 1000.

PRIORITIZING PRIVACY

At first glance, the intrusion upon seclusion tort seems like it might apply to information gathering on the Internet.¹³⁷ For instance, cookies “intentionally intrude upon the solitude or seclusion of another.”¹³⁸ However, the tort’s broad interpretation of voluntariness and its narrow standard of “highly offensive to the reasonable person” should quell that possibility.¹³⁹ One commentator points out that many people are aware of cookies and their browsers can be set to reject them.¹⁴⁰ Moreover, cookies and other such information gathering are often small-scale, and, taken alone, relatively innocuous intrusions.¹⁴¹ Finally, many people consider the Internet to be a “public” place, which is exempt from this tort.¹⁴² Notably, courts have rejected this theory in the following cases: obtaining unlisted phone numbers, selling subscription lists to direct mail companies, and collecting and disclosing an individual’s past insurance history.¹⁴³

The tort of public disclosure of private fact requires a disclosure of private information that is (1) widely disseminated; (2) highly offensive to a reasonable person; and (3) not “newsworthy” or “of legitimate concern to the public.”¹⁴⁴ This tort might be useful against online profiling and the database swaps that facilitate such profiling.¹⁴⁵ However, the standard for “widely disseminated” is difficult to meet. Databases that are widely disseminated may be considered public record, which is not tortious under the private fact tort.¹⁴⁶ Conversely, databases that are sold to a few parties—thus, seemingly private—are often considered not to have been

137. Blumenfeld, *supra* note 27, at 358-59; CATE, *supra* note 16, at 89; *see also* Gindin, *supra* note 13, at 1189 (“Because this tort has been applied to wiretaps, liability would likely be imposed for the unauthorized access to or interception of electronic communications and information systems”). *But see* Kearns, *supra* note 13, at 1000 (“[The] tort of intrusion does not apply to information privacy because this tort relates to physical intrusions and trespass”).

138. Helms, *supra* note 2, at 310.

139. *Id.*; Overton & Giddings, *supra* note 3, at 44.

140. *See* Helms, *supra* note 2, at 310. Writing in 2001, Helms noted that he was not aware of any such claim having been made. *Id.*

141. Solove, *supra* note 2, at 1432 (noting that “the danger is created by the aggregation of information”).

142. Overton & Giddings, *supra* note 3, at 44; Solove, *supra* note 2, at 1433.

143. *See id.* at 1432-33.

144. CATE, *supra* note 16, at 90.

145. Helms, *supra* note 2, at 311; Solove, *supra* note 2, at 1433.

146. Overton & Giddings, *supra* note 3, at 44; Solove, *supra* note 2, at 1433; Trubow, *supra* note 2, at 536-37. Birthdate, marital status, military record, professional or occupational licenses, and litigation are examples of public records. Gindin, *supra* note 13, at 1190.

widely disseminated. Also, the information contained in these databases would likely not be considered highly offensive.¹⁴⁷ Indeed, this tort has historically achieved limited success.¹⁴⁸

The misappropriation of a name or likeness is best known for its use to protect the value of a famous person's name or picture.¹⁴⁹ However, a detailed profile might also be a likeness that should not be appropriated, because these profiles are arguably parts of the person's personality.¹⁵⁰ Therefore, mailing lists should not be sold.¹⁵¹ It is not clear that "name or likeness" amounts to personality.¹⁵² And again, consent could also be a sticking point, as most users of the Internet voluntarily or knowingly surrender much of their personal information. In fact, every case that has invoked this theory to enjoin the sale of names and addresses to direct marketers has failed.¹⁵³

The false light tort applies when one publicizes someone in a distorted manner "that is both highly offensive to the reasonable person and done with knowing or reckless disregard as to the falsity of the portrayal."¹⁵⁴ This tort will probably be generally useless in the cyberspace context be-

147. Helms, *supra* note 2, at 311 ("[I]t is not likely that even the most detailed profile would rise to the level of a 'highly offensive' disclosure."); Trubow, *supra* note 2, at 537 ("Most of the information stored in commercial computer files is not offensive or embarrassing, even though it does provide a detailed description of an individual's behavior, tastes, and values"). *But see* Gindin, *supra* note 13, at 1191 (suggesting this tort may be the basis for suit in cases in which "personal information . . . is disseminated electronically to a significant number of people").

148. *See* CATE, *supra* note 16, at 90. It is important to remember that much online profiling occurs in secret, so the merits of such a claim may be wholly irrelevant. Solove, *supra* note 2, at 1433.

149. Helms, *supra* note 2, at 311. The tort requires an identifiable plaintiff, that the defendant appropriated the name or likeness to his own advantage, and that the appropriation occurred without consent. Overton & Giddings, *supra* note 3, at 41.

150. Trubow, *supra* note 2, at 539.

151. Helms, *supra* note 2, at 311; Komuves, *supra* note 87, at 566.

152. *See* Kearns, *supra* note 13, at 1000 n.132 ("The concept of name or likeness also would have to be expanded, however, to include personal information"); *see also* Litman, *supra* note 8, at 1291 ("Tort law provides a remedy for unauthorized commercial exploitation of celebrities' identities, but not for conveying accurate personal information, however lucrative the conveyance." (internal citations omitted)).

153. *See* Gindin, *supra* note 13, at 1192; Helms, *supra* note 2, at 311; Komuves, *supra* note 87, at 566-67. Some commentators have suggested the tort would be appropriate only for application to cases in which a name or likeness was misappropriated for use in an Internet advertisement. *See* Overton & Giddings, *supra* note 3, at 41; Cody, *supra* note 40, at 1196 n.67.

154. Helms, *supra* note 2, at 312.

PRIORITIZING PRIVACY

cause informational privacy concerns almost always involve information that is true.¹⁵⁵

The inadequacies of tort law make state and federal statutes attractive alternatives. Statutes are tailored to address specific problems, especially those involving new technologies. However, the current statutes are ineffective with regard to Internet privacy, and the Federal Trade Commission, ostensibly the federal government's Internet regulatory body, is once again calling for industry self-regulation over new federal legislation.¹⁵⁶

2. *Federal Statutes*

The United States does not have an omnibus statute that regulates the collection, dissemination, and use of information on and through the Internet. Rather, federal statutory protection must come from a collection of related and distantly related statutes.¹⁵⁷ Only one of these statutes, the Children's On-line Privacy Protection Act ("COPPA"),¹⁵⁸ specifically addresses informational privacy on the Internet, and it is restricted to information gathering by children-oriented websites. The "umbrella" protection provided by these statutes is weak because the statutes lose effectiveness when translated to cyberspace,¹⁵⁹ are weak to begin with,¹⁶⁰ are often ex-

155. Kearns, *supra* note 13, at 1000; *see also* Solove, *supra* note 2, at 1433 (noting that this tort is designed to protect one's reputation, but that the information collected in databases is often not directly harmful to one's reputation). To be sure, this tort could probably be used against online profilers who have recklessly compiled and published erroneous data. Gindin, *supra* note 13, at 1192.

156. *See, e.g.*, Carrie Kirby, *FTC Drops Call for New Internet Privacy Laws*, SAN FRANCISCO CHRON., Oct. 5, 2001, at B1.

157. *See, e.g.*, Blumenfeld, *supra* note 27, at 360 (noting in 1998 that "[c]urrent federal privacy legislation takes an industry sectorial approach, consisting of a handful of disparate statutes directed at specific industries that collect personal data and none of which specifically or effectively covers the collection, use, and disclosure of information online"). For a thorough listing of federal statutes that directly or indirectly apply to privacy issues, *see* Eugene J. Yannon, *Technology and the Law: Privacy Law*, MD. BAR J., Nov.-Dec. 2001, at 24, 27.

158. 15 U.S.C. §§ 6501-6506 (2000).

159. *See, e.g.*, Pippin, *supra* note 88, at 143 (attributing part of the confusion in applying non-Internet laws to the Internet to "the difficulty associated with applying traditional terminology to modern Internet practice and, for that matter, the absence of any reference to the Internet within the legislation"); Cody, *supra* note 40, at 1200 ("[T]he application of these statutes to information collected over the Internet is unclear").

160. *See* CATE, *supra* note 16, at 78 (noting that the statutes "often include significant loopholes"); Komuves, *supra* note 87, at 558-59 (arguing that the statutes "allow Congress to state that they have addressed privacy concerns, but [are] riddled with exceptions, making them ineffective").

tremely narrow in scope, and leave more territory unprotected than protected.¹⁶¹

Consider, for instance, the Privacy Act.¹⁶² The Privacy Act regulates the federal government's collection and use of personal information in federal agencies.¹⁶³ While it does not regulate private actors or state and local agencies, one could argue that the Privacy Act at least manages to restrict the federal governmental data that gets into the hands of private Internet databases. However, the Privacy Act is crippled by the Freedom of Information Act ("FOIA")¹⁶⁴ and over ten exceptions that permit information to be disclosed without consent of the information's owner.¹⁶⁵ By far the most insidious exception is the one for "routine use," which agencies have learned to define "expansively."¹⁶⁶ Moreover, the Act appears to cover only information retrieved by name or some other identifying particular.¹⁶⁷ In other words, one might still find all the people suffering from AIDS by searching under the word "positive."¹⁶⁸

Aside from COPPA, the Electronic Communications Privacy Act¹⁶⁹ ("ECPA") would seem to be the federal statute with the greatest applicability to the Internet. The ECPA was designed to protect private electronic communications, such as e-mail, from the government, individuals, and third parties.¹⁷⁰ However, like the Privacy Act, the ECPA has been weakened by a number of exceptions. For instance, certain exceptions allow online service providers to disclose communications.¹⁷¹ The most striking

161. See Komuves, *supra* note 87, at 559 ("The absence of federal legislation regulating other areas is perhaps even more important than [a] listing of what federal law does protect."); see also Solove, *supra* note 2, at 1444 ("[T]he federal statutes cover only a small geography of the database problem").

162. 5 U.S.C. § 552a (2000).

163. Blumenfeld, *supra* note 27, at 360.

164. 5 U.S.C. § 552 (2000).

165. See CATE, *supra* note 16, at 78 (describing the exceptions and the Privacy Act's relationship with FOIA). For example, the Privacy Act applies neither to Congress nor to law enforcement agencies. *Id.*

166. Bunker et al., *supra* note 2, at 583-84; see also Susan Clement et al., *The Evolution of the Right to Privacy After Roe v. Wade*, 13 AM. J. L. & MED. 368, 394 (1987).

167. *Id.* at 393.

168. *Id.*

169. 18 U.S.C. §§ 2510-2520, 2701-2709 (1997).

170. CATE, *supra* note 16, at 84 (mentioning e-mail as an electronic communication); Cody, *supra* note 40, at 1200 (describing purpose of the ECPA).

171. See CATE, *supra* note 16, at 84-85; Gindin, *supra* note 13, at 1197-1200.

PRIORITIZING PRIVACY

exception is that only one party needs to consent to the disclosure.¹⁷² Furthermore, interceptions of communications are lawful if the system is “readily accessible to the general public.”¹⁷³ Finally, there is no prohibition on revealing the “circumstances,” as opposed to the content, of a communication.¹⁷⁴

Other federal statutes do not suffer from rule-swallowing exceptions, but they are so narrow as to make their applicability on the Internet exceedingly limited. The Right to Financial Privacy Act of 1978¹⁷⁵ and the Family Educational Rights and Privacy Act of 1974¹⁷⁶ are examples of such legislation. The former protects the privacy of individual bank records, while the latter applies strictly to a subset of educational records.

3. *Federal Statutes in Recent Internet Cases*

Perhaps more useful than pages of theoretical statutory analysis is a look at how the federal statutes have fared poorly in cases involving informational privacy on the Internet.¹⁷⁷ In March 2001, a New York federal district court ruled on motions to dismiss the federal claims filed against DoubleClick, Inc. in the consolidated action *In re DoubleClick, Inc. Privacy Litigation*.¹⁷⁸ DoubleClick is an advertising agency that places banner advertisements on its affiliated websites. When users access these sites, DoubleClick places a cookie on the users’ hard drives.¹⁷⁹ Over time, DoubleClick uses these cookies to develop detailed user profiles.¹⁸⁰ Along with several state claims, plaintiffs filed three federal claims, alleging violations of Titles I and II of the ECPA¹⁸¹ and of the Computer Fraud and

172. Cody, *supra* note 40, at 1200 (describing the one-party consent as the “most glaring exception” and an exception with “a direct effect on personal identifiable informational collection and disclosure”); *see also* Gindin, *supra* note 13, at 1198.

173. CATE, *supra* note 16, at 84-85; Gindin, *supra* note 13, at 1198.

174. John F. Delaney & M. Lorrane Ford, *The Law of the Internet: A Summary of U.S. Internet Case Law and Legal Developments*, 1244 PRACTISING L. INST./CORP. 103, 271; *see* Kang, *supra* note 19, at 1234. One commentator believes that *United States v. Hambrick*, 55 F. Supp. 2d 504 (W.D. Va. 1999), suggests that the context/content distinction is only a restriction on disclosures to governmental parties. *See* Pippin, *supra* note 88, at 151.

175. 12 U.S.C. § 3401 (2000).

176. 20 U.S.C. § 1232(g) (2000).

177. For more on federal statutes and their applicability to the Internet, *see* Pippin, *supra* note 88, at 143-54; CATE, *supra* note 16, at 80-88; and Solove, *supra* note 2, at 1440-44.

178. 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

179. *Id.* at 502-03.

180. *Id.*

181. 18 U.S.C. §§ 2510, 2701 (1997).

Abuse Act (“CFAA”).¹⁸² The court found that the plaintiffs had failed to state a claim with regard to all three federal statutes.

First, the plaintiffs alleged that in accessing the cookies, DoubleClick violated Title II of the ECPA, which contains the restriction on access to stored electronic communications.¹⁸³ The court, however, ruled in favor of DoubleClick, which argued that its actions fell under an exemption to the statute.¹⁸⁴ The court found that the cookies were communications intended for DoubleClick’s website affiliates, and that those websites had authorized DoubleClick’s access to the cookies.¹⁸⁵ The court also mentioned that “Title II in no way outlaws collecting personally identifiable information or placing cookies.”¹⁸⁶

Second, the plaintiffs claimed that DoubleClick had intercepted electronic communications (presumably in its gathering of the information that is inscribed in the cookies), thereby violating Title I of the ECPA (“the Federal Wiretap Act”).¹⁸⁷ On this count, the court also found in favor of DoubleClick—based on an exemption.¹⁸⁸ DoubleClick had intercepted communications with the consent of its website affiliates, and the plaintiffs failed to provide facts that would support an inference that DoubleClick had a primarily tortious intent.¹⁸⁹ The court noted that plaintiffs seemed to indicate that DoubleClick’s intents were purely commercial.¹⁹⁰

Third, DoubleClick allegedly violated the CFAA, which restricts access to certain computers, by placing cookies on the plaintiffs’ hard

182. *Id.* at § 1030.

