Mainstreaming Privacy Torts

Danielle Keats Citron

No. 2010 - 16

UNIVERSITY of MARYLAND SCHOOL of LAW

Mainstreaming Privacy Torts

Danielle Keats Citron†

In 1890, Samuel Warren and Louis Brandeis proposed a privacy tort and seventy years later, William Prosser conceived it as four wrongs. In both eras, privacy invasions primarily caused psychic and reputational wounds of a particular sort. Courts insisted upon significant proof due to those injuries' alleged ethereal nature. Digital networks alter this calculus by exacerbating the injuries inflicted. Because humiliating personal information posted online has no expiration date, neither does individual suffering. Leaking databases of personal information and postings encouraging assaults invade privacy in ways that exact significant financial and physical harm. It would be nearly impossible now to argue that these injuries are mere trivialities.

Unfortunately, privacy tort law is ill-equipped to address these changes. Prosser built the modern privacy torts based on precedent and a desire to redress harm. Although Prosser's approach succeeded in the courts because it blended theory and practice, it conceptually narrowed the interest that privacy tort law sought to protect. Whereas Warren and Brandeis conceived privacy tort law as protecting a person's right to develop his personality free from unwanted publicity and unwanted access by others, Prosser saw it as addressing specific emotional, reputational, and proprietary injuries caused by four kinds of activities prevalent in the twentieth century.

---

† Professor of Law, University of Maryland School of Law. I owe special thanks to Don Gifford, Richard Boldt, Deborah Hellman, and David Super for their insights on multiple drafts. I am grateful to Randy Bezanson, Joshua Blackman, Susan Freiwald, Amy Gajda, Mark Graber, David Gray, Oscar Gray, Leslie Meltzer Henry, Helen Norton, Nik Peifer, Amanda Pustilnik, Neil Richards, Rob Rhee, Paul Schwartz, Jana Singer, Dan Solove, Max Stearns, Lior Strahilevitz, Eugene Volokh, Greg Young, and the participants at the "Prosser's *Privacy* at 50" symposium at the University of California Berkeley Law School and the University of Maryland School of Law's legal theory faculty workshop for their thoughtful suggestions. Adam Farra, Dan Federline, Alice Johnson, Dave Martin, Susan McCarty, and Kaveh Saba did excellent research. Dean Phoebe Haddon of the University of Maryland School of Law generously supported this research. Lily Schroeder, Jordan Bergsten, and the editors of the *California Law Review* kindly provided expert guidance and feedback.

Since then, courts have too often rigidly interpreted the four privacy torts. Prosser's conceptualization of privacy interests worth protecting is too narrow to accommodate the privacy interests implicated by networked technologies. As a result, the privacy torts often cannot properly redress contemporary privacy injuries.

A potential solution lies in taking the best of what Prosser had to offer—his method of borrowing from doctrine and focusing on injury prevention and remedy—while ensuring that proposed solutions are transitional and dynamic. Any updates to privacy tort law should protect the broader set of interests identified by Warren and Brandeis, notably a person's right to be free from unwanted intrusions and disclosures of personal information. While leaking databases and certain online postings compromise that interest, courts could invoke long-standing tort remedies to address these wrongs, rather than conceiving new, potentially unattainable, privacy torts. To that end, courts could employ mainstream tort doctrines rather than creating new privacy torts. They might also consider the ways that the internet magnifies privacy harms in assessing privacy claims to ensure law's recognition of them.

INTRODUCTION

Privacy tort law is a product of prior centuries' hazards. In the late nineteenth century, snap cameras and recording devices provided a cheap way to capture others' private moments without detection.[1] The penny press profited from the publication of revealing photographs and gossip about people's personal lives.[2]

Two scholars of the late nineteenth century, Samuel Warren and Louis Brandeis, responded by calling for tort law to protect individuals' "right to be let alone."[3] According to them, a privacy tort would secure for each person the right to determine "to what extent his thoughts, sentiments, and emotions shall be communicated to others."[4] In other words, it would permit individuals to decide "whether that which is [theirs] shall be given to the public."[5] In their view, the privacy tort protected individuals' ability to decide how much personal information is revealed to others and, in this way, to develop their "inviolate personality" without interference.[6] Daniel Solove has characterized Warren and Brandeis's "right to be let alone" as "view[ing] privacy as a type of immunity or seclusion."[7]

Courts gradually recognized tort claims based on Warren and Brandeis's "right to privacy" formulation.[8] In early cases, the privacy tort protected against a filmmaker's release of a movie documenting a woman's operation[9] and a landlord's placement of a hidden camera in a couple's bedroom.[10] It remedied a newspaper's revelation of a woman's humiliating disease[11] and the publication

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 194 (1890).

2. *Id.* at 196.

3. *Id.* at 193.

4. *Id.* at 198.

5. *Id.* at 199; *see* Amy Gajda, *Judging Journalism: The Turn Toward Privacy and Judicial Regulation of the Press*, 97 CALIF. L. REV. 1039, 1045–48 (2009) (discussing the "legally protected interest" arising from Warren and Brandeis's *The Right to Privacy* as people's need to be free from unwanted publicity and unwanted invasions from yellow journalists and gossip mongers).

6. Warren & Brandeis, *supra* note 1, at 198.

7. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1101 (2002) [hereinafter Solove, *Conceptualizing Privacy*]. Solove explained that Warren and Brandeis did not intend to provide a comprehensive theory of privacy. *Id.* Instead, they simply wanted to "explore the roots of a right to privacy in the common law and explain how such a right could develop." *Id.*

8. W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 117 (5th ed. 1984) [hereinafter PROSSER & KEETON] (explaining that privacy torts are an outstanding illustration of the influence of legal periodicals on the courts); William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 422 (1960); *see, e.g.*, Mau v. Rio Grande Oil, Inc., 28 F. Supp. 845, 846 (N.D. Cal. 1939) (attributing California and southern states' recognition of privacy torts to Warren and Brandeis's "right to be let alone" formulation in the *Harvard Law Review*).