183. *DoubleClick*, 154 F. Supp. 2d at 507.

184. DoubleClick claimed that 18 U.S.C. § 2701(c)(2) (1997) exempted its actions from Title II of the ECPA. *See DoubleClick*, 154 F. Supp. at 507.

185. *See id.* at 507-11. The plaintiffs responded to this by reasoning that though the contents of the cookies were communicated to the website affiliates, the cookie identification numbers remained solely on their hard drives. The court found these arguments inapposite, as well. It found that the permanent nature of cookies and their identification numbers should place them outside the scope of Title II’s regulation of *temporarily* stored electronic communications. *See id.* at 511-13. Furthermore, even if cookies were considered stored communications, the identification numbers were communications intended for DoubleClick and DoubleClick was authorized to access its own communications. *Id.* at 513-14.

186. *Id.* at 510.

187. *Id.* at 514.

188. DoubleClick looked to 18 U.S.C. § 2511(2)(d) (1997), which among other things, allows interception if one of the parties to the communication has given prior consent, unless the communication is intercepted for purpose of committing a criminal or tortious act. *See DoubleClick*, 154 F. Supp. 2d at 514.

189. *Id.* at 514-19.

190. *See id.* at 518-19.

PRIORITIZING PRIVACY

drives.¹⁹¹ Though DoubleClick did not deny these allegations, the court found that the plaintiffs failed to allege damages sufficient to meet the statute's requirements. The alleged cost of remedying the plaintiffs' computers was nominal because browsers can easily be set to reject cookies.¹⁹² Furthermore, the court found that neither the disclosure of demographic information nor receiving targeted advertising is an economic loss for a computer user.¹⁹³

These same federal statutes had slightly better, though distinguishable, showings in two other cases from 2001, *In re Intuit Privacy Litigation*¹⁹⁴ and *In re Toys R Us, Inc., Privacy Litigation*.¹⁹⁵ In the former case, the plaintiffs alleged that Intuit's placement of and access to cookies on their hard drives violated the three federal statutes. Intuit's motions to dismiss the Title I ECPA claim and the CFAA claim were granted on grounds similar to those articulated by the court in *DoubleClick*.¹⁹⁶ In the latter case, the plaintiffs also maintained that the company violated these statutes by using cookies.¹⁹⁷ The court dismissed the Title II ECPA claim on both the *DoubleClick* reasoning and the argument that cookies fall outside the scope of Title II of ECPA because they are permanently, rather than temporarily, stored electronic communications. Unlike DoubleClick, though, the remaining three claims from *Intuit* and *Toys R Us* survived at least in part.¹⁹⁸

However, these successes can be distinguished. For instance, the court did not dismiss the Title II ECPA claim in *Intuit*, but Intuit did not make the arguments that had been made by the defendants in *DoubleClick* and *Toys R Us*.¹⁹⁹ The CFAA claim from *Toys R Us* survived the damages inquiry that led to the dismissal of the corresponding claims in *DoubleClick* and *Intuit* only because the court "liberally construed," at least for this preliminary stage, that a single act could involve numerous hard drives.²⁰⁰ It

191. *Id.* at 519.

192. *Id.* at 524-25.

193. *See id.* at 525.

194. 138 F. Supp. 2d 1272 (C.D. Cal. 2001).

195. MDL no. M-00-1381 MMC, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. Oct. 9, 2001).

196. *Intuit*, 138 F. Supp. 2d at 1277-81.

197. *See Toys R Us*, 2001 U.S. Dist. LEXIS 16947, at *3-*5. *Toys R Us* involved the use and placement of cookies by both Toys R Us, Inc. and Coremetrics, Inc., the company whose technology Toys R Us websites utilized.

198. Actually, one part of the Title I ECPA claim from *Toys R Us* was dismissed, but with leave to amend. *See id.* at *22-*23.

199. *See Intuit*, 138 F. Supp. 2d at 1275-77.

200. *Toys R Us*, 2001 U.S. Dist. LEXIS 16947, at *35-*36.

is not clear that this interpretation will survive further litigation. In *DoubleClick*, the court specifically limited the assessment of damages under CFAA to a single act on a particular computer.²⁰¹ Moreover, it is important to note that these rulings are on the defendants' motions to dismiss. Thus, while the Title I ECPA claims failed in *DoubleClick* and *Intuit* for a failure to show tortious or criminal purposes, the defendant's motion to dismiss the Title I ECPA claim in *Toys R Us* failed only because "no evidence concerning [defendant's] purpose ... [was] before the Court at this stage of the proceedings."²⁰²

It is clear from these cases that the current federal statutes are weak, and that they have a very limited applicability to the Internet. In fact, the *DoubleClick* court noted "[t]he absence of evidence in the legislative or judicial history of any of these Acts to suggest that Congress intended to prohibit conduct like DoubleClick's."²⁰³

4. State Statutes

Though several states have privacy statutes, the state statutory regime will not provide much of a haven for online informational privacy. To begin with, the majority of these statutes apply only to government activities.²⁰⁴ Moreover, state statutes tend to cast a much smaller net than federal statutes do.²⁰⁵ Three states—Virginia, Georgia, and West Virginia—do have laws regulating the use of computers or computer networks to examine personal data without authorization.²⁰⁶ However, these are likely to be as riddled with exemptions as are federal statutes. States' additional attempts to enact more significant legislation have been thwarted by the Commerce Clause.²⁰⁷ It appears that state statutes will struggle to address the largely interstate and international transactions on the Internet.²⁰⁸

201. See *DoubleClick*, 154 F. Supp. 2d at 524 ("[T]he suggestion that DoubleClick's accessing of cookies on millions of plaintiffs' computers could constitute a single act is refuted by the statute's plain language").

202. *Toys R Us*, 2001 U.S. Dist. LEXIS 16947, at *25-*27.

203. *DoubleClick*, 154 F. Supp. 2d at 526.

204. See CATE, *supra* note 16, at 88 ("At least thirteen states have general privacy statutes applicable to government activities. Some states also have statutory privacy rights that apply to the privacy sector").

205. For instance, Overton and Giddings found that "Florida laws . . . generally provide even less protection than that afforded through federal laws." Overton & Giddings, *supra* note 3, at 49.

206. Bradley A. Slutsky & Allison S. Brantley, *Privacy on the Internet: A Summary of Government and Legal Responses and a Practical Guide to Protecting Your Client*, 637 PRACTISING L. INST./PATENTS 85, 92 (2001).

207. *Id.* at 92-93.

208. Blumenfeld, *supra* note 27, at 359-60.

PRIORITIZING PRIVACY

5. *The Federal Trade Commission*

The Federal Trade Commission (“FTC”) is the last noteworthy leg of the current legal regime. Drawing on the Federal Trade Commission Act (“FTCA”),²⁰⁹ the FTC has broad investigative authority over unfair business practices.²¹⁰ The FTC has become the federal government’s default Internet regulatory commission, both issuing recommendations for government policy and prosecuting websites for informational privacy violations. While its actions have resulted in some protection of informational privacy on the Internet,²¹¹ the FTC is limited in its effect. For instance, the term “unfair business practices” restricts FTC action to anti-competitive practices, such as the stealing of personal information from another website, and the deception of consumers, such as websites violating their privacy statements. This may require companies to provide more explicit privacy policies on their websites, but it does not require them to make their privacy statements or links thereto conspicuous. It also does not ensure that Internet users actually read the privacy statements from start to finish.²¹² By concentrating on whether companies’ business practices are unfair or fair, the FTC misses the crux of the informational privacy problem, which is that these companies have the capability to buy, sell, and collect information through their websites. Moreover, the FTC has numerous other responsibilities (the most notable of which is the oversight of real world businesses) and limited resources with which to fulfill them.²¹³

B. A Constitutional Commitment

The failure of the current legal system has led to many suggested solutions, including the expansion of tort law, a comprehensive Internet statute, and property rights in personal information.²¹⁴ However, these sugges-

209. 15 U.S.C. § 41 (1997).

210. Pippin, *supra* note 88, at 133-35.

211. For example, in *FTC v. Toysmart*, the FTC prevented bankrupt Toysmart.com from violating its privacy policy and selling its compilation of users’ personal information. Kerr, *supra* note 111, at 126-27; John C. Yates, *E-Compliance: Internet Law and Privacy Issues*, 1248 PRACTISING L. INST./CORP. 511, 517-21 (2001). In the settlement of another case, the FTC required Reverseauction.com to delete the personal information Reverseauction.com had obtained improperly from eBay. Kerr, *supra* note 111, at 124-26.

212. For a general study on privacy policies and the effect of the FTC, see Pollack, *supra* note 101. See Pollack, *id.* at 684-90, for a particularly interesting empirical study of privacy policies.

213. See Rotenberg, *supra* note 130, at 311 (expressing doubt as to the ability of the FTC to operate as “an effective privacy agency”).

214. See, e.g., Gindin, *supra* note 13, at 1222-23 (calling for comprehensive federal legislation); Kang, *supra* note 19, at 1246-73 (describing the market motif and restoring

tions miss the point. They all seek to protect informational privacy from a specific threat—the Internet, computer databases, technologically advanced data collection, or some combination thereof—rather than addressing the problem comprehensively. This is not to say a comprehensive approach will resolve all the threats. Indeed, a solution designed to answer a particular threat will probably better prevent that particular threat than some generalized solution might. The point, rather, is that these suggested solutions, however effective in their limited scope, are no more than fingers in the dam when the foundation and the infrastructure of the dam itself are under siege.

The problem is that the Internet's effect on informational privacy is greater than the threat the Internet, as a technology, poses to informational privacy. As a technology, the Internet raises informational privacy concerns because, in an information age, it has created a platform for websites that collect more detailed information about people than ever before and provided a means to disseminate greater quantities of information in less amount of time with fewer errors and over larger distances than ever before. If one could speak about the "Internet part" of one's life, this would be but a blip—though a large blip—on the radar screen of informational privacy. But this is not possible. With the digitalization of information, the Internet pervades even the lives of those who do not send e-mail or use the World Wide Web.²¹⁵ Databases that store bank statements, welfare records, and the transactions of frequent shopper cards are all linked by the Internet.²¹⁶ The effect of the Internet on informational privacy is greater than the threat the Internet, as a technology, poses to informational privacy because even those who avoid the technology of the Internet face a greater threat to informational privacy. Because the Internet has changed the very nature of life in an information age, it reaches beyond its network of com-

default rules to individuals); Litman, *supra* note 8, at 1301-11 (advocating a tort law-based solution).

215. See Froomkin, *supra* note 9, at 1465 (noting that recent technological developments "provide the means for the most overwhelming assault on informational privacy in the recorded history of humankind" and that "[u]nless something happens to counter these developments, it seems likely that soon all but the most radical privacy freaks may live in the informational equivalent of a goldfish bowl"); Kang, *supra* note 19, at 1284 ("The new communications technologies are transforming our society, propelling us further into the Information Age."); Shimanek, *supra* note 80, at 456 ("The Internet has, for better or worse, fundamentally changed our lives and revolutionized the way we work, communicate, and shop").

216. For a list of electronic data that is routinely collected about individuals, see CATE, *supra* note 16, at 2.

PRIORITIZING PRIVACY

puters and its amalgamation of websites to create a heightened concern in informational privacy generally—for the whole of society.

As a result, the new legal regime must look past protecting against particularized threats and toward establishing a commitment to informational privacy. This requires a constitutional right to informational privacy.²¹⁷ A constitution is the infrastructure of a legal regime. It provides the basic contours from which the specifics can be shaped and determined. As such, constitutional protection is simultaneously uniform and flexible. Constitutional rights provide a foundational, baseline commitment that can be expanded by judicial and legislative interpretation. This sort of commitment is necessary for those interests that are so ubiquitous that they have become part of a society's framework. Such interests are a basic concern in all contexts and, yet, have the potential to become particularized concerns in certain contexts.

The Internet has elevated informational privacy to this level. The Internet's pervasiveness has made informational privacy a concern in nearly every facet of life. Informational privacy is no longer simply a discrete question of controlling access to certain types of information, such as financial records, medical files, or telephone listings. Only a constitutional right can ensure informational privacy will in fact be part of the framework for every debate. However, the threat to informational privacy can be greater or lesser in varying contexts, especially with changing technologies. As such, the legal protection must be adaptive. Only a constitutional right can also provide such flexibility. Thus, a constitutional commitment is required for the new, generalized interest in informational privacy.

A constitutional commitment would avoid many pitfalls of alternative solutions. For instance, critics of a property-right regime argue that information asymmetries, transactional costs, and bounded rationality will lead consumers to give up their information too easily.²¹⁸ Indeed, some have

217. One critic of a constitutional right to informational privacy has argued that a constitutional right treats privacy as a "uniform human value," and therefore "discounts how the boundaries of informational privacy have changed over time." Michael Grossberg, *Some Queries About Privacy and Constitutional Rights*, 41 CASE W. RES. L. REV. 857, 860 (1991). This critique should not apply here because the argument for this constitutional right to informational privacy is grounded in the recognition that informational privacy has evolved and that the constitutional right is necessary *because* informational privacy has come much closer to universal valuation.

218. See *supra* note 48 and accompanying text; Froomkin, *supra* note 9, at 1535 ("given that property-law-based solutions are undermined in the marketplace, some European nations have gone further and removed a consumer's freedom to contract away her right to certain classes of data").

noted that the primary problem with the Internet arises after disclosure.²¹⁹ A constitutional right, however, is inalienable. Even the current, weak constitutional right to informational privacy “reflects a residual safety valve function for immunity from access.”²²⁰ And while a consumer still might waive her constitutional right as she might waive a property right, the inalienability of the former creates an enduring presumption against disclosure that does not exist with the latter. The Constitution, which has been compared to lashing Odysseus to the mast, protects us against our own fleeting whims. The ever-present “shadow of a claim” resulting from a strong constitutional right will likely influence information gatherers and disseminators to reevaluate their methods and to educate consumers.²²¹

A constitutional right would also avoid many of the criticisms surrounding statutory solutions. Critics consider the mandatory, top down approach of statutes stifling and overbearing.²²² Others argue a statute would be crippled by its inapplicability to new technologies.²²³ Statutes are also easily swept aside by a changing public sentiment²²⁴ and unable to compensate for other important values, such as the First Amendment.²²⁵ In

219. See *supra* notes 50, 57, and accompanying text.

220. Turkington, *supra* note 13, at 518.

221. See Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PENN. L. REV. 1, 147 (“Even if privacy claims predictably lose in most cases after litigation, the shadow of the claim remains. Officials who take seriously the rights enunciated by the courts, (or pressure groups who can invoke those rights), will take into account the citizen’s interests in privacy when constructing government operating procedures”).

222. See, e.g., Pollack, *supra* note 101, at 659 (“[T]op down regulation . . . prevents persons from individually choosing to allow a ‘harm’ that, in their personal opinion, is ‘harmless’”); cf. Krasovec, *supra* note 26, at 107 (“[M]any Internet users feel [the current] lack of direct control is the ultimate value of the Internet.”); CATE, *supra* note 16, at 131 (“The purpose of these rights is to facilitate—not interfere with—the development of private mechanisms and individual choice as a means of valuing and protecting privacy”).

223. See Froomkin, *supra* note 9, at 1542 (“Rules that focus too narrowly on specific uses or users are doomed to lag behind technology.”); Helms, *supra* note 2, at 314 (“Federal statutes, due to rapidly changing technology, are inflexible and often cannot address the core problems related to Internet privacy”); Pollack, *supra* note 101, at 659 (“Statutory prohibitions may fail because they consistently emerge only after the harm has been done and the technology has advanced to other anti-privacy methods.”); Kearns, *supra* note 13, at 1002 (“existing legislation aimed at protecting privacy generally is ineffective when new technologies emerge”).

224. See *id.* at 1002 (“Legislation can be amended or repealed, and a reliance on measures that are changed easily to protect . . . privacy is insufficient”);

225. See Cohen, *supra* note 48, at 1428 (noting that “[d]ata privacy opponents” argue that “legislation designed to protect informational privacy [cannot] provide for both constitutionally-required and socially-valued uses of personally-identified information”); see

PRIORITIZING PRIVACY

contrast, the decision to invoke one's constitutional right ultimately lies with the individual. Constitutional protections are not tied to specific technologies; their applicability is based on judicial interpretation and thus can adapt to new technologies.²²⁶ Finally, one of the greatest advantages of a constitutional right is that it is permanent and inalienable, solid against fickle public sentiment,²²⁷ but that beyond a certain point, its scope is subject to judicial interpretation.²²⁸ This has allowed major constitutional rights, such as the First Amendment and the Establishment Clause, to co-exist.²²⁹

Moreover, a constitutional commitment would encompass a number of the themes that data privacy scholars have deemed necessary in a solution. It would clarify a bias toward informational privacy,²³⁰ place the ultimate

also CATE, *supra* note 16, at 111 (“it is . . . important that privacy laws . . . extend protection consonant with other legally protected, popularly shared values”); Froomkin, *supra* note 9, at 1506-23 (discussing how the First Amendment restricts informational privacy legislation); *cf.* Litman, *supra* note 8, at 1312 (“The flexibility of a tort law remedy permits courts to define its scope, by, for example, limiting it based on free speech or information policy issues”). Volokh devotes an article to concerns about the “downstream effects of any [information privacy based] speech exception.” *See* Volokh, *supra* note 42, at 1051.

226. *See* Kearns, *supra* note 13, at 1003 (“Unlike the statutory attempts to prevent technology from encroaching on privacy, constitutional protections address fundamental rights, not specific technologies, and would not be outpaced readily by advances in technology”). The current constitutional right to informational privacy has *not* adapted to apply to the Internet. *See infra* Part III.C. However, the current constitutional right also differs in many ways from a fundamental constitutional right. Indeed, its status as a constitutional right, of any stripe, is in question. *See infra* Part III.

227. *See* Kearns, *supra* note 13, at 1003 (“Constitutional protections are not subject to whimsical change the way the common law or legislation can be”).

228. *See* Flaherty, *supra* note 13, at 854 (describing how courts would balance interests to determine scope of constitutional right to privacy); Chlapowski, *supra* note 13, at 135 (arguing that the constitutional right is a “mechanism to balance the interests of the individual and the interests of the government when those interests conflict”); Kearns, *supra* note 13, at 1003 n.153 (“Protections provided by the Constitution do, and should, change as society evolves and needs develop”). In fact, one commentator has argued that if a constitutional right to informational privacy is recognized, that right “should exist narrowly and evolve slowly to accommodate changing societal and legal climates.” Kitajima, *supra* note 13, at 581. Moreover, “[a] limited right to informational privacy would more effectively balance an individual’s privacy rights against the public’s right to information than would an absolute privacy right, which may run afoul of First Amendment free speech rights.” *Id.* at 577.

229. *See, e.g.,* Martha M. McCarthy, *Free Speech Versus Anti-Establishment: Is There a Hierarchy of First Amendment Rights?*, 108 ED. L. REP. 475, 484 (1996).

230. *See* CATE, *supra* note 16, at 109 (noting the importance of “clarity, consistency, precision, and intelligibility” in data protection law); Solove, *supra* note 2, at 1461 (“Solving the problem requires meaningful limits on how data can be used—limits that

responsibility with the individual,²³¹ and compel data gatherers and disseminators to internalize the value of informational privacy.²³²

As a final point, it is important to note that this argument does not claim that a constitutional right to informational privacy will solve the problems posed by the Internet. As Froomkin aptly concludes, “[t]here is no magic bullet, no panacea.”²³³ For instance, one of the greatest threats posed by the Internet is the surreptitious transfer of collected information. It is not clear how a constitutional right would redress that situation. Neither does this Article intend to pass judgment on any solution. Rather, a constitutional commitment is exactly that: a commitment. The dynamics of informational privacy have changed and the necessary new legal regime requires a commitment to informational privacy. A constitutional right provides that commitment—a basic guarantee.²³⁴ As such, it would naturally bridge many of the difficulties and benefits of more one-sided and focused alternatives. Ultimately, from the constitutional baseline, any number of stronger protections might arise.

IV. THE CONSTITUTIONAL RIGHT TO INFORMATIONAL PRIVACY

The current federal and state constitutional rights to informational privacy are weak. Although the United States Supreme Court has recognized a federal constitutional interest in informational privacy, it is disputed

are clear rather than ambiguous and amorphous. It involves the basic guarantees to people that their information is being treated thoughtfully”).

231. See CATE, *supra* note 16, at 103-05 (“The most important protection for information privacy is individual responsibility and action . . . Individuals, rather than waiting for the government to take action, must accept the responsibility to know and insist on legal rights.”); Gindin, *supra* note 13, at 1223 (“although . . . a comprehensive federal privacy policy is necessary to guarantee the individual’s right to control the collection and distribution of personal information, the individual must exercise this control”).

232. See Cohen, *supra* note 48, at 1437-38 (“At minimum . . . law can and should establish a new set of institutional parameters that supply incentives for the design of privacy-enhancing technologies to flourish”); Froomkin, *supra* note 9, at 1539 (noting that laws are necessary because “making things illegal, or regulating them, does influence outcomes”); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 520 (1999) (“The trick would be to change the legal entitlements in a way sufficient to change the incentives of those who architect the technologies of consent.”); Pollack, *supra* note 101, at 654 (“pure self regulation does not work; business requires a strong government push”).

233. Froomkin, *supra* note 9, at 1543.

234. See Flaherty, *supra* note 13, at 852-53 (“The purpose of creating a constitutional right to privacy is . . . to allow individuals to assert privacy claims in various arenas that extend beyond general and specific data protection laws”).

PRIORITIZING PRIVACY

whether the Court has recognized a federal constitutional *right* to informational privacy. In contrast, ten state supreme courts recognize an explicit state constitutional right to privacy.²³⁵ The strength of those rights and their application to informational privacy, however, remains dubious. State constitutional rights to informational privacy in the remaining forty states generally mirror the federal interpretation.

In light of the need for a constitutional commitment to informational privacy as an answer to the Internet, this Part considers the degree to which the federal and state constitutions protect informational privacy. It then explores the extent to which those existing constitutional rights have been applied to the Internet. I find that constitutional protection of informational privacy is weak and underutilized, and that it remains thus because there has not been a need for anything more. This Part therefore finishes where it began, with the Internet having created a need for a constitutional commitment to informational privacy.

A. The Federal Right

The leading Supreme Court case on the constitutional interest in informational privacy is *Whalen v. Roe*.²³⁶ The *Whalen* Court recognized an “individual interest in avoiding disclosure of personal matters.”²³⁷ However, the Court found that the statute in question did not facially “establish a constitutional violation.”²³⁸ The majority opinion found that the statute adequately prevented the risk of public disclosure, and furthermore, that the government’s interest in the medical information in question was “essential.”²³⁹

There is significant debate over whether *Whalen* recognizes a constitutional right or merely a constitutional interest in informational privacy.²⁴⁰

235. These states are Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington. *See infra* Part III.B.

236. 429 U.S. 589 (1977).

237. *Id.* at 599.

238. *Id.* at 600.

239. *Id.* at 602.

240. *See, e.g.,* Patricia I. Carter, *Health Information Privacy: Can Congress Protect Confidential Medical Information in the ‘Information Age’?*, 25 WM. MITCHELL L. REV. 223, 238 (1999) (“the United States Supreme Court recognized a limited right to informational privacy in *Whalen v. Roe*”); Turkington, *supra* note 13, at 498 (“*Whalen* was the first case in which the Court explicitly recognized there were two branches to privacy rights under the Constitution: the right to informational privacy (in avoiding disclosure of personal matters) and the right of privacy-autonomy (independence of decisionmaking).” *But see, e.g.,* Kang, *supra* note 19, at 1230 n.157 (noting that “[a] right to informational privacy has not been clearly established as a matter of federal constitutional law” and that *Whalen* is “the closest the Court has come to finding such a right”); Kitajima, *supra* note

The importance of this debate lies in the consequent level of constitutional protection. If there is only a constitutional interest, one's privacy interest can be invaded if the invader has a counterbalancing "need" for the information. On the other hand, if there is a constitutional right, such "ends justifies the means" rationale cannot be used unless the counterbalancing "need" is a compelling governmental interest or is based in a competing constitutional right.

The debate appears to rise from the fact that the Court addressed the issue of whether a constitutional right to informational privacy existed or not, but failed to find a violation of any such right.²⁴¹ Commentators seem to disagree over whether the Court could have recognized a constitutional right to informational privacy without having explicitly protected it.²⁴² Undergirding the debate is the very notable fact that the Court "did not simply rubber-stamp the statute under a rational-basis, due process scrutiny."²⁴³

Since *Whalen*, the Court has not wavered or expounded on its constitutional approach to informational privacy. In fact, the Court seemed almost to weaken the constitutional interest in *Nixon v. Administrator of General*

13, at 577 ("[T]he Supreme Court has never explicitly recognized an informational privacy right").

241. Indeed, some scholars have skirted the debate by taking this exact stance or other such vague language. *See, e.g.*, Gindin, *supra* note 13, at 1186 ("The right to informational privacy was first addressed by the U.S. Supreme Court in *Whalen v. Roe*"); Clement et al., *supra* note 166, at 397 ("The [*Whalen*] Court recognized . . . that the duty to prevent unauthorized disclosure may, in some circumstances, be rooted in the Constitution").

242. For instance, Kitajima cites the following from the *Whalen* opinion as evidence that "[t]he Court did not decide whether a broad informational privacy right exist[s]: 'We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional or by a system that did not contain comparable security provisions.'" Kitajima, *supra* note 13, at 578 (citing *Whalen*, 429 U.S. at 605). However, Cate appears to simply regard this as evidence that "the Supreme Court has never decided a case in which it found that a government regulation or action violated the constitutional privacy right created in *Whalen*." CATE, *supra* note 16, at 63; *see also* Komuves, *supra* note 87, at 561 ("Although recognized to exist, courts have not been ready to find rights of 'informational privacy' in most circumstances").

243. Kang, *supra* note 19, at 1230 n.157 (explaining why "what the Court did is more instructive than what the Court said"); *see also* Chlapowski, *supra* note 13, at 146 (noting that the Court "scrutinized the statute by using a balancing test and not traditional strict scrutiny analysis").

PRIORITIZING PRIVACY

Services,²⁴⁴ a case frequently cited for its confirmation of the *Whalen* analysis.²⁴⁵

Many lower federal courts, however, have recognized a constitutional right to informational privacy post-*Whalen*.²⁴⁶ The clearest examples are the few decisions in which courts have found a violation of the constitutional right to informational privacy.²⁴⁷ Most of the remaining decisions have held, like *Whalen*, that the privacy intrusion is counter-balanced by other significant interests.²⁴⁸ Unlike *Whalen*, though, they explicitly recognize the right to informational privacy.²⁴⁹ Courts have generally acknowledged the right when the government has compelled disclosure of or disseminated intimate or highly personal information.²⁵⁰ As in *Whalen*, the right has not been absolute; the courts have made use of a balancing test that is greater than rational review, but less than strict scrutiny.²⁵¹

244. 433 U.S. 425 (1997).

245. See *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 458 (1977) (finding “the privacy interest asserted by appellant . . . weaker than that found wanting in . . . *Whalen v. Roe*”). For the purposes of the constitutional interest in informational privacy, most commentators have treated *Nixon* and *Whalen* basically as one and the same. See, e.g., Carter, *supra* note 240, at 239 n.8 (citing *Nixon* as support for the *Whalen* principle); Kang, *supra* note 19, at 1230 n.157 (noting that the Court “continued” the *Whalen* “trend” in *Nixon*).

246. See Kitajima, *supra* note 13, at 577 (“Despite the Supreme Court’s silence on [the constitutional right to informational privacy], some circuit courts have used . . . *Whalen v. Roe* to create a right to informational privacy”).

247. See, e.g., *Doe v. Borough of Barrington*, 729 F. Supp. 376 (D.N.J. 1990); *Carter v. Broadlawns Med. Ctr.*, 667 F. Supp. 1269 (S.D. Iowa 1987).