9. Feeney v. Young, 181 N.Y.S. 481 (App. Div. 1920).

10. Hamberger v. Eastman, 206 A.2d 239 (N.H. 1964).

11. Barber v. Time, Inc., 159 S.W.2d 291 (Mo. 1942) (involving the publication of the name and picture of a woman with an eating disorder in her hospital room).

of nude pictures taken by the police.[12] It also redressed an insurance company's unauthorized use of someone's image in its advertising campaign.[13]

These twentieth-century privacy intrusions inflicted injuries of a particular sort. They harmed individuals' "peace of mind," causing humiliation and mental distress.[14] They tainted people's images in the community, resulting in lost jobs and businesses.[15] And they undermined people's ability to control their public persona.[16] In Warren and Brandeis's estimation, privacy intrusions produced "mental pain and distress, far greater than could be inflicted by mere bodily injury."[17]

Yet, because those privacy invasions involved twentieth-century technologies, revelations of embarrassing personal information and intrusions into private spheres were often temporary. Films, for example, appeared in theaters for a limited time and although they might have been archived for future viewing, only a small number of people likely viewed them. Newspapers remained in circulation for only a few days and then lingered in little-seen library files.

Although twenty-first century technologies can similarly interfere with individual privacy, they magnify the harm suffered. The searchable, permanent nature of the internet extends the life and audience of privacy disclosures, and exacerbates individuals' emotional and reputational injuries. For instance, if pictures and videos of a young girl's sexual abuse are posted online, they may remain there indefinitely, ensuring that the victim remains haunted by the abuse as an adult.[18] Likewise, individuals' creditworthiness and employability can be seriously compromised when businesses fail to secure databases of personal information from identity thieves.[19] Further, people can suffer physical harm after website operators host postings that encourage third parties to assault individuals.[20]

---

12. York v. Story, 324 F.2d 450 (9th Cir. 1963), *cert. denied*, 376 U.S. 939 (1964); *see also* Trammell v. Citizen's News Co., Inc. 148 S.W.2d 708 (Ky. 1941) (involving the publication of a person's debt).

13. Pavesich v. New England Life Ins. Co., 50 S.E. 68, 69–70 (Ga. 1905).

14. *Id.* at 197; *see, e.g.*, Housh v. Peth, 133 N.E.2d 340, 343 (Ohio 1956).

15. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 175 (2008) [hereinafter SOLOVE, UNDERSTANDING PRIVACY].

16. These intrusions also lowered social standards, perverting and belittling discourse. Warren & Brandeis, *supra* note 1, at 196.

17. Warren & Brandeis, *supra* note 1, at 196.

18. *See* John Schwartz, *Child Pornography, and an Issue of Restitution*, N.Y. TIMES, Feb. 3, 2010, http://www.nytimes.com/2010/02/03/us/03offender.html.

19. Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CALIF. L. REV. 241, 251–53 (2007) [hereinafter Citron, *Reservoirs of Danger*].

20. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 100 (2007) [hereinafter SOLOVE, FUTURE OF REPUTATION]; Ben Neary, *Internet Rape Case Jolts Wyoming City*, ABC NEWS, Feb. 6, 2010, http://abcnews.go.com/US/wireStory?id=9766537.

Unfortunately, privacy tort law is ill-suited to address these changes. William Prosser reshaped tort law's protection of the "right to privacy" as the Reporter for the *Second Restatement on Torts* in the 1950s, and the privacy tort framework has not been modified to address the modern challenges arising since that time.[21] Prosser created a privacy taxonomy based on his twin interests in doctrine and policymaking. For Prosser, privacy tort law protected against emotional, reputational, and proprietary injuries caused by (1) public disclosure of private facts, (2) intrusion on seclusion, (3) depiction of another in a false light, and (4) appropriation of another's image for commercial gain.[22]

Although Prosser's privacy taxonomy tackled privacy injuries caused by twentieth-century technologies, it may not be dynamic enough to address privacy injuries produced by digital networks. This is partially attributable to the taxonomy's narrow articulation of the interests that privacy tort law protected. Whereas Warren and Brandeis saw privacy tort law as broadly protecting the right to develop one's personality free from unwanted access and exposure, Prosser conceived it as narrowly addressing the emotional, reputational, and proprietary harm produced by the four privacy-threatening activities prevalent in his time. Then, too, courts have rigidly applied Prosser's taxonomy, perhaps because of their skepticism about "psychic wounds."[23] This has left many of today's privacy injuries—exacerbated by modern technologies—without privacy tort solutions.

Consider today's databases that leak personal information to criminals, as well as certain online postings of personal information. When insecure databases release individuals' Social Security numbers to identity thieves, they interfere with those individuals' interest in keeping their sensitive personal information from others. Likewise, website operators who reveal individuals' home addresses, along with instructions for viewers to assault them, deprive those individuals of their right to be "let alone." These operators invade people's anonymity, exposing them to being watched, followed, and attacked by assailants. Although these practices impinge upon individuals' privacy, the four privacy torts fail to address them.

Even in cases covered by Prosser's four privacy torts, courts may deny recovery, despite plaintiffs' significant suffering. To prevent privacy plaintiffs from recovering for trivialities, courts have erected a number of substantial barriers to recovery.[24] Thus, plaintiffs often must prove that the defendant

21. G. EDWARD WHITE, TORT LAW IN AMERICA: AN INTELLECTUAL HISTORY 176 (2003).

22. Prosser, *supra* note 8, at 422–23.

23. From the start, courts took a skeptical view of privacy tort claims because they responded to intangible injuries that were difficult to measure. WHITE, *supra* note 21, at 176; *cf.* Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 393 (2009) [hereinafter Citron, *Law's Expressive Value*] (explaining that nineteenth-century tort law discounted women's suffering by refusing to recognize claims mainly pursued by women, such as those for emotional distress).

24. Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW

intended to invade another's privacy,[25] that the defendant's conduct was "highly offensive to the reasonable person," and that the information was sufficiently private.[26]

In the past, embarrassing disclosures of private facts might have fallen short of a privacy tort's "highly offensive to the reasonable person" standard on the grounds that the harm was minor. Although a newspaper's publication of a person's private information might have been embarrassing or unflattering, it might not have been sufficiently offensive because it did not concern the sensational or morbid and because memories would surely fade.[27] In the present, however, private facts posted online persist indefinitely, ever searchable by prospective clients, employers, and friends. This compounds the emotional and reputational harm that individuals suffer, dispelling prior eras' concerns that privacy plaintiffs would recover for trivialities—a concern which may have contributed to the rigidity of Prosser's narrow framework.

In this Article, I argue that privacy tort law should be updated to tackle the information age's privacy injuries. This piece unfolds in three Parts. Part I highlights how twenty-first century technologies magnify privacy injuries. Part II traces privacy tort law's development, exploring Warren and Brandeis's conception of privacy torts' legally protected interest and Prosser's more limited approach. It also explores how Prosser's combination of theory and practice made privacy taxonomy so successful, and yet so rooted in another time. Finally, it discusses privacy tort law's inability to prevent and deter privacy injuries caused by networked technologies.

Part III suggests strategies for ensuring the prevention and remedy of contemporary privacy injuries. It considers taking the best of what the privacy tort's intellectual forefathers had to offer while ensuring that it can adapt to changing technologies. It grapples with ways that courts could enrich Prosser's conception of the interests protected by privacy tort law with those identified by Warren and Brandeis. In that sense, it considers ways that we can return to the principles laid out in *The Right to Privacy* in order to move forward.

Part III then argues that, rather than inventing new privacy torts, privacy tort law could invoke mainstream tort doctrines to remedy invasions of individuals' right to be "let alone." As Prosser knew and mined with great success, tort innovations can have a greater chance of adoption if they derive from established law. Part III also discusses ways to ensure that the modern

---

& CONTEMP. PROBS. 326, 328 (1966). Of mental distress damages generally, Calvin Magruder wrote: "Against a large part of the frictions and irritations and clashing of temperaments incident to participation in a community life, a certain toughening of the mental hide is a better protection than the law could ever be." Calvin Magruder, *Mental and Emotional Disturbance in the Law of Torts*, 49 HARV. L. REV. 1033, 1035 (1936).

25. *See, e.g.*, McCormick v. Haley, 307 N.E.2d 34, 38 (Ohio Ct. App. 1973).

26. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

27. *See, e.g.*, Virgil v. Sports Illustrated, 424 F. Supp. 1286 (S.D. Cal. 1976).

privacy torts can tackle emotional and reputational harm caused by damaging information posted online.

I.
THE CHANGING FACE OF PRIVACY INJURIES

This Part explores how twenty-first century technologies intensify privacy harm. It discusses how digital networks exacerbate the damage inflicted upon people's psyche and reputations. It also surveys the extensive economic and physical injuries resulting from today's privacy invasions.

A. Mental and Reputational Injuries Intensified

During the nineteenth century and the better part of the twentieth, privacy intrusions often inflicted psychic and reputational harm.[28] Privacy intrusions interfered with a person's "sentiments, thoughts and feelings,"[29] producing discomfort and irritation.[30] For instance, in *Housh v. Peth*,[31] a creditor repeatedly called a debtor at work and at home late at night demanding payment.[32] The plaintiff testified that the calls caused her "nervousness, worry, humiliation, mental anguish and loss of sleep."[33] The court determined that the defendant's malicious, systematic harassment invaded the plaintiff's right to privacy.[34] Similarly, a court awarded damages for a couple's mental suffering after a photographer published a photograph of their deceased conjoined twins.[35] It reasoned that "expos[ing] . . . to public view" the corpse of a child invaded "[t]he most tender affections of the human heart."[36]

Feelings of shame regularly accompanied individuals' mental distress. A husband and wife attested to their humiliation after discovering that their landlord placed a recording device in their bedroom to listen to their conversations and sounds.[37] The husband explained that he could not perform

28. WHITE, *supra* note 21, at 234.

29. Flores v. Mosler Safe Co., 164 N.E.2d 853, 855 (N.Y. 1959).

30. Sheldon W. Halpern, *The Right of Publicity: Commercial Exploitation of Associative Value of Personality*, 39 VAND. L. REV. 1199, 1205 (1986).

31. 133 N.E.2d 340, 341 (Ohio 1956).

32. *Id.* at 340.

33. *Id.*

34. *Id.* at 344.

35. Douglas v. Stokes, 149 S.W. 849, 850 (Ky. 1912).

36. *Id.*

37. Hamberger v. Eastman, 206 A.2d 239 (N.H. 1964). In another case, a woman experienced self-consciousness and embarrassment after a newspaper published a picture of her after the wind blew up her skirt at an amusement park. Daily Times Democrat v. Graham, 162 So. 2d 474, 476 (Ala. 1964); *see also* Gonzales v. Sw. Bell Tel. Co., 555 S.W.2d 219, 222–23 (Tex. Civ. App. 1977) (upholding a privacy claim in a case where a telephone company's intrusion on the plaintiffs' home to reclaim phones inflicted significant emotional harm, including the wife's stomach pains and nervousness).

his normal duties as a father and husband.[38] According to the wife, the experience "curtailed" their sex life.[39]