248. See, e.g., *Doe v. S.E. Pa. Transp. Auth.*, 72 F.3d 1133, 1138, 1143 (3d Cir. 1995) (holding the “right of privacy in one’s prescription drug records” subordinate to “a self-insured employer’s need for access to employee prescription records under its health insurance plan”); *Barry v. City of New York*, 712 F.2d 1554, 1563-64 (2d Cir. 1983) (finding that a municipal regulation requiring limited financial disclosure did not violate the “constitutional right to privacy”); *Schacter v. Whalen*, 581 F.2d 35, 37 (2d Cir. 1978) (determining that the “constitutional rights” have not been violated due in part to the fact that “the information is crucial to implementation of sound state policy”); *Plante v. Gonzalez*, 575 F.2d 1119, 1134, 1137 (5th Cir. 1978) (noting that the “Supreme Court has clearly recognized that the privacy of one’s personal affairs is protected by the Constitution,” but finding that disclosure of certain financial information is necessary to “improve[] the electoral process”).

249. E.g., *Tavoulares v. Wash. Post Co.*, 724 F.2d 1010, 1019 (C.A.D.C. 1984) (noting that “[r]ecent Supreme Court decisions indicate that a litigant’s interest in avoiding public disclosure of private information is grounded in the constitution itself”).

250. *Turkington*, *supra* note 13, at 504-08, 517-19.

251. See *CATE*, *supra* note 16, at 64 (describing the “intermediate” scrutiny used by federal appellate courts). The Third Circuit adopted a balancing test with seven factors in *United States v. Westinghouse Electric Corp.*, 638 F.2d 570, 578 (3d Cir. 1980). See *Ki-*

Two circuits are notable exceptions to this trend; they have not recognized a constitutional right to informational privacy. In *Walls v. City of Petersburg*,²⁵² the Fourth Circuit recognized a limited right to informational privacy, one only for information related to an individual's fundamental rights.²⁵³ The Sixth Circuit has "completely rejected the right to informational privacy."²⁵⁴ In *J.P. v. DeSanti*,²⁵⁵ the court concluded that *Whalen* did not create a right to informational privacy.²⁵⁶ The opinion relied primarily on an earlier Supreme Court decision, *Paul v. Davis*,²⁵⁷ which had held that the publication of an arrest was not a violation of the right to privacy.²⁵⁸

Thus, the federal constitutional right to informational privacy is, at best, *limited*. Whether the Supreme Court has recognized the right remains in dispute. The lower federal courts have adopted the right, but at least two Circuits remain outstanding. Moreover, the lower courts subject the right to a balancing test that has produced few victories,²⁵⁹ and the victories have involved intimate or highly personal information. Indeed, a recent decision in a New Jersey federal court found that information concerning the general area in which a person lives is not information of an extremely personal or private nature.²⁶⁰ With regard to the Internet, this case could prove particularly troublesome.²⁶¹ Finally, any degree of protection found by the courts regarding a federal constitutional right to informational pri-

tajima, *supra* note 13, at 578-80. For a thorough analysis of *Whalen* and its lower federal court progeny that calls for the explicit recognition of intermediate scrutiny for the right to informational privacy, see Chlapowski, *supra* note 13. See generally Turkington, *supra* note 13, at 501-19, for an extensive look at how the balancing test has played out in the lower federal courts.

252. 895 F.2d 188 (4th Cir. 1990).

253. *See id.* at 193; *see also* Kitajima, *supra* note 13, at 580.

254. *Id.* at 580-81.

255. 653 F.2d 1080 (6th Cir. 1981).

256. *See id.* at 1088-89.

257. 424 U.S. 693 (1976). Outside the Sixth Circuit, *Paul v. Davis* has been interpreted as limiting the right to informational privacy to disseminations of information outside the public record. Turkington, *supra* note 13, at 500-01.

258. *See* DeSanti, 653 F.2d at 1088-89.

259. *See, e.g.,* Carter, *supra* note 240, at 240 (noting that the Third Circuit's *Westinghouse* test "has generally not favored the protection of individual informational privacy").

260. *See* Paul v. Farmer, 92 F. Supp. 2d 410, 416 (D.N.J. 2000).

261. In fact, the court speaks explicitly to the issue of protecting information on the Internet. *See id.* The extremely limited recent treatment of the constitutional right to informational privacy and the Internet will be discussed in Part III.C *infra*.

PRIORITIZING PRIVACY

vacy would only extend over the government.²⁶² This, too, could prove particularly troublesome when it comes to the Internet.²⁶³

As a final comment on the federal right, it is worthwhile to note that the federal constitutional right to informational privacy is based primarily on a privacy-as-control definition of informational privacy.²⁶⁴ The lower federal courts *have* protected both the acquisition and dissemination of information.²⁶⁵ However, “[e]mployment of the right to challenge the publication or dissemination of information . . . has been less frequent and the jurisprudence is less developed, than it is in the instances where the acquisition of information has been challenged as violating the constitutional right to privacy.”²⁶⁶ This does not mean that the constitutional right is incapable of addressing informational privacy as this Article has defined it. As was discussed with regard to information-gathering technologies, concern over the disclosure of information is a necessary step toward awareness about the consequences of disclosure.²⁶⁷ It does mean, however, that the protection will be weak because, in focusing on disclosure alone, the courts may miss the true informational privacy concerns, as the Supreme Court appears to have done in *Whalen*.²⁶⁸

262. *See, e.g.*, CATE, *supra* note 16, at 66 (“As with other constitutional rights, this information privacy right applies only to government activities”).

263. Commentators now argue that the greatest threat to informational privacy on the Internet comes from private parties. *See, e.g.*, Shimanek, *supra* note 80, at 459 (noting that “databases of personal information on citizens compiled by the private sector are estimated to be more inclusive, extensive, and detailed than government databases”). Each passing day can only add further weight to this argument. This issue will be considered more fully in Part III.C *infra*. Moreover, the government can legally buy much information from private collectors, circumventing any federal constitutional restriction on governmental collection of information.

264. *Whalen*, and consequently *Nixon*, reveal such a view. *See supra* text accompanying notes 38-42.

265. Turkington, *supra* note 13, at 501.

266. *Id.* at 502.

267. *See supra* note 67 and discussion *supra* Part I.B.2.

268. For my full discussion of this point and a parallel criticism by Solove, see *supra* note 56 para. 2. In addition to his criticism of *Whalen*, Solove illustrates this potential failure in his analysis of *Doe v. Southeastern Pennsylvania Transportation Authority*, 72 F.3d 1133 (3d Cir. 1995). *See* Solove, *supra* note 2, at 1438-39. Doe began to fear that other people had learned of his HIV-infection and furthermore began to perceive that they treated him differently. The court, however, held that the constitutional right to informational privacy had not been violated because there had not been a disclosure of information. This “missed the nature of Doe’s complaint.” *Id.* at 1438. Taking Solove’s critique one step further, I argue that the court’s impetus to protect the information would have been far greater if it had understood informational privacy as this Article does, as a right to understand the real and perceived consequences of disclosure.

B. The States

All things being equal, federal constitutional protection of Internet privacy is far more valuable than that offered by the states. The Internet is without geographical constraints. As Fred Cate vividly explains, “[I]n the context of global information networks and national and multinational information users, state protection is of limited significance.”²⁶⁹ Thus, state constitutional protection of informational privacy has something to offer only if it is, or might be, more protective than current federal constitutional protection. Moreover, any such state constitutional right will be more worthwhile as a model for revising current federal protection.

Eleven states have a constitutional right to informational privacy that may provide greater protection than the federal constitution provides. They fall into two categories: implied rights to privacy and explicit rights to privacy.

Some state constitutional rights to privacy are implied, just as the federal constitutional right to privacy generally arises.²⁷⁰ When a state constitutional provision is parallel to a federal constitutional provision, state courts may—if they so choose—interpret the state provision to provide greater protection than the corresponding federal provision.²⁷¹ Of the states whose general right to privacy is implied,²⁷² few have interpreted it to be broader than the implied federal right.²⁷³ Of these, only a small num-

269. CATE, *supra* note 16, at 68.

270. *See, e.g., id.* at 52 (pointing out that the U.S. Supreme Court has interpreted a right to privacy from the amendments).

271. *See, e.g.,* TURKINGTON & ALLEN, *supra* note 19, at 122 (describing how the “supremacy clause of the federal constitution imposes a floor, but not a ceiling, on a state court’s interpretation of individual rights”). For an interesting introduction to the several ways state courts have chosen to view parallel federal provisions, see Mark Silverstein, *Privacy Rights in State Constitutions: Models for Illinois?*, 1989 U. ILL. L. REV. 215, 216-17.

272. Not all states have implied a right to privacy. Maryland, for instance, has not. 74 Op. Att’y Gen. 19 (Md. 1989).

273. The Minnesota Supreme Court has recognized an implied constitutional right, but it has yet to apply this constitutional right to protect individual privacy. Carter, *supra* note 240, at 260-61.

PRIORITIZING PRIVACY

ber might embrace a right to informational privacy.²⁷⁴ I have found only one state that fits this narrow category: New Jersey.²⁷⁵

Ten state constitutions contain explicit provisions for privacy.²⁷⁶ Of these ten provisions, eight were adopted by amendment.²⁷⁷ Since the U.S. Constitution lacks an explicit provision for privacy, these state constitutional rights to privacy begin with the presumption that they are stronger than the federal right. Indeed, the eight provisions adopted by amendment were incorporated in anticipation of an expanded federal right.²⁷⁸ Com-

274. For instance, Tennessee recognizes an implied right of individual privacy, *see* *Davis v. Davis*, 842 S.W.2d 588, 600 (Tenn. 1992), but does not extend it to informational privacy. Carter, *supra* note 240, at 258; *see also* *Cutshall v. Sundquist*, 193 F.3d 466 (6th Cir. 1999); *Doe v. Sundquist*, 2 S.W.3d 919 (Tenn. 1999). Moreover, some state courts have followed *Whalen* directly and as such, are of limited relevance to this Article. *See, e.g.*, *Augustin v. Barnes*, 626 P.2d 625 (Colo. 1981).

275. However, a number of states that have search and seizure provisions that mirror the Fourth Amendment have recognized constitutional privacy with regard to search and seizure that in some cases is stronger than the federal right. Depending upon the facts, these cases could be interpreted as minor forays into a state constitutional protection of informational privacy that is stronger than a federal right. This argument and a few of those states will be briefly considered in Part IV *infra*.

276. These states are Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington. One commentator has claimed that at least twelve states recognize an explicit right to privacy, but provides neither a list nor a citation. *See* Yannon, *supra* note 157, at 28. This author has searched all fifty state constitutions and has found an explicit right to privacy in only ten states. *See* ALASKA CONST. art. I, § 22; ARIZ. CONST. art. II, § 8; CAL. CONST. art. I, § 1; FLA. CONST. art. I, § 23; HAW. CONST. art. I, §§ 6-7; ILL. CONST. art. I, § 6; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10; S.C. CONST. art. I, § 10; WASH. CONST. art. I, § 7. The word “privacy” appears in several other state constitutions, but in a wholly different context. *See, e.g.*, IDAHO CONST. art. I, § 22 (“A crime victim, as defined by statute, has the following rights: (1) To be treated with fairness, respect, dignity and privacy throughout the criminal justice process”). Similarly, Lawrence Gostin claims that “[m]ore than a dozen states have adopted constitutional amendments designed to protect a variety of privacy interests.” Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 498 (1995) (citing ROBERT E. SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS 17-18 (1981)). Smith mentions the ten states I have noted and also includes New York and Pennsylvania. However, the New York and Pennsylvania state constitutions do not explicitly mention privacy.

277. Gormley, *supra* note 15, at 1423-24. The provisions in Washington and Arizona were adopted as parts of the original constitutions.

278. Silverstein, *supra* note 271, at 226 (“Generally, states added express protections of privacy to their constitutions between 1968 and 1980, during a period when commentators expected that the Supreme Court’s privacy/autonomy cases would continue to expand the federal protection of individual liberty”); *see also* Gormley, *supra* note 15, at 1423-25.

pared with their forty colleagues, these states have “a clear opening for following an independent path.”²⁷⁹

The following analysis of these eleven states—New Jersey and the ten states with explicit constitutional provisions for privacy—must be tempered with a caveat. On the whole, state constitutional protection for informational privacy has been of little significance.²⁸⁰ Case law remains sparse,²⁸¹ often making it difficult to say with confidence anything more than that a state appears to have embraced a constitutional right to informational privacy. Assertions as to scope are often no more than guesses. Even California, the state with the most protective state constitutional provision, has produced little protection for informational privacy.²⁸² This should not, however, be taken to mean that the state constitutions are useless. That state constitutional protection has not been of particular significance does not mean it must remain that way.

I. *Alaska*

Article I, section 22 of the Alaska Constitution reads: “The right of the people to privacy is recognized and shall not be infringed.”²⁸³ In line with the state’s strong tradition of protecting privacy,²⁸⁴ the Alaska Supreme Court has extended its constitutional right to the protection of informational privacy. In *Falcon v. Alaska Public Offices Commission*,²⁸⁵ the court struck down a statute that required a physician who was running for public office to disclose names of his patients. Addressing the claim under article I, section 22, the court stated, “certain types of information communicated in the context of the physician-patient relationship fall within a constitutionally-protected zone of privacy.”²⁸⁶ The court went on to balance the interests at stake.²⁸⁷ *Falcon*’s progeny have revealed that the Alaska courts seek to protect “sensitive” or “intimate” personal informa-

279. Silverstein, *supra* note 271, at 215. For a thorough, though old, analysis of the rights to privacy in all ten states, see generally *id.* See also SMITH, *supra* note 276, for a useful discussion of privacy statutes and cases.

280. CATE, *supra* note 16, at 66.

281. See Komuves, *supra* note 87, at 564-65.

282. CATE, *supra* note 16, at 68.

283. ALASKA CONST. art. I, § 22 (adopted by amendment 1972).

284. Even before Alaska adopted its privacy amendment, the state supreme court implied a right to privacy in striking down a junior high regulation that restricted the length of boys’ hair. See Silverstein, *supra* note 271, at 228 (discussing *Breese v. Smith*, 501 P.2d 159 (Alaska 1975)).

285. 570 P.2d 469 (Alaska 1977).

286. *Id.* at 478.

287. See *id.* at 480.

PRIORITIZING PRIVACY

tion, of the nature that “if disclosed even to a friend, could cause embarrassment or anxiety.”²⁸⁸

Article I, section 22 has been explicitly restricted to state actors.²⁸⁹ However, in that same case, the Alaska Supreme Court used the existence of the right as a public policy justification for subjecting a private party to a common law privacy violation.²⁹⁰ The court seemed almost as if it were attempting to justify applying the constitutional right to private parties.²⁹¹

Finally, it is noteworthy that the Alaska right to informational privacy reflects a privacy-as-control definition of informational privacy. This is particularly clear in the recent case *Rollins v. Ulmer*,²⁹² where the court refuted a privacy claim based on “fear of stigmatizing” due to the registration of certain medical information.²⁹³

2. *Arizona*

The privacy provision in the Arizona Constitution²⁹⁴ was adopted in 1911 as part of the original constitution. As such, unlike many of the explicit privacy provisions in other state constitutions, Arizona did not adopt its privacy provision in the 1970s with a liberty interest in mind.²⁹⁵ By 1984, however, it appeared that the Arizona Supreme Court was prepared to give life to an informational privacy interest. In *Mitchell v. Superior*

288. *Doe v. Alaska Superior Court*, 721 P.2d 617, 629 (Alaska 1986). In *Doe*, the court refused to find a privacy interest in a letter written to a public official. An Alaska appellate court has also protected conversations between psychologists and their patients, see *State v. R.H.*, 683 P.2d 269, 280-281 (Alaska Ct. App. 1984), and most recently, the Alaska Supreme Court has recognized the privacy right in the disclosure of certain medical prescriptions, though it did not find a violation of the right, see *Rollins v. Ulmer*, 15 P.3d 749, 752-53 (Alaska 2001).

289. See *Luedtke v. Nabors Alaska Drilling, Inc.*, 769 P.2d 1123, 1130 (Alaska 1989) (“we decline to extend the constitutional right to privacy to the actions of private parties”).

290. See *id.* at 1132-33.

291. The court appeared willing to apply article I, section 22 to private parties, citing the Thirteenth Amendment as a constitutional provision that has been applied to private parties. *Id.* at 1130. However, “[t]he parties . . . failed to produce evidence that Alaska’s constitutional right to privacy was intended to operate as a bar to private action.” *Id.*

292. 15 P.3d 749 (Alaska 2001).

293. *Id.* at 753.

294. “No person shall be disturbed in his private affairs, or his home invaded, without authority of the law.” ARIZ. CONST. art. II, § 8.

295. One commentator has mocked its unusual language as having an exception as broad as the privacy it purports to protect. See CATE, *supra* note 16, at 67 (further noting that the right claimed would presumably exist without having been written into the constitution).

Court,²⁹⁶ the Arizona Supreme Court recognized the petitioner's assertion of "his Constitution-based right of privacy regarding the information in the report that pertains to his personal life."²⁹⁷ Since then, though, a strict informational privacy interest has been absent from the Arizona Supreme Court case law. The explicit right to privacy has generally been limited to questions of search and seizure, surveillance, and other Fourth Amendment privacy concerns.²⁹⁸ Moreover, the right is limited to state actors.²⁹⁹

3. *California*

California's article I, section 1 right to privacy is most notable because it was enacted specifically to address informational privacy concerns, and those goals have been explicitly pursued.³⁰⁰ In particular, the provision sought to provide protection against data gathering and technologically improved surveillance.³⁰¹ It was a response to the ability of computer databases to create profiles and sought to prevent: (1) the secret gathering of information; (2) the overbroad collection and retention of unnecessary personal information; (3) the improper use of information; and (4) the lack of a check for inaccurate records.³⁰² The California Supreme Court recognized these principles in 1975 in *White v. Davis*,³⁰³ and it reiterated them in 1994 in the seminal case *Hill v. NCAA*.³⁰⁴

More significant than the informational privacy purpose of the privacy right is that the California courts have delivered on these promises. California has consistently upheld the expectations that banks, credit card companies, and telephone companies will not release information of their own volition.³⁰⁵ The California Supreme Court has also subjected involun-

296. 690 P.2d 51 (Ariz. 1984).

297. *Id.* at 53.

298. *See, e.g.*, *State v. Bolt*, 689 P.2d 519 (Ariz. 1984) (discussing the unconstitutionality of warrantless entry); *State v. Cramer*, 851 P.2d 147 (Ariz. Ct. App. 1992) (finding that the use of infrared heat measuring devices for surveillance is constitutional).

299. *Cluff v. Farmers Ins. Exchange*, 460 P.2d 666, 669 (Ariz. Ct. App. 1969).

300. "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." CAL. CONST. art. I, § 1. While stated as a general inalienable right, the "moving force" behind the amendment was the specific concern of informational privacy. *White v. Davis*, 533 P.2d 222, 233 (Cal. 1975) (en banc).

301. *See White*, 533 P.2d 222, 233 (Cal. 1975).

302. *Id.* at 234.

303. *See id.* at 233-34.

304. 865 P.2d 633, 654 (Cal. 1994) ("Informational privacy is the core value furthered by the Privacy Initiative").

305. Silverstein, *supra* note 271, at 240.

PRIORITIZING PRIVACY

tary polygraph tests to strict scrutiny and invalidated a state plan to distribute copies of fingerprints that were originally taken for the issuance of drivers' licenses.³⁰⁶ "Well-established social norms" determine which categories of information are protected.³⁰⁷ Moreover, in 1994 the Supreme Court confirmed what appellate courts had been saying for two decades: California's constitutional right is applicable to private parties.³⁰⁸ Of course, the right to informational privacy is not absolute. The *Hill* court made explicit a sliding scale balancing test—the level of countervailing interest necessary varies according to the centrality of the implicated privacy interest.³⁰⁹

Perhaps the most noteworthy element of California's constitutional right to informational privacy is its consistency with this Article's definition of informational privacy. The California Supreme Court has noted, "Legally recognized privacy interests [include] . . . interests in precluding the dissemination or misuse of sensitive and confidential information ('informational privacy')." ³¹⁰ To be sure, the court emphasizes an element of control not apparent in this Article's conception of informational privacy.

4. *Florida*

It took the state of Florida two attempts to nail down a constitutional amendment that begins to protect informational privacy. In 1968, Florida added "private communications" to the state constitution's search and seizure clause.³¹¹ While this provision facially appears to add an element of informational privacy, it did very little in reality. The Florida Supreme Court ruled in 1980 that article I, section 12 did not prevent the disclosure of highly personal information.³¹² That same year Florida voters added

306. *Id.* at 240-41.

307. *Hill*, 865 P.2d at 654.

308. *See id.* at 644 ("the Privacy Initiative in Article I, Section 1 of the California Constitution creates a right of action against private as well as government entities"). In cases such as *Cutter v. Brownbridge*, 228 Cal. Rptr. 545 (Dist. Ct. App. 1986), and *Porten v. University of San Francisco*, 134 Cal. Rptr. 839 (Dist. Ct. App. 1976), appellate courts had been interpreting the court's language in *White* as a green light to go against private parties.

309. *See Hill*, 865 P.2d at 655-56.

310. *Id.* at 654.

311. "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated." FLA. CONST. art. I, § 12 (adopted by amendment 1968).

312. *See Shevin v. Byron, Harless, Schaffer, Reid & Assocs.*, 379 So. 2d 633, 639 (Fla. 1980). The court refused to prevent disclosure of interviews that a psychological consulting firm had conducted. *See id.* at 635-36.

article I, section 23³¹³ and “gained some constitutional protection from the disclosure of intimate information regarding their personal affairs.”³¹⁴ A desire to protect personal, private information was part of the impetus for the second amendment.³¹⁵

Florida’s protection of informational privacy begins with *Winfield v. Division of Pari-Mutuel Wagering*.³¹⁶ Ruling on the disclosure of bank records, the Florida Supreme Court established a balancing test for protecting informational privacy.³¹⁷ Two years later, the court decided *Rasmussen v. South Florida Blood Service, Inc.*,³¹⁸ Florida’s leading case on informational privacy. It found that article I, section 23 protects “the right to determine whether or not sensitive information about oneself will be disclosed to others.”³¹⁹ This case has been cited as “[t]he paradigm of weighing the governmental interest in truth-seeking [against] strong privacy interests.”³²⁰

Nevertheless, Florida’s protection of informational privacy has been criticized as weak.³²¹ To begin with, the language of the privacy provision is biased against protecting “public records.”³²² This has not only caused courts to avoid protecting intimate information that is actually in public records,³²³ but it has also caused Florida courts to second-guess the pri-

313. “Every natural person has the right to be let alone and free from governmental intrusion into the person’s private life except as otherwise provided herein. This section shall not be construed to limit the public’s right of access to public records and meetings as provided by law.” FLA. CONST. art. I, § 23 (adopted by amendment 1980).

314. Silverstein, *supra* note 271, at 246-47.

315. See Daniel R. Gordon, *Upside Down Intentions: Weakening the State Constitutional Right to Privacy, A Florida Story of Intrigue and a Lack of Historical Integrity*, 71 TEMPLE L. REV. 579, 604 (1998) (“The privacy provision was intended to provide a high level of protection for personal, private information”).

316. 477 So. 2d 544 (Fla. 1985).

317. See *id.* at 547-48.

318. 500 So. 2d 533 (Fla. 1987).

319. *Id.* at 536.

320. Turkington, *supra* note 13, at 512-13.

321. See Gordon, *supra* note 315, at 580 (criticizing Overton & Giddings, *supra* note 3, for “grossly understat[ing] how little informational privacy protection exists under the Florida constitution”). Gordon’s article is a detailed, semi-quantitative look at how Florida’s informational privacy right has been far outpaced by the attention Florida courts have given the question of behavioral privacy.

322. “This section shall not be construed to limit the public’s right of access to public records and meetings as provided by law.” FLA. CONST. art. I, § 23.

323. See *Michel v. Douglas*, 464 So. 2d 545 (Fla. 1985); *Forsberg v. Hous. Auth. of City of Miami Beach*, 455 So. 2d 373 (Fla. 1984). In *Post-Newsweek Stations, Inc. v. Doe*, 612 So. 2d 549 (Fla. 1992), the court found that the privacy amendment did not protect names and addresses contained in public records.

PRIORITIZING PRIVACY

vacy of seemingly private information.³²⁴ In addition, and perhaps more significantly, the privacy provision does not protect against private action.³²⁵ If implicated, however, the right to privacy is fundamental, and can only be overcome by a compelling governmental interest.

Any right protected by the Florida constitution reflects a privacy-as-control conception of informational privacy.³²⁶

5. *Hawaii*

Hawaii has followed a path eerily similar to Florida's, but it has ended up with a greater constitutional protection of informational privacy both on paper and in the courtroom. In 1968, Hawaii amended its search and seizure provision, contained in article I, section 6, to consider privacy explicitly.³²⁷ The drafters of the provision aimed to both protect against electronic surveillance and preserve personal autonomy and informational privacy.³²⁸ In ensuing interpretations, however, the former took precedence over the latter, leading to a second amendment in 1978 that would "unquestionably protect informational privacy and personal autonomy."³²⁹

This second amendment has been described as "the most specific and protective of any of the state constitutional provisions guarding privacy interests."³³⁰ It reads: "The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest.

324. See Overton & Giddings, *supra* note 3, at 39 ("When such information is not contained in a so-called 'public record,' the court has been cautious in protecting the disclosure of personal information"). For instance, an individual's smoking habits have been interpreted as being on public record. See *City of North Miami v. Kurtz*, 653 So. 2d 1025, 1028 (Fla. 1995).

325. See Overton & Giddings, *supra* note 3, at 41 ("the provision provides no protection from private or commercial intrusion because the present provision is limited to governmental intrusions").

326. See Silverstein, *supra* note 271, at 247 ("In the view of the Florida Supreme Court, the freestanding privacy provision protects an individual's right to control the flow of personal information to others").

327. "The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures and invasion of privacy shall not be violated . . ." HAW. CONST. art. I, § 7 (amended as art. I, § 5 in 1968; renumbered to art. I, § 7 in 1978 with no changes in language).

328. Silverstein, *supra* note 271, at 241.

329. *Id.* at 242-43; see also Julia B.L. Worsham, Case Note, *Privacy Outside of the Penumbra: A Discussion of Hawai'i's Right to Privacy After State v. Mallan*, 21 U. HAW. L. REV. 273, 281 (1999) ("This new section was intended to eliminate confusion over the scope of the right to privacy, and to establish privacy as a fundamental right in the informational and personal autonomy sense").

330. CATE, *supra* note 16, at 67.

The legislature shall take affirmative steps to implement this right.”³³¹ The Hawaii Supreme Court has stated on several occasions that this provision protects a right to informational privacy.³³² Notably, it has found a reasonable expectation of privacy in personal financial affairs.³³³ Although the Supreme Court has not yet determined whether the right should extend to private parties, legislative history indicates that the amendment was intended to apply to private action,³³⁴ and the Hawaii Supreme Court has relied heavily on the legislative history when interpreting article I, section 6.³³⁵

The Hawaii constitutional right to informational privacy incorporates elements of both the privacy-as-control definition and this Article’s definition of informational privacy. The Supreme Court has found a right to “avoid[] disclosure of personal matters,”³³⁶ and the legislative history reveals a concern about the “possible abuses in the use of highly personal and intimate information” by others.³³⁷

6. *Illinois*

The legislative history of the 1970 Illinois Constitution’s privacy provision in article I, section 6³³⁸ seems to imply a strong desire to protect informational privacy, demonstrating a concern even for the disclosure of nonpersonal information.³³⁹ However, by 1989, the Illinois Supreme Court had done little to advance this proposition. The Supreme Court appeared

331. HAW. CONST. art. I, § 6 (adopted by amendment 1978).

332. *See* State v. Mallan, 950 P.2d 178 (Haw. 1998); McCloskey v. Honolulu Police Dep’t, 799 P.2d 953, 956-57 (Haw. 1990); Nakano v. Matayoshi, 706 P.2d 814, 818-19 (Haw. 1985).

333. *See* Nakano, 706 P.2d at 819.

334. *See* McCloskey, 799 P.2d at 956 (“it is the intent of [this] Committee to insure that privacy is treated as a fundamental right for purposes of constitutional analysis. Privacy as used in this sense concerns the possible abuses [of] highly personal and intimate information in the hands of government or private parties.” (quoting Committee of the Whole Rep. No. 15)).

335. *Id.* at 956-57; Nakano, 706 P.2d at 818-19.