In some cases, these feelings had a crippling effect on individuals. In one instance, a plastic surgeon televised a before-and-after picture of a patient's face-lift without her consent.[40] The patient explained that when she learned of the disclosure she was "devastated" and "'felt terrible' that everyone at her former office knew about her face-lift."[41] Ultimately, she refused to go out in public.[42]

The publication of embarrassing information or use of a person's image in an advertisement produced reputational harm as well. For instance, in *Melvin v. Reid*,[43] the defendant made a movie about the plaintiff's years as a prostitute and her involvement in a murder trial.[44] There, the plaintiff's disclosed behavior occurred many years before the defendant made the film; when the defendant released the picture, the plaintiff had been living a conventional life.[45] The plaintiff brought a privacy suit, alleging that the film exposed her to public contempt, ridicule, and scorn.[46] She contended that the movie undermined her hard-won respectability and good name.[47] The court upheld the plaintiff's privacy claim, finding that she had a right to pursue safety and happiness without such publicity.[48]

---

38. *Eastman*, 206 A.2d at 242.

39. FREDERICK S. LANE, AMERICAN PRIVACY: A 400-YEAR HISTORY OF OUR MOST CONTESTED RIGHT 144 (2009). The court found that the landlord's use of a peeping Tom device raised a valid invasion of privacy claim. *Eastman*, 206 A.2d at 242. As Frederick Lane notes, however, on remand, the jury sided with the landlord, seemingly accepting his explanation that he did not install the device for "vicarious thrills" but instead to monitor the operation of a pump in the plaintiffs' basement. LANE, *supra*, at 144.

40. Vassiliades v. Garfinckel's, 492 A.2d 580, 586 (D.C. 1985).

41. *Id.*

42. *Id.* The court upheld the patient's "'right of private personality and emotional security.'" *Id.* at 587 (quoting Afro-Am. Publ'g Co. v. Jaffe, 366 F.2d 649, 653 (D.C. Cir. 1966)). Similarly, after a magazine used a woman's picture to promote a story about sexual antics, the woman testified that she was so upset that she "felt like crawling in a hole and never coming out" and dreaded going back to work. Braun v. Flynt, 726 F.2d 245, 248 (5th Cir. 1984).

43. 297 P. 91 (Cal. Dist. Ct. App. 1931).

44. *Id.* at 91.

45. *Id.* Historian Lawrence Friedman provides fascinating insights about the *Melvin* case. LAWRENCE M. FRIEDMAN, GUARDING LIFE'S DARK SECRETS: LEGAL AND SOCIAL CONTROLS OVER REPUTATION, PROPRIETY, AND PRIVACY 216–19 (2007). He contends that the woman had not truly resurrected herself as she claimed. *Id.* at 218. Friedman explains: "There is good evidence that she was, in fact, as phony as a three dollar bill. A journalist in Arizona argues that she was still working as a prostitute and a madam" and that "[d]uring her lifetime she had several husbands, but they had the distressing habit of turning up dead." *Id.* at 218. For an insightful review of Lawrence Friedman's book, see Neil M. Richards, *Privacy and the Limits of History*, 21 YALE J.L. & HUMAN. 165 (2009) (reviewing FRIEDMAN, *supra*).

46. *Reid*, 297 P. at 91.

47. FRIEDMAN, *supra* note 45, at 217.

48. *Id.* at 291. Similarly, a court upheld a privacy claim against a creditor who publicized the plaintiff's debt because it undermined the plaintiff's reputation in the community. Trammell v. Citizens News Co., 148 S.W.2d 708 (Ky. 1941).

These types of emotional and reputational harms are alive and well today, and they are, in many ways, far worse.[49] While public disclosures of the past were more easily forgotten, memory decay has largely disappeared.[50] Because search engines reproduce information cached online, people cannot depend upon time's passage to alleviate reputational and emotional damage.[51] Unlike newspapers, which were once only easily accessible in libraries after their publication, search engines now index all content on the web, and can produce it instantaneously. The Internet thus ensures that damaging personal information is not forgotten, evoking a Nietzschean image of persistent memory:

> What if some day or night a demon were to steal into your loneliest loneliness and say to you: 'This life as you now live it and have lived it you will have to live once again and innumerable times again;' . . . . Would you not throw yourself down and gnash your teeth and curse the demon who spoke thus?[52]

The Internet guarantees a Nietzschean "eternal return" of damaging disclosures.[53]

Consider these examples. A stalker spied on sports reporter Erin Andrews at a hotel, secretly taping her while she undressed in her hotel room.[54] He posted over ten videos of her online.[55] Google Trends data suggested that just after the release of the videos, much of the nation began looking for some variation on "Erin Andrews peephole video."[56] Nearly nine months later, Ms. Andrews explained: "'I haven't stopped being victimized—I'm going to have to live with this forever. . . . When I have kids and they have kids, I'll have to explain to them why this is on the Internet.'"[57] She further lamented that when she walks into football stadiums to report on a game, she faces the taunts of fans who have seen her naked online.[58] She explained that she "'felt like [she]

---

49. SOLOVE, THE FUTURE OF REPUTATION, *supra* note 20.

50. VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 9 (2009).

51. SOLOVE, THE FUTURE OF REPUTATION, *supra* note 20, at 74.

52. FRIEDRICH NIETZSCHE, THE GAY SCIENCE 194 (Bernard Williams ed., Josefine Nauckoff trans., Cambridge Univ. Press 2001) (1887); *see* MILAN KUNDERA, THE UNBEARABLE LIGHTNESS OF BEING 5 (Michael Henry Heim trans., 1984) ("In the world of eternal return the weight of unbearable responsibility lies heavy in every move we make.").

53. Friedrich Nietzsche wrote of the concept of eternal return, which posits that the universe has been recurring, and will continue to recur as we once experienced it, an infinite number of times. NIETZSCHE, *supra* note 52, at 341.