336. McCloskey, 799 P.2d at 957.

337. *Id.* at 956 (quoting Committee of the Whole Rep. No. 15).

338. “The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means.” ILL. CONST. art. I, § 6 (adopted with new Illinois constitution 1970).

339. *See* Silverstein, *supra* note 271, at 278-79, 291 (“Suggesting that article I, section 6 goes even further in protecting informational privacy, [Delegate] Dvorak offered the example of a government data bank indexed by social security numbers and storing such nonpersonal information as weight, height, and age. The committee members believed [that] would unreasonably invade privacy under article I, section 6”).

PRIORITIZING PRIVACY

to adopt a dual approach in *People v. Tisler*,³⁴⁰ choosing to promote privacy in the search and seizure context, but foregoing development of further substantive rights to privacy.³⁴¹ Following *Tisler*, the growth of a right to informational privacy was limited to vague assertions that article I, section 6 provided rights that surpassed the federal right to privacy³⁴² and was relegated to the appellate courts.³⁴³ While the Illinois appellate courts found a constitutional right of privacy in bank records,³⁴⁴ this dearth of specific Supreme Court activity led one commentator to accuse the Illinois high court of a “disdain for the state right of privacy.”³⁴⁵

In 1992, however, the Illinois Supreme Court confirmed that the right to privacy in Illinois “affords greater protection” than the federal right,³⁴⁶ and explicitly granted a right to informational privacy.³⁴⁷ The Illinois Appellate Court has since also confirmed the constitutional right of privacy in bank records.³⁴⁸ However, the Illinois right to privacy does not appear to apply to private action.³⁴⁹

7. Louisiana

The privacy language in article I, section 5 of the Louisiana Constitution is literally an expansion of its search and seizure provision³⁵⁰ and, as

340. 469 N.E.2d 147 (Ill. 1984).

341. See Silverstein, *supra* note 271, at 268, 269 (arguing that the *Tisler* court “segregated the search and seizure portion of article I, section 6,” thus discouraging the development of “an outright state constitutional protection of informational privacy”).

342. See, e.g., *People v. Porter*, 521 N.E.2d 1158, 1162 (Ill. 1988) (“our State Constitution may afford protection of certain rights not covered by the Federal Constitution. For instance, our state constitution grants certain privacy rights not addressed or afforded by the Federal Constitution”).

343. See Silverstein, *supra* note 271, at 270 (“Appellate court holdings have applied article I, section 6 to . . . informational privacy”).

344. See *People v. Jackson*, 452 N.E.2d 85, 89 (Ill. App. Ct. 1983).

345. Silverstein, *supra* note 271, at 270.

346. *In re May 1991 Will County Grand Jury*, 604 N.E.2d 929, 934 (Ill. 1992).

347. See *id.* at 935 (“A person has a reasonable expectation that his private records will not be exposed to public view We believe that the individual's privacy interest in his physical person, as well as his privacy interest in his documents, must be protected”).

348. See *Dufour v. Mobile Oil Corp.*, 703 N.E.2d 448, 452 (Ill. App. Ct. 1998). The Illinois Supreme Court does not appear to have yet addressed this issue.

349. One commentator claims that the Illinois constitutional right to privacy does apply to private parties, but he cites a case that only applies it to private actors in the context of employment discrimination. See Kearns, *supra* note 13, at 1010 n.181.

350. “Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy.” LA. CONST. art. I, § 5.

such, has primarily been interpreted in that context. One commentator, writing soon after the language was adopted, has argued that the privacy provision protects informational privacy.³⁵¹ However, as of 1989, “[I]tigators [had] seldom argued for substantive rights of privacy.”³⁵²

Louisiana courts have weighed the state-mandated public right to know against an individual’s interest in avoiding certain sensitive disclosures that may cause embarrassment or result in an unreasonable intrusion.³⁵³ In particular, the Louisiana Supreme Court discussed the constitutional right of privacy “in the context of disclosure of facts about an individual or his property.”³⁵⁴

Moreover, the Louisiana Supreme Court interpreted the provision to provide more protection than the Fourth Amendment. For instance, in *State v. Hernandez*,³⁵⁵ the court noted that the right of privacy is “one of the most conspicuous instances in which our citizens have chosen a higher standard of individual liberty than that afforded by the jurisprudence interpreting the federal constitution.”³⁵⁶ The Court also appears to have determined that the right to privacy should be applicable against private actors.³⁵⁷

Whatever right to informational privacy exists in Louisiana, the search and seizure overtones clearly ground it in a privacy-as-control definition of informational privacy. Search and seizure provisions are intended to avoid and regulate disclosure, a major tenet of the privacy-as-control conception of informational privacy.³⁵⁸

351. See Silverstein, *supra* note 271, at 254 n.356.

352. *Id.* at 254.

353. See, e.g., *Capital City Press v. E. Baton Rouge Parish Metro. Council*, 696 So. 2d 562, 566-67 (La. 1997) (finding no right to privacy and rejecting even the use of a balancing test with regard to the disclosure of an applicant’s resume); *Broderick v. State Dep’t of Env’tl. Quality*, 761 So. 2d 713, 715 (La. Ct. App. 2000) (affirming the trial court’s finding that “the competing public interest was outweighed by the [constitutional] privacy interest, particularly because it found that the public interest would not be further served by disclosure”); *Trahan v. Larivee*, 365 So. 2d 294, 298-99 (La. Ct. App. 1978) (considering the constitutional right to privacy in certain government employment evaluations).

354. *Capital City Press*, 696 So. 2d at 566.

355. 410 So. 2d 1381 (La. 1982).

356. *Id.* at 1385.

357. See *Moresi v. Dep’t of Wildlife & Fisheries*, 567 So. 2d 1081, 1092 (La. 1990) (finding that, although no violation of the right to privacy occurred, the lack of the phrase “no law shall” indicates a protection that “goes beyond limiting state action”).

358. See *supra* Part I.A.

PRIORITIZING PRIVACY

8. *Montana*

The explicit right to individual privacy in article II, section 10 of the Montana Constitution³⁵⁹ has been interpreted to provide greater protection for informational privacy than the federal constitution.³⁶⁰ In the oft-cited 1982 case, *Montana Human Rights Division v. Billings*,³⁶¹ the court stated this proposition explicitly³⁶² while holding that employees maintained a privacy interest in employment records, even though the information had been voluntarily conveyed to the city and was arguably “general knowledge.”³⁶³

The Montana Supreme Court still relies on its holding from this case.³⁶⁴ In *State v. Burns*,³⁶⁵ the court cited *Montana Human Rights Division* in support of a privacy interest in personnel records that were being sought in discovery.³⁶⁶ The *Burns* court labeled the constitutional privacy provision “one of the most stringent protections of its citizens’ right to privacy in the country.”³⁶⁷ In *Missouliau, Inc. v. Board of Regents of Higher Education*,³⁶⁸ the Montana Supreme Court cited *Montana Human Rights Division* while upholding a privacy interest in the job performance evaluations of university presidents against a statutory/constitutional public right to know.³⁶⁹

The constitutional right to privacy is determined by a two-pronged test: (1) is there an expectation of privacy; and (2) does society recognize that expectation as reasonable?³⁷⁰ The right can be overcome only by a compelling state interest.³⁷¹ One commentator, however, criticizes the

359. “The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.” MONT. CONST. art. II, § 10.

360. Silverstein, *supra* note 271, at 231-32.

361. 649 P.2d 1283 (Mont. 1982).

362. *See id.* at 1286 (“This Court has recognized that the protection it offers is more substantial than that inferred from the Federal Constitution”).

363. *Id.* at 1286-87.

364. The Montana Supreme Court most recently cited *Montana Human Rights Division* in a favorable light in *Associated Press, Inc. v. Montana Dep’t of Revenue*, 4 P.3d 5, 12 (Mont. 2000).

365. 830 P.2d 1318 (Mont. 1992).

366. *See id.* at 1320.

367. *Id.*

368. 675 P.2d 962 (Mont. 1984).

369. *See id.* at 967-70.

370. *See Burns*, 830 P.2d at 1320. In *Montana Human Rights Division*, the court noted that “relatively innocuous telephone records” did not maintain a right to privacy. 649 P.2d at 1287.

371. *Montana Human Rights Div.*, 649 P.2d at 1288.

courts for having failed to truly embrace the historical intent to protect privacy to a greater degree, and against the intrusions of modern society.³⁷² His comments are lent credence by the fact that in 1985 the Montana Supreme Court retreated from an interpretation that allowed the application of the constitutional right to private action.³⁷³

The Montana constitutional right to informational privacy adopts a privacy-as-control definition. In fact, the *Montana Human Rights Division* court cited the following definition of privacy: “Privacy has been defined as the ability to control access to information about oneself.”³⁷⁴

9. *New Jersey*

New Jersey does not have an explicit constitutional right to privacy. However, it has an implied right to privacy that its supreme court has expanded beyond the scope of federal court decisions³⁷⁵ and, more importantly, into the realm of informational privacy.³⁷⁶ Two cases are particularly noteworthy because they consider concerns that may be relevant to the threat the Internet poses to informational privacy. First, in *State v. Hunt*,³⁷⁷ the New Jersey Supreme Court departed from the federal standard³⁷⁸ and protected the privacy of telephone records from unreasonable government intrusion.³⁷⁹ The Court argued that, “it is unrealistic to say that the cloak of privacy has been shed because the telephone company and some of its employees are aware of this information.”³⁸⁰ This conclusion could have ramifications for Internet Service Providers and their records, since those providers and their employees are almost directly analogous to telephone companies and their employees.

372. See generally William C. Rava, Comment, *Toward a Historical Understanding of Montana's Privacy Provision*, 61 ALB. L. REV. 1681 (1998).

373. The Montana Supreme Court overruled a long line of private search cases in *State v. Long*, 700 P.2d 153 (Mont. 1985), holding that the constitutional right to privacy restricts only state action. See *id.* at 156.

374. *Montana Human Rights Division*, 649 P.2d at 1287.

375. Silverstein, *supra* note 271, at 215 n.6. Silverstein cites *State v. Saunders*, 381 A.2d 333 (N.J. 1977), and *In re Quinlan*, 355 A.2d 647 (N.J. 1976), as support for this claim.

376. *Doe v. Poritz*, 662 A.2d 367, 412 (N.J. 1995) (“We have found a [state] constitutional right of privacy in many contexts, including the disclosure of confidential or personal information”).

377. 450 A.2d 952 (N.J. 1982).

378. See *id.* at 955 (“In this case we are persuaded that the equities so strongly favor protection of a person’s privacy interest that we should apply our own standard rather than defer to the federal provision”).

379. See *id.* at 956.

380. *Id.*

PRIORITIZING PRIVACY

Second, though the New Jersey Supreme Court determined in *Doe v. Poritz*³⁸¹ that there is no reasonable expectation of privacy in individual bits of information, such as a name or address,³⁸² it further concluded that a compilation of information implicates a privacy interest.³⁸³ The court reasoned that no matter how public the information, the scattered information still maintained the ability to “remain obscure.”³⁸⁴ Although the state interest in disclosure “substantially” outweighed the privacy interest of past sex offenders,³⁸⁵ the implications of these findings for Internet practices such as online profiling could be significant.

10. *South Carolina*

Though article I, section 10 of the South Carolina Constitution contains an explicit reference to the word “privacy,”³⁸⁶ the word is no more than an addendum to the search and seizure provision and has been interpreted as such. Indeed, one commentator noted in 1989 that the South Carolina Supreme Court had yet to specifically interpret the privacy language in the state constitution.³⁸⁷ It appears that this has remained the case. The South Carolina Supreme Court seems to mention “the right to privacy” only as it is generally protected by article I, section 10.³⁸⁸ The court has been more concerned with intrusion than disclosure or dissemination, and there is no independent right to informational privacy in South Carolina.

Perhaps the closest the South Carolina Supreme Court has come to considering informational privacy as an interest separate from search and seizure was in *Southern Bell Telephone & Telegraph Co. v. Hamm*.³⁸⁹ In *Hamm*, the court considered a constitutional challenge to the use of Caller

381. 662 A.2d 367 (N.J. 1995).

382. *See id.* at 407.

383. *See id.* at 409 (finding that the “totality of the information disclosed to the public” created a privacy interest).

384. *Id.* at 411. In *Poritz*, the court was ruling on the constitutionality of registration and notification laws for sex offenders. Here, the government compiled and disseminated the information—even information in the public record. By doing so the government reduced the costs and effort necessary for others to gather the information and the government also publicized connections between the information that may otherwise never have been made. *See id.*

385. *Id.* at 411.

386. “The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated.” S.C. CONST. art. I, § 10 (adopted by amendment in 1971).

387. *See Silverstein, supra* note 271, at 258.

388. *See, e.g., State v. Andrews*, 479 S.E.2d 808, 810 (S.C. 1996).

389. 409 S.E.2d 775 (S.C. 1991).

ID.³⁹⁰ The case differs from most that invoke article I, section 10 because it considered a claim under the South Carolina privacy provision as parallel to a Fourteenth Amendment federal privacy claim rather than a Fourth Amendment challenge.³⁹¹ In addition, the court examined the caller's "interest in not revealing" her telephone number.³⁹² Ultimately, the court followed the United States Supreme Court's lead in *Smith v. Maryland*³⁹³ and found no privacy interest in avoiding disclosure.³⁹⁴

11. *Washington*

The explicit privacy provision in the Washington Constitution³⁹⁵ was originally intended as Washington's version of the Fourth Amendment.³⁹⁶ However, by the early 1980s, the Washington Supreme Court had begun extending the state constitutional right of privacy to informational privacy and personal autonomy.³⁹⁷ The Washington Supreme Court has interpreted its 1986 decision, *Peninsula Counseling Center v. Rahm*,³⁹⁸ as granting rational basis scrutiny to the privacy interest in avoiding "disclosure of intimate information to government agencies."³⁹⁹ Only a "legitimate governmental interest" is necessary to overcome the constitutional provision.⁴⁰⁰ In *Peninsula*, the court found an informational privacy interest in avoiding disclosure of certain medical information, but found it subject to the government interest in maintaining adequate mental health facilities and ensuring care for individual patients.⁴⁰¹ The court cited *Peninsula* in *O'Hartigan v. Department of Personnel*,⁴⁰² where it ruled that the government interest in having law enforcement officers of high moral character outweighed a privacy interest in not taking a polygraph.⁴⁰³

390. *See id.* at 779.

391. *See id.*

392. *Id.*

393. 442 U.S. 735 (1979).