54. Leslie Casimir, *The ESPN Girl Takes a Stand*, GLAMOUR, Apr. 2010, at 161.

55. Lynn Lamanivong, *Erin Andrews' Video Voyeur Gets 2½* Years, CNN, Mar. 15, 2010, http://www.conn.com/2010/CRIME/03/15/espn.erin.andrews.sentence/index.html.

56. Steve Johnson, *Erin Andrews Nude Video Coverage Full of Hypocrisy*, CHI. TRIB., July 23, 2009, http://www.chicagotribune.com/features/yearinreview/chi-0723-espn-andrewsjul23,0,3410514.column.

57. Casimir, *supra* note 54, at 162.

58. *Id.*

was continuing to be victimized'" each time she talked about it.[59]

When a woman named Amy was four years old, her uncle videotaped his rape of her.[60] Although Amy's uncle was arrested and jailed when Amy was nine, causing the sexual abuse to stop, the photographs and videos of the sexual abuse had already been circulated on the Internet.[61] Those images are now the most widely distributed child pornography of all time.[62] Amy, who is now twenty years old, testified that: "'[e]very day of my life, I live in constant fear that someone will see my pictures, recognize me and that I will be humiliated all over again.'"[63]

These cases exemplify the permanent emotional and reputational damage that online disclosures can produce. Targeted individuals suffer anxiety and shame every time they see the postings and learn that others have seen them. For instance, the searchable, permanent nature of the Internet ensures that Amy must grapple with the pain of her sexual abuse more than ten years after it occurred. And employers may not want to get involved with people such as Ms. Andrews, who come with publicized baggage.[64]

In short, individuals now must live with digital records of their lives that are deeply humiliating and reputation-harming, as well as searchable and accessible from anywhere, and by anyone, in the world.[65] Often, the information is taken out of context, producing a distorted and damaging view of the person. Daniel Solove calls these privacy-invading online disclosures "digital scarlet letters."[66]

B. Financial Injuries Multiplied

In the past, privacy invasions cost people work and clients. For instance, the disclosure of a person's debts may have resulted in an employer's refusal to hire him or a potential client's decision to work with another person. While this, of course, remains true today, such individuals now suffer other kinds of financial injuries as well. Following are examples of the broadening scope of financial injuries faced by victims of privacy invasion.

Business entities, government agencies, and other actors collect massive databases of sensitive personal information, such as Social Security numbers (SSNs), biometric images, and medical data, to identify employees, facilitate

59. Michael Y. Park, *Erin Andrews Calls Peeping-Tom Video a 'Nightmare'*, PEOPLE, Sept. 1, 2009, http://www.people.com/people/article/0,,20301731,00.html.

60. Susan Donaldson James, *'Misty Series' Haunts Girl Long After Rape*, ABC NEWS, Feb. 8, 2010, http://abcnews.go.com/print?id=9773590.

61. *Id.*

62. *Id.*

63. *Id.*

64. Citron, *Law's Expressive Value*, *supra* note 23, at 397.

65. SOLOVE, THE FUTURE OF REPUTATION, *supra* note 20, at 76.

66. *Id.*

instant credit, report payroll taxes, and administer health care.[67] Because databases of sensitive personal information are treasure troves for criminals, data-security breaches are increasingly prevalent.[68] Malicious computer hackers, corrupt insiders, and careless employees cause the data leaks that make these breaches possible.[69] Accordingly, from 2005 to 2009, over 341 million records of sensitive personal information were involved in security breaches in the United States.[70]

Data leaks lead to identity theft and fraud, which cause a host of problems for their victims. Identity thieves use SSNs and biometric data to empty bank accounts, exhaust others' credit card limits, secure loans, and flip property.[71] Such thieves can destroy people's credit, precluding their ability to borrow money.[72] Other identity thieves use stolen health insurance information to obtain health care, leaving individuals with hefty hospital bills and someone else's treatment records.[73] Identity theft can undermine individuals' ability to obtain employment, because employers assess individuals' credit reports in making hiring decisions.[74] Some individuals can repair their credit reports, but only after spending, on average, over $5,720.[75] Others, however, may lack the knowledge and means to repair their credit reports. They may be unable to take out loans and get insurance, and might even face financial ruin.

The mere prevalence of identity theft today causes people to incur financial costs even without experiencing identity theft. They expend time and money to monitor their credit, distracting them from their jobs to their financial detriment.[76] Individuals pay for identity theft insurance, which, nonetheless,

67. Citron, *Reservoirs of Danger*, *supra* note 19.

68. *Id.* at 251.

69. *Id.* at 248.

70. *A Chronology of Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/ar/ChronDataBreaches.htm#2009 (last updated Oct. 18, 2010).

71. John Leland & Tom Zeller Jr., *Technology and Easy Credit Give Identity Thieves an Edge*, N.Y. TIMES, May 30, 2006, http://www.nytimes.com/2006/05/30/us/30identity.html.

72. According to a Javelin Strategy & Research study, the incidence of identity theft jumped sharply in 2008, up 22% from the prior year. Over 9.9 million people fell victim to criminals who used their identifying information to impersonate them for financial gain. Danielle Citron, *Thinking Hard About the Privacy Risks of E-Health Records Systems*, CONCURRING OPINIONS (Feb. 9, 2009, 9:37 EST), http://www.concurringopinions.com/archives/2009/02/thinking_hard_a.html.

73. Margaret Collins, *Stealing Your Identity for Liposuction*, BUSINESS WEEK, at 60, Apr. 19, 2010; *see also* ANITA L. ALLEN, WHY PRIVACY ISN'T EVERYTHING: FEMINIST REFLECTIONS ON PERSONAL ACCOUNTABILITY 117 (2003).

74. Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information* 9 (GWU Law School Public Law Research, Paper No. 102, 2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=583483.

75. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 78 (2009); Daniel B. Prieto, *Data Mine: Stopping Identity Theft*, NEW REPUBLIC, Dec. 19, 2005, at 17.

76. Citron, *Reservoirs of Danger*, *supra* note 19, at 253.

often fails to reimburse the full costs if identity theft arises.[77]

Website operators have also raised individuals' risk of identity theft by posting SSNs online for thieves to use. In *City of Kirkland v. Sheehan*,[78] operators of a website critical of law enforcement personnel listed the SSNs of officers on their site.[79] In enforcing the plaintiffs' privacy claim, the court explained that SSNs allow others to "control, manipulate, or alter other personal information."[80]

Financial harms can even arise from more benign uses of digital information. Information brokers amass digital dossiers on individuals that include incomplete and misleading data, selling them to potential employers and costing individuals jobs.[81] In most instances, these individuals have no idea that such digital dossiers have cost them work opportunities.[82] Individuals featured therein also cannot force data brokers to disclose or correct those dossiers.

These financial injuries have much in common with economic harm long redressed under other branches of tort law. For example, when defendants misrepresent information related to business deals, plaintiffs can recover for economic harm caused by the defendant's lies.[83] Likewise, plaintiffs can recover for financial losses when defendants intentionally or negligently interfere with individuals' prospective or current business relationships.[84] The financial injuries caused by misrepresentation and interference with business relations resemble the economic losses suffered by individuals whose information has been released into the hands of identity thieves and whose jobs are lost due to false information generated by data brokers.

---

77. *Id.*; *see* Chuck Jaffe, *Stupid Investment of the Week*: *Identity-Theft Insurance Isn't Even Worth Its Small Price*, MARKET WATCH, Dec. 5, 2006, http://www.marketwatch.com/story. Industry experts note that Consumer Reports finds that identity theft insurance has little value due to its high deductibles. Richard G. Clarke, *Is ID Theft Insurance Worth Recommending to Agency Clients?*, INS. J., Oct. 9, 2008, http://www.insurancejournal.com/news/national/2008/10/09/94495.htm?print=1.

78. No. 01-2-09513-7 SEA, 2001 WL 1751590 (Wash. Sup. Ct. May 10, 2001).

79. *Id.*

80. *Id.* at *6.

81. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004) [hereinafter SOLOVE, DIGITAL PERSON].

82. Only in the exceptional case do people discover that their digital dossiers contain incomplete and misleading information about them. For instance, in 2009, data broker ChoicePoint provided an employer with a dossier on a Georgia man that falsely asserted that he had two felony convictions. *Your Bottom Line: Protecting Your Privacy* (CNN television broadcast Oct. 3, 2009), *available at* http://transcripts.cnn.com/TRANSCRIPTS/0910/03/ybl.01.html (transcript). The employer refused to hire the man and explained the reason to him. *Id.* A congressman from Georgia was able to convince ChoicePoint to remove the false criminal information from his dossier. *Id.*

83. PROSSER & KEETON, *supra* note 8, at § 110. For instance, plaintiffs have recovered for economic losses suffered after investing in a bankrupt automobile agency based on false assurances of profits. Hanson v. Ford Motor Co., 278 F.2d 586 (8th Cir. 1960).

84. PROSSER & KEETON, *supra* note 8, at §§ 129, 130.

C. Physical Injuries Exacerbated

In the past, physical injuries associated with privacy invasions typically involved a person's physical manifestations of emotional distress. For instance, individuals often suffered sleeplessness in the face of privacy invasions.[85] Today, the physical harm associated with information disclosures can become as serious as murder. For example, in *Remsburg v. Docusearch, Inc.*,[86] a disturbed man obsessed with Amy Boyer purchased her Social Security number and work address from information broker Docusearch.[87] The stalker confronted Ms. Boyer at work and killed her.[88]

In a similar vein, website operators facilitate physical assaults by exposing personal information online. In 1997, an anti-abortion group hosted a website called the *Nuremberg Files*, which provided a detailed profile of abortion providers.[89] This was part of a campaign by a group to terrorize abortion doctors.[90] The website included data on more than two hundred individuals, including their names, home addresses, photographs, driver's license numbers, SSNs, and information about family members—such as the schools their children attended.[91] It listed in grey the names of doctors who had been wounded and put a line through the names of doctors who had been murdered.[92] After the website's creation, two abortion doctors were shot at their homes.[93] In 1998, an abortion clinic in Alabama was bombed and another doctor killed by sniper fire at his home in New York.[94] Immediately afterwards, the website put a strike through the deceased doctor's name.[95]

In other cases, website operators have hosted "advertisements" of women's home addresses and their purported interest in rape fantasies, which in at least one case led to the rape and assault of a woman.[96] In early December 2009, an advertisement on Craigslist listed a picture of a woman, her home address, and her alleged "need" for a "real aggressive man with no concern for women."[97] The advertisement was posted by the woman's ex-boyfriend.[98] It prompted a man to show up at the woman's front door, assault and rape the

85. *See* note 37 and accompanying text (discussing relevant cases).
86. 816 A.2d 1001 (N.H. 2003).
87. *Id.* at 1005–06.
88. *Id.*
89. SOLOVE, THE FUTURE OF REPUTATION, *supra* note 20, at 100.
90. *Id.*
91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.* at 101.
95. *Id.*
96. Neary, *supra* note 20; DeeDee Correll, *Craigslist Implicated in Rape Case; A Wyoming Man is Accused of Using the Website to Engineer an Ex-Girlfriend's Assault*, L.A. TIMES, Jan. 11, 2010, at A9.
97. Neary, *supra* note 20.
98. *Id.*

woman, and leave her bound and gagged on the floor.[99] The assailant claimed that he did so at the invitation of the woman's advertisement and thought he was fulfilling her rape fantasy.[100] Although Craigslist had taken the posting down after the woman complained, it remained up long enough for the assailant to see it.[101]