394. *See Hamm*, 409 S.E.2d at 779-80. *Hamm* also reveals that article I, section 10 applies only to state action. *See id.* at 778.

395. "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." WASH. CONST. art. I, § 7.

396. Silverstein, *supra* note 271, at 248 n.306.

397. *See id.* at 249.

398. 719 P.2d 926 (Wash. 1986).

399. *O'Hartigan v. Department of Personnel*, 821 P.2d 44, 48 (Wash. 1991).

400. *Id.*

401. *See Peninsula*, 719 P.2d at 929-30.

402. 821 P.2d 44 (Wash. 1991).

403. *See id.* at 49.

PRIORITIZING PRIVACY

In the recent case *In re Meyer*,⁴⁰⁴ the Washington Supreme Court clarified matters significantly. It noted that the Washington Constitution protects an “interest in confidentiality, or the nondisclosure of personal information.”⁴⁰⁵ However, it confirmed its 1997 ruling in *Ino Ino, Inc. v. City of Bellevue*,⁴⁰⁶ which held that this right to informational privacy is no greater than that protected by the federal constitution.⁴⁰⁷

Given the weak status of the Washington right, it is interesting to note Justice Pearson’s stirring and forward-looking dissent in *Peninsula*. Describing our “information-intensive society” as “dependent upon the marvels of the modern computer” and invoking Orwell and information law scholar Alan Westin, Justice Pearson called for Washington Constitution article I, section 10 to be interpreted as protecting a fundamental right of informational privacy.⁴⁰⁸

C. The Story Thus Far

Given the sheer magnitude and significance of the threat posed by the Internet to informational privacy, one might think that every legal weapon would be wielded and every battlement manned, especially the federal and state constitutions.⁴⁰⁹ Indeed, the Supreme Court, staring into its crystal ball in 1977, left open a rallying point in *Whalen*: “We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.”⁴¹⁰ As exemplified in Justice Pearson’s dissent in *Peninsula*⁴¹¹ and elsewhere, state supreme court justices have left similar “invitations.”⁴¹²

404. 16 P.3d 563 (Wash. 2001).

405. *Id.* at 567.

406. 937 P.2d 154 (Wash. 1997).

407. *See In re Meyer*, 16 P.3d at 567-69.

408. *Peninsula Counseling Center v. Rahm*, 719 P.2d 926, 930-33 (Wash. 1986) (Pearson, J., dissenting).

409. *See Kitajima, supra* note 13, at 577-81 (“the growth of the Internet . . . will likely prompt the Supreme Court to consider the informational privacy issue. . . . We live in an ‘information age,’ where people are more concerned than ever about access and misuse of their personal information”).

410. *Whalen v. Roe*, 429 U.S. 589, 605 (1977). Justice Brennan was slightly more forthcoming in his concurrence. “The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.” *Id.* at 606 (Brennan, J., concurring).

411. 719 P.2d at 930.

412. *See supra* text accompanying note 408.

Reality does not reflect reason, however. Few claims of privacy violations on or due to the Internet have invoked a constitutional right to informational privacy. Perhaps the best illustration of the scarcity of claims is seen in the paradigm case of *Crowley v. CyberSource Corp.*⁴¹³ In *Crowley*, the plaintiff claimed that he gave Amazon.com his personal information,⁴¹⁴ which Amazon.com allegedly then transferred to CyberSource, who stored it and used it to create a personal profile.⁴¹⁵ Though California has arguably the strongest constitutional protection of informational privacy, Crowley's state law-based causes of action included only common law claims of unjust enrichment, invasion of privacy, negligence, fraud by concealment, and breach of contract.⁴¹⁶

On the federal legislative front, where constitutional rhetoric might be expected as a means of fanning the flames for Internet legislation,⁴¹⁷ it is the *lack* of a constitutional right that was cited as a reason for the Children's On-line Privacy Protection Act,⁴¹⁸ the only Internet privacy-specific federal legislation.⁴¹⁹ Most other Congressional references to the constitutional right to privacy in the Internet context regard concerns about legislation that might encroach on the constitutional right.⁴²⁰ Only Senator

413. 166 F. Supp. 2d 1263 (N.D. Cal. 2001).

414. *Id.* at 1265.

415. *Id.*

416. *Id.* at 1267. Crowley's failure to include a constitutional claim for privacy could have resulted from any number of reasons, but probably because the constitutional rights to informational privacy have traditionally been perceived as weak, useless, and sometimes laughable. See generally *infra* text accompanying note 423-425.

417. For instance, in a different context, Representative Sherman once invoked the constitutional right to privacy in the following vivid argument: "it is also mind-boggling to contemplate the picture of Uncle Sam riding roughshod over privacy rights that have been guaranteed under our Constitution since the days of our Founding Fathers." 147 CONG. REC. E2289 (1997).

418. 15 U.S.C. §§ 6501-06 (2000).

419. Representative Inslee stated: "With no Constitutional protections over the sharing of personal information to third parties . . . online, Acts such as COPPA . . . which I introduced, are necessary safeguards of our privacy. Americans have a right to privacy in regards to their personal information, and I recognize the Children's Online Privacy Protection Act as enhancing this right." 146 CONG. REC. E616-01 (2000).

420. This has been the case in House and Senate discussions about legislation that would attempt to restrain "cyber terrorism," 146 CONG. REC. H978 (2000), online sexual predators, 144 Cong. Rec. H4498 (1998), unsolicited commercial email, 147 CONG. REC. S2996 (2001), and children's access to online pornography, 144 CONG. REC. H9909 (1998).

PRIORITIZING PRIVACY

Leahy has come close to invoking the constitutional right to privacy as a reason for *expanding* Internet privacy.⁴²¹

Lastly, commentators have also been hesitant to call on the constitutional right to privacy as a solution to the Internet threat.⁴²²

As this Part has shown, both the federal and state constitutional rights to informational privacy are weak at best, and this is a likely reason that the campaign to protect privacy on the Internet does not discuss such a right. Indeed, commentators who dismiss both the federal and state constitutions as possible sources of protection often do so *because* those constitutional rights are weak.⁴²³ Moreover, the few constitutional claims made have not met with much success.⁴²⁴ In fact, even in cases where the Inter-

421. As the chairman of the Internet privacy-focused Senate Democratic Privacy Task Force, Senator Leahy noted in his December 2000 report on the lack of Internet privacy legislation that “[t]he right to privacy is a personal and fundamental right protected by the Constitution of the United States.” 146 CONG. REC. S11777 (2000). Senator Leahy has sponsored several bills purporting to “protect the privacy and constitutional rights of Americans.” 145 CONG. REC. S4040 (1999); 146 Cong. Rec. S2727 (2000); 146 CONG. REC. S2738 (2000). Senator Dodd appears once to have implicitly invoked the constitutional right. *See id.* at S713.

Actually, if considered more closely, legislators acting to manifest a constitutional right to privacy might be a negative indicator. Such a situation could reflect the inability of the constitutional right to serve independently as a remedy in and of itself.

422. In a student-authored note, Thomas Kearns argues that “constitutional safeguards are a more effective means of ensuring that new technology does not erode privacy.” Kearns, *supra* note 13, at 1003. Kearns never mentions the Internet in particular, but he is strongly concerned about computer databases. *See id.* at 990-95. In another student-authored note, Kyla Kitajima does not call for a constitutional right, but notes “[a] constitutional informational privacy right will be helpful in many Internet contexts.” Kitajima, *supra* note 13, at 582. *See also supra* notes 13-17 and accompanying text for the point that few commentators have called for a constitutional right to informational privacy at all.

423. *See, e.g.,* CATE, *supra* note 16, at 68 (concluding that “[e]ven the most protective state constitutional provisions . . . have yielded little protection for information privacy”); Kang, *supra* note 19, at 1230 (citing the fact that “it is unclear to what extent the Constitution actually protects information privacy” as a reason why federal constitutional law will provide little protection).

424. For example, in *A.A. v. New Jersey*, 176 F. Supp. 2d 274 (D.N.J. 2001), plaintiffs brought suit alleging that the Internet Registry Act, an act requiring the notification portion of a sex offender registry to be posted on the Internet, violated their federal constitutional right to informational privacy in their home addresses, and in the totality of the information assembled and posted. The claim centered on “the implications of the undifferentiated disclosure” necessarily resulting from publication on the Internet. *Id.* at 297-98. The court upheld only the privacy interest in the home addresses, concluding that the remainder of the information was not sufficiently personal or intimate to warrant protection. *See id.* at 302. Note that this ruling reveals the privacy-as-control blindness seen so often in informational privacy cases. The court focused on the fact that the proposed

net has not been specifically alleged as the reason for the privacy violation, courts have hinted that the constitutional right to informational privacy is too weak to protect against the Internet.⁴²⁵

A second possible explanation for the lack of constitutional claims to privacy on the Internet is that the constitutional right to informational privacy rarely applies to private action. Commentators have frequently cited the state action doctrine as the reason why the federal constitution should not be used to protect data privacy.⁴²⁶ Unfortunately, on the Internet, private parties are quickly becoming, if they are not already, the primary threat to informational privacy.⁴²⁷ Of course, this does not explain why Crowley did not bring a state constitutional claim for informational privacy on the Internet in his case since California's constitutional right to privacy does extend to private parties.

Internet registry “dispenses with any safeguards designed to carefully limit disclosure of protected information,” and failed to adequately consider the consequences of disclosure or the perceived consequences of a *compilation* of information. *Id.* at 302-05.

Two years earlier, similar federal constitutional claims had been made in a Michigan federal district court and a Kansas state appellate court. *See Akella v. Michigan Dep't of State Police*, 67 F. Supp. 2d 716, 720 (E.D. Mich. 1999); *State v. Stevens*, 992 P.2d 1244, 1247 (Kan. App. 1999). Both cases resulted in similarly unsuccessful rulings. *See Akella*, 67 F. Supp. 2d at 730; *Stevens*, 992 P.2d at 1248-49.

425. For instance, in *Valley Presbyterian Hospital v. Superior Court*, 94 Cal. Rptr. 2d 137 (Cal. Ct. App. 2000), a California appellate court implied that information on the Internet would be considered public record with a minimal privacy interest. *Id.* at 141 (noting that the privacy interest in the case was minimal partly because the information in question is “easily accessed on the Internet”). But, consider *Arakawa v. Sakata*, 133 F. Supp. 2d 1223 (D. Haw. 2001), in which the court seemed to say that the availability of information on the Internet has strengthened the constitutional privacy interest in one's social security number. *Id.* at 1229.

426. *See, e.g.*, Helms, *supra* note 2, at 314 (arguing that federal constitutional protection has a “considerable weakness[]” with regard to privacy on the Internet because “[c]onstitutional claims do not address the most prevalent source of privacy violations—private companies”); Kang, *supra* note 19, at 1230 (finding that “the collection of personal information in America . . . is largely unregulated by law[]” partly because “federal constitutional law provides no protection of an individual's information privacy from invasion by the private sector”); Solove, *supra* note 2, at 1435 (noting that “the Constitution only protects against state action, and many databases belong to the private sector”).

427. *E.g.*, Kang, *supra* note 19, at 1201 (noting that in the cyberspace context “the private sector has come to rival government in the use of personal information”); Overton & Giddings, *supra* note 3, at 26 (calling intrusions by private or commercial entities “without question, . . . the greatest privacy challenge in the coming decade and the twenty-first century”); Cody, *supra* note 40, at 1199 (“Although the government, as a single entity, may rank first in the collection and use of personal identifiable information, the combined collection activities of the private sector far outweigh the collection practices of the government”).

PRIORITIZING PRIVACY

These explanations beg the real question, though: Why has the constitutional right to informational privacy remained weak and restricted? The underlying reason is need. Historically, Americans have not had a general interest in privacy, and in particular, informational privacy.⁴²⁸ Privacy law in the United States is just over a hundred years old, and as Ken Gormley has put it,

the most distinctive characteristic of privacy—which can be gleaned from a hundred-year examination of the cases—is its heavy sensitivity to historical triggers. . . . [E]ach type of privacy . . . has been directly jolted into existence by transformations in American life and technology, which have created a societal mood powerful enough to incubate a new, legally protected right.⁴²⁹

From the very beginning, privacy law has been a piece-meal response to particularized interests and concerns, lurching about like a child playing blind man’s bluff.⁴³⁰ The advent of the Internet has changed the story completely, injecting a generalized interest in informational privacy into American society.⁴³¹

V. THE STATE CONSTITUTIONAL EXPERIMENT

The discussion has seemingly come to an impasse. A constitutional right to informational privacy is needed, yet this Article has shown that the

428. See Sunosky, *supra* note 52, at 84 (“the United States is reluctant to acknowledge that personal data privacy is a basic human right”).

429. Gormley, *supra* note 15, at 1439; see also Solove, *supra* note 2, at 1430 (“Privacy law is best described with the notion of the bricoleur—a person who uses whatever is at hand as a tool to solve problems”); Rotenberg, *supra* note 130, at 310 (“It is critical to understand that the recent history of privacy law in the United States is largely a story of efforts by Congress to pass laws to safeguard privacy as new technologies emerge”).

430. Warren and Brandeis’s foundational article, *The Right to Privacy*, was motivated by the development of the camera. See Warren & Brandeis, *supra* note 36. The Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (Supp. V 1999), arose from Judge Robert Bork’s Supreme Court confirmation hearings, during which reporters gained access to records of the Bork family video rentals. See Pippin, *supra* note 88, at 152-53. The Driver’s Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (Supp. V 1999), was a response to the murder of actress Rebecca Shafer, in which the murderer allegedly obtained the personal information used to stalk the victim from a state department of motor vehicles. See Pippin, *supra* note 88, at 153.

431. Indeed, much of the current concern is that if we continue to lack a concerted effort toward one solution for the Internet problem, “privacy fears will create so much unfocused pressure that an ‘incoherent body of law’ will result through ‘scattershot’ legislation.” Irving, *supra* note 5, at 676.

federal and state constitutional rights to informational privacy are weak. Clearly, one must advocate a change in constitutional doctrine, but where to begin?

All things being equal, a federal right would better address the interstate and international transactions that are central to the Internet. In fact, a strong federal right may not be as hopeless a pipe dream as it first seems. For instance, though the ultimate issue was not a constitutional one, the Supreme Court did positively address the *Whalen* “interest in avoiding disclosure” in *United States v. Reporters Committee for Freedom of the Press*.⁴³² The Court found that “the power of compilations to affect personal privacy . . . outstrips the combined power of the bits of information contained within.”⁴³³ This should provide “grounds for optimism with respect to informational privacy.”⁴³⁴ One commentator’s analysis is particularly lucid:

Previously, the court had resisted finding a privacy interest in records unless the records contained intimate, personal information, such as health or family information, and unless the records had been held in more or less strict confidence What the Court found in *Reporters Committee* is that there *is* an expectation of privacy in a computerized, comprehensive record of all of an individual’s activities—but not necessarily an expectation of privacy in a single criminal event.⁴³⁵

Other grounds for optimism arise from the concept of anonymity, a distant relative of, if not sometimes a synonym for, informational privacy.⁴³⁶ Anonymity advocates find protection for informational privacy in the First Amendment freedom to speak anonymously. The Supreme Court has held that there is a constitutional right to speak anonymously about political ideas,⁴³⁷ and one commentator has argued that this right, considered with other Court cases, can be construed as an argument for the right

432. 489 U.S. 749, 762 (1989) (quoting *Whalen v. Roe*, 429 U.S. 589, 598-600 (1977)). The issue in *Reporters Committee* was whether certain FBI “criminal rap sheets” should be disclosed under the FOIA. *See id.* at 757.

433. *Id.* at 765.

434. Flaherty, *supra* note 13, at 840.

435. Robert R. Belair, *Redefining Information Privacy*, PRIVACY J., July 1989, at 7.

436. *See* Kearns, *supra* note 13, at 979 (“Information privacy also is tied to the concept of anonymity but . . . is concerned with [one’s] personal information”).

437. *See* McIntyre v. Ohio Elections Comm’n, 514 U.S. 334 (1995).

PRIORITIZING PRIVACY

to read anonymously on the Internet.⁴³⁸ The Court has recently granted certiorari to a case involving the right to anonymously petition door-to-door.⁴³⁹

Even though these cross-doctrine tidings seem promising,⁴⁴⁰ the Supreme Court has not directly indicated a change in the federal constitutional right to informational privacy. In fact, David Flaherty, formerly Canada's privacy commissioner and an advocate of the U.S. Constitutional right to informational privacy, has noted, an "important qualification . . . is that the [U.S.] Supreme Court has never made a broad general finding of a constitutional right to privacy . . . nor has the Constitution been explicitly amended to this effect, nor is it on anyone's agenda, nor has it even been contemplated."⁴⁴¹

More importantly, all things are *not* equal. Several state constitutions have begun to extend the constitutional right of informational privacy to private action, whereas the federal constitution is firmly entrenched in the concept that constitutional rights apply only against state actors.⁴⁴² The Internet is shifting the primary problem of computer databases to private parties.⁴⁴³ A constitutional right that does not apply to private parties will be impotent as a baseline commitment to informational privacy.⁴⁴⁴

Thus, the states must serve as the breeding ground for an effective constitutional right to informational privacy. This is not a foreign concept. Rallying under Justice Brennan's banner,⁴⁴⁵ "[a]s the United States Supreme Court has restricted the scope of federal protection of civil liberties,

438. Helms cited *Lamont v. Postmaster General*, 381 U.S. 301 (1965), and *Stanley v. Georgia*, 394 U.S. 557 (1969), as evidence of one's right to read without state interference or oversight. See Helms, *supra* note 2, at 309.

439. See *Watchtower Bible & Tract Soc'y of New York, Inc. v. Village of Stratton*, 240 F.3d 553, *cert. granted*, 122 S. Ct. 392 (2001).

440. See Gindin, *supra* note 13, at 1185 (noting in 1997 that "it seems likely the Supreme Court will hold that the Constitution protects a right of informational privacy" because "some informational privacy protections can be found in the First and Fourth Amendments").

441. Flaherty, *supra* note 13, at 837.

442. See *supra* note 426 and accompanying text (discussing the "state action doctrine").

443. See *supra* note 427 and accompanying text.

444. At least one commentator has suggested expanding the federal constitutional right to private parties for exactly this reason. See Kearns, *supra* note 13, at 1006-09.

445. In 1977, Justice Brennan wrote a law review article praising state constitutions as protective instruments of individual rights. See generally William J. Brennan, Jr., *State Constitutions and the Protection of Individual Rights*, 90 HARV. L. REV. 489 (1977).

civil liberties advocates have turned a hopeful eye toward the states.”⁴⁴⁶ It is true that the state constitutional rights to informational privacy have also been generally weak, but a few leaders, such as New Jersey and California, provide rights that both are stronger than federal protection and exemplify the ultimate goal.⁴⁴⁷ New Jersey’s state constitution does not explicitly mention a right to privacy, but the state supreme court has protected information, even that which has become public.⁴⁴⁸ California has an explicit right to privacy that is grounded in a proper conception of informational privacy and has been extended to cover private actions.⁴⁴⁹ The proper conception of informational privacy is particularly important. As discussed *supra*, the U.S. Supreme Court appeared to rule unfavorably in *Whalen* because it misconstrued the concept of informational privacy.⁴⁵⁰ Equally unconvincing is the fact that other states, like Hawaii and Montana, are close behind California and New Jersey in pushing the envelope of constitutional protection for informational privacy.⁴⁵¹

Moreover, state constitutional rights have room to and will probably grow beyond the federal right. Ten states have constitutions that expressly provide for privacy and nearly all of these states have at some time or another relied on that clause to surpass the federal minimums.⁴⁵² And as with the U.S. Supreme Court, the state supreme courts exhibit a number of cross-doctrine tidings that should serve as grounds for optimism. Several states have recognized that their constitutional search and seizure rights exceed the protection provided by the Fourth Amendment.⁴⁵³ This is particularly relevant given how the Internet is merging surveillance and in-

446. Silverstein, *supra* note 271, at 215; *see also* *Katz v. United States*, 389 U.S. 347, 350-51 (1967) (“the protection of a person’s *general* right to privacy . . . is, like the protection of his property and of his very life, left largely to the law of the individual states”). For example, the Illinois delegates who implemented Illinois’s explicit right to privacy did so “[knowing] that state courts could interpret state constitutional provisions to afford higher standards of liberty than the minimums required by the federal constitution. . . . They believed that state constitutional guarantees formed a defense against the possible constriction of federal protections.” Silverstein, *supra* note 271, at 287.

447. *But see* Kang, *supra* note 19, at 1231 n.158 (comparing California’s constitutional right of informational privacy to the common law tort of invasion).

448. *See* discussion *supra* Part II.B.9.

449. *See* discussion *supra* Part II.B.3.

450. *See supra* note 56; *see also supra* note 268 and accompanying text.

451. *See* discussion *supra* Parts II.B.5 and II.B.8.

452. Silverstein, *supra* note 271, at 227.

453. *See, e.g.,* *State v. Bolt*, 689 P.2d 519 (Ariz. 1984); *State v. Koppel*, 499 A.2d 977 (N.H. 1985); *In re Shon Daniel K.*, 959 P.2d 553 (N.M. 1998); *State v. Mills*, 411 S.E.2d 193 (N.C. 1991); *Commonwealth v. Sell*, 470 A.2d 457b (Pa. 1983); *State v. Welch*, 624 A.2d 1105 (Vt. 1992); *State v. Cleator*, 857 P.2d 306 (Wash. Ct. App. 1993).

PRIORITIZING PRIVACY

formational technologies.⁴⁵⁴ The following examples bode well for informational privacy. Washington and Vermont have rejected the “reasonable expectation of privacy” standard⁴⁵⁵ that often hinders protection against pervasive technologies.⁴⁵⁶ Alaska, Massachusetts, Pennsylvania, and Vermont have disagreed with *United States v. White*,⁴⁵⁷ finding to some degree that one-party consent to monitoring conversations requires a warrant.⁴⁵⁸ Pennsylvania, Idaho, and Hawaii require a warrant for the use of pen registers under all circumstances,⁴⁵⁹ contrary to the Court in *Smith v. Maryland*.⁴⁶⁰ Finally, Colorado has found an expectation of privacy in toll records,⁴⁶¹ and Pennsylvania has held that caller ID violates state privacy rights.⁴⁶² In Ken Gormley’s words, “All of the above cases confirm that one of the significant features of privacy in the next few decades will be that new technology and evolving social conditions will push more and more cutting-edge issues into the states.”⁴⁶³

Recognizing that federal constitutional protection may be more effective,⁴⁶⁴ it is important to see the pursuit of a state constitutional right to informational privacy as merely one step in a larger scheme. Hopefully,

454. For a discussion of how the convergence of surveillance and informational privacy concerns warrants a stronger constitutional right to informational privacy, see generally Kearns, *supra* note 13.

455. *See* *State v. Kirchoff*, 587 A.2d 988 (Vt. 1991); *State v. Myrick*, 688 P.2d 151 (Wash. 1984). Silverstein notes that in *State v. Myrick* the Washington Supreme Court argued that “the scope of constitutional protections should not diminish just because government conduct or technological developments diminish the degree of privacy that citizens actually expect.” Silverstein, *supra* note 271, at 250-51.

456. Froomkin, *supra* note 9, at 1510 (“expectations are notoriously unstable: The more widely a technology is deployed and used, the less reasonable the expectation not to be subjected to it”).

457. 401 U.S. 745 (1971).

458. *See* *State v. Glass*, 583 P.2d 872 (Alaska 1978); *Commonwealth v. Blood*, 507 N.E.2d 1029 (Mass. 1987); *Commonwealth v. Brion*, 652 A.2d 287 (Pa. 1994); *State v. Blow*, 602 A.2d 552 (Vt. 1991).

459. *See* *State v. Rothman*, 779 P.2d 1 (Haw. 1989); *State v. Thompson*, 760 P.2d 1162 (Idaho 1988); *Commonwealth v. Melilli*, 555 A.2d 1254 (Pa. 1989).

460. 442 U.S. 735 (1979).

461. *See* *People v. Corr*, 682 P.2d 20 (Colo. 1984).

462. *See* *Barasch v. Pa. Public Utility Comm’n*, 576 A.2d 79 (Pa. 1990).

463. Gormley, *supra* note 15, at 1431.

464. *See* Kearns, *supra* note 13, at 1009 n.183 (noting the problems with a multitude of state protections); *see also* Jennifer DiGiovanni, *Justice Charles M. Leibson and the Revival of State Constitutional Law: A Microcosm of a Movement*, 86 KY. L.J. 1009, 1017 (1997) (“state constitutionalism is fundamentally incompatible with the perception of most Americans that they are national citizens”). Robust state constitutionalism could be dangerous, “resulting in the sort of factionalism that led to the great schism that caused the Civil War.” *Id.* at 1017-18.

the state constitutional schemes, once developed, will carry over into the federal regime.⁴⁶⁵ The states may help this “reverse incorporation” if they move toward the definition of informational privacy adopted by this Article and the California courts.⁴⁶⁶ In the meantime, the need for constitutional redress to the Internet’s threats to informational privacy demands the unique pace and ability of the states in experimenting with, expanding, and adopting new rights.⁴⁶⁷ “[S]tates serving as the constitutional laboratories . . . will most likely secure privacy’s survival and expansion deep into the next century.”⁴⁶⁸

VI. CONCLUSION

The Internet poses a severe threat to informational privacy. The rules, however, have changed more than most have acknowledged. Informational privacy, rather than an interest primarily in avoiding disclosure, is a concern with the real and perceived consequences of disclosure. The Internet, as the most extensive computer database ever in existence, has done more than pose a threat to this form of privacy. By creeping into the lives of all but the most radical techno-phobes, the Internet has elevated informational privacy to a generalized concern. The current legal regime is impotent; in its place, a commitment to informational privacy must be made on a constitutional scale. Only then will the legal landscape have both the sufficient foundation and flexibility to protect a generalized interest in informational privacy.

The constitutional right to informational privacy, however, remains weak at both the federal and state levels. The leading U.S. Supreme Court

465. See Gormley, *supra* note 15, at 1422 (“More importantly, [state rights] ha[ve] served as an experimentation ground for new, untested types of privacy . . . which in turn have had a profound impact on federal pronouncements on privacy law”).

466. Recall that the conception of informational privacy adopted by this Article and by the California courts differs from the conception embraced by the U.S. Supreme Court. This Article’s definition does not sharply distinguish between informational privacy and privacy-as-autonomy-in-decisionmaking. *Cf.* Whalen v. Roe, 429 U.S. 589, 599 (1977) (identifying “two different kinds” of privacy interests, where “[o]ne is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions”). Because the privacy-as-autonomy-in-decisionmaking theory of privacy has been somewhat blessed by the Court, *see* Griswold v. Connecticut, 381 U.S. 479 (1965); Roe v. Wade, 410 U.S. 113 (1973), this Article’s conception of informational privacy could make more headway in federal courts.

467. See Gormley, *supra* note 15, at 1431 (noting that privacy rights “will be experimented with and refined under state constitutions with far greater frequency”).

468. *Id.*

PRIORITIZING PRIVACY

case, *Whalen v. Roe*, appears to have established no more than a constitutional interest in informational privacy. Moreover, whatever federal constitutional right exists applies only to state actors. Whereas the problem of the Internet is increasingly one of private databases. The state courts appear to have squandered their potential to raise the constitutional bar above federal minimums. Though nine of the ten states with explicit rights to privacy have recognized some constitutional right to informational privacy, many are weak. Furthermore, only two of those nine states apply the right to private parties. Of the forty states without an express provision for privacy, only New Jersey appears to have developed an implied right to informational privacy worth mentioning.

A constitutional commitment, then, must be initiated in either the federal or state regimes. Due to the unique trans-boundary nature of the Internet, a federal right is preferable. For the moment, however, both schemes are weak and it is the state constitutional system that offers greater promise in the short term. A few of the states already have noteworthy constitutional rights to informational privacy, and California, arguably the forerunner in the pack, grounds its right in a conception of informational privacy that closely mirrors the definition espoused by this Article. Moreover, the states are traditionally fertile grounds for constitutional experimentation. One should therefore seek to strengthen the constitutional right to informational privacy in the states. The ultimate goal, however, would not be to implement fifty disparate schemes, but to carry over such changes to the federal landscape.

We no longer live in an information *age*, an era that will come to a certain conclusion. With the proliferation of the Internet, the digital revolution has become our everyday digital reality. The transformation of information into a currency and a gatekey is on a steady crescendo. As a result, privacy in information has become a permanent priority. To that, we must deliver a constitutional response.