A similar incident involving Craigslist occurred in August 2009. A Craigslist's Casual Encounters[102] listing included a posting of a teenager's picture, work address, cell phone number, and email address.[103] The listing suggested that the young woman had rape fantasies.[104] Immediately thereafter, men called the teenager, flooded her email inbox with messages containing pornography, and confronted her as she left work.[105] In the same vein, in 2009, a Long Island, New York, mother allegedly posted an advertisement on Craigslist seeking sex and directing men to the mother of her nine-year-old daughter's rival.[106]

In an early case of online impersonation, a security guard pretended to be a woman in a chat room, claiming that the woman wanted to be assaulted.[107] The chat room posting asserted: "I want you to break down my door and rape me."[108] It also provided the woman's name, address, and instructions about how to get past her building's security system.[109] Over the next few weeks, nine men showed up at her door, often in the middle of the night.[110]

The physical harm that website operators and data brokers facilitate resembles the physical injuries that result when landlords fail to secure their

99. Correll, *supra* note 96 (recounting court testimony that the man allegedly said to the victim "I'll show you aggressive" before he attacked her).

100. *Id.*

101. Neary, *supra* note 20.

102. Users post their information on the Casual Encounters section of Craigslist to arrange consensual sexual encounters. *See* Douglas Quenqua, *Recklessly Seeking Sex on Craigslist*, N.Y. TIMES, Apr. 19, 2009, at ST1 ("Although sex is solicited online in many places—legally and otherwise—the Casual Encounters listings are a major hub, offering to do for casual sex what the rest of the site does for no-fee apartments, temp jobs and old strollers."); Kashmir Hill, *Using Craigslist to Crowdsource Revenge*, TRUE/SLANT (June 1, 2010, 7:43 AM), http://trueslant.com/KashmirHill/2010/06/01/using-craigslist-to-crowdsource-revenge/ ("For those who don't regularly surf Craigslist to make personal connections, 'casual encounters' is an area usually frequented by those interested in one-off sexual adventures with strangers.").

103. *Mo. Woman Charged with Cyberbullying Teen*, CBS NEWS, Aug. 18, 2009, http://www.cbsnews.com/stories/2009/08/18/tech/main5249367.shtml.

104. *Id.*

105. *Id.*

106. Correll, *supra* note 96.

107. HAL ABELSON, KEN LEDEEN & HARRY LEWIS, BLOWN TO BITS: YOUR LIFE, LIBERTY, AND HAPPINESS AFTER THE DIGITAL EXPLOSION 249–51 (2008); U.S. DEP'T OF JUSTICE, 1999 REPORT ON CYBERSTALKING, *available at* http://www.justice.gov/criminal/cybercrime/cyberstalking.htm (Report from the Attorney General to the Vice President).

108. ABELSON, LEDEEN & LEWIS, *supra* note 107, at 250.

109. *Id.*

110. *Id.*

property.[111] Data brokers and website operators exercise control over, and have the ability to secure, information they host much as landlords do for their buildings' common areas.

Contemporary privacy injuries are worse and more widespread than those of the past. As modern technology becomes more integrated with our society, these injuries last longer and invade more areas of people's lives. The next Part explores the interests that privacy tort law protects and its limitations in the face of these injuries.

II.
THE EVOLUTION OF PRIVACY TORT LAW

This Part begins by sketching Warren and Brandeis's vision of the privacy tort and the interests that it protected. For Warren and Brandeis, the tort secured people's ability to limit access to themselves and to determine the amount of personal information revealed to others and, in this way, to develop their personalities without interference. This Part also explores how Prosser shifted, and ultimately narrowed, the privacy tort's development with his blend of doctrine and policymaking. Finally, this Part explains why the privacy torts often fail to prevent and remedy twenty-first century privacy problems.

A. Warren and Brandeis's Right to Be "Let Alone"

In 1890, Warren and Brandeis called for a tort to protect a person's "right to privacy," a right to be free from the prying eyes and ears of others.[112] They sought to protect a person's personality from societal and technological developments that saw no boundary.[113] They argued that such a tort would tackle the problem of "[i]nstantaneous photographs and newspaper enterprise[s] [that had] invaded the sacred precincts of private and domestic life."[114] Such "political, social, and economic" change interfered with people's ability to

111. *See* Kline v. 1500 Mass. Ave. Apartment Corp., 439 F.2d 477, 480–81 (D.C. Cir. 1970) (finding landlord liable where a poorly secured building resulted in tenants' physical beating at the hands of criminals); Novak v. Capital Mgmt. & Dev. Corp., 452 F.3d 902 (D.C. Cir. 2006) (holding that a club operator had a duty to use reasonable care in protecting patrons from danger of attack in an alley because operators controlled the alley and knew about prior criminal conduct there).

112. Warren & Brandeis, *supra* note 1, at 195. The story behind the writing of *The Right to Privacy* is illuminating. The penny press actively covered the domestic social engagements of Samuel Warren and his wife Mabel Bayard, who was the daughter of a U.S. Senator. MELVIN I. UROFSKY, LOUIS D. BRANDEIS: A LIFE 97 (2010). Warren had a "deepseated abhorrence" for the society pages, which prompted him to recruit his law partner Brandeis to coauthor *The Right to Privacy*. Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295, 1302 (2010) (contending that Warren and Brandeis wanted to protect elites from the unwanted gaze of social inferiors while shoring up traditional Gilded Age notions of gender roles and the "cult of domesticity.").

113. UROFSKY, *supra* note 112, at 100.

114. Warren & Brandeis, *supra* note 1, at 195.

determine how their private lives are portrayed to the public.[115] In Warren and Brandeis' view, the common law secured the right to determine "to what extent [one's] thoughts, sentiments, and emotions shall be communicated to others."[116] Thus, the privacy tort would prevent the publication of a person's private life from "being depicted at all."[117]

Warren and Brandeis argued that tort law should protect the privacy of the individual from "invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds."[118] They believed that without a cause of action for privacy breaches, society might sacrifice its "robustness of thought and delicacy of feeling."[119] As Randall Bezanson explained, Warren and Brandeis gave a legal definition to the boundary between the public and the private—"between occasions when personal information should be the business of others and occasions when it should be no one else's affair."[120]

The Right to Privacy offered a distinct view of the privacy tort's legally protected interest. The tort of privacy protected individuals' ability to develop their "inviolate" personalities without unwanted interference from prying eyes.[121] It preserved people's ability to decide how much of themselves and their personal information would be revealed to others.[122] As Warren and Brandeis underscored, privacy invasions injured a person's "estimate of himself."[123] They inflicted "mental pain and distress, far greater than could be inflicted by mere bodily injury."[124]

Warren and Brandeis explained that the "harm wrought by such invasions" was not "confined to the suffering of those who may be made the subjects of journalistic or other enterprise."[125] For them, "[e]ven gossip apparently harmless, when widely and persistently circulated, is potent for evil" in its ability to "belittle the relative importance of things."[126] According to Edward Bloustein, Warren and Brandeis envisioned the privacy tort as protecting an individual's "independence, dignity, and integrity"—for them, determining how much of oneself to reveal to others "define[d] man's essence

115. *Id.* at 196.
116. *Id.* at 198.
117. *Id.* at 218.
118. *Id.* at 206.
119. *Id.* at 196.
120. Randall P. Bezanson, The Right to Privacy *Revisited: Privacy, News, and Social Change, 1890-1990*, 80 CALIF. L. REV. 1133, 1135 (1992). In many respects, the line between public and private was far easier to identify in the late nineteenth century than it is today.
121. *Id.* at 17.
122. Warren & Brandeis, *supra* note 1, at 213.
123. *Id.* at 197.
124. *Id.* at 196.
125. *Id.*
126. *Id.*

as a unique and self-determining being."[127]

Shortly after the publication of *The Right to Privacy*, courts adopted privacy torts in the manner that Warren and Brandeis suggested.[128] In 1905, the Supreme Court of Georgia recognized a privacy tort claim in a case involving the non-consensual use of the plaintiff's picture in a newspaper advertisement.[129] Invoking Warren and Brandeis's article, the court enforced the plaintiff's claim, finding that special damages were not necessary to state a cause of action because an infringement on privacy "is a direct invasion of a legal right."[130] The court noted that the "right of privacy" secures a person's "right to live as one will."[131] As the court underscored, privacy tort law protected a person's "desire to live a life of seclusion" or to "live a life of privacy as to certain matters, and of publicity as to others."[132] By 1911, courts and legislatures in nine states recognized some version of Warren and Brandeis's "right to privacy."[133] In recognizing privacy claims, courts underscored that the privacy tort protected one's "inviolate personality."[134]

B. Prosser's Blend of Social Engineering and Doctrine

Seventy years after *The Right to Privacy*'s publication, Prosser engaged in work that changed the trajectory of privacy tort law. As the Reporter for the *Second Restatement of Torts* and as a scholar, Prosser deemphasized tort privacy's protection of a person's right to be "let alone" and instead focused on the conduct and injuries involved in privacy invasions.[135] He argued that privacy tort law protected against four types of activities and the emotional, reputational, and proprietary injuries that they inflicted.[136] Prosser's approach grew out of his desire to redress and prevent injuries and to honor precedent in a manner that would prevent the privacy tort from bleeding into other torts. While Prosser "gave privacy a doctrinal unity and continuity that it had not

127. EDWARD J. BLOUSTEIN, INDIVIDUAL AND GROUP PRIVACY 10 (2003).

128. Edward Bloustein pointed to numerous cases that use Warren and Brandeis's conceptualization of the tort of privacy in upholding a privacy claim. Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 977, 979 (1964).

129. Pavesich v. New England Life Ins. Co., 50 S.E. 68, 68–69 (Ga. 1905); *see, e.g.*, Afro-Am. Publ'g Co. v. Jaffe, 366 F.2d 649, 654 (D.C. Cir. 1966) (recognizing an invasion of privacy claim based on Warren and Brandeis's article as vindicating the right of private personality, the right to be let alone, which stands on "high ground, cognate to the values and concerns protected by constitutional guarantees").

130. *Pavesich*, 50 S.E. at 73.

131. *Id.* at 70.

132. *Id.*

133. Benjamin E. Bratman, *Brandeis and Warren's 'The Right to Privacy and the Birth of the Right to Privacy'*, 69 TENN. L. REV. 623, 643 (2002).

134. Mau v. Rio Grande Oil, Inc., 28 F. Supp. 845, 846 (N.D. Cal. 1939).

135. Prosser, *supra* note 8, at 392–400.

136. *Id.*; WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS 829–42 (3d ed. 1964) [hereinafter PROSSER, HANDBOOK 3d].

previously possessed,"[137] he also narrowed its reach.

Prosser's interest in policymaking led him to suggest an approach to tort law driven by particular harms. Generally speaking, Prosser saw tort law as "social engineering," or the adjustment of "conflicting interests of individuals to achieve a desirable social result."[138] He recommended that judges resolve tort cases in the way that would produce the "greatest happiness of the greatest number."[139] For Prosser, tort law should prevent and remedy losses caused by antisocial conduct.[140] To that end, Prosser organized torts around injuries caused by particular hazards.[141]

Oliver Wendell Holmes exemplified this harm-based approach.[142] In *The Common Law*, Holmes explained that the evil against which tort law was directed was the inflicting of harm.[143] Tort law protected against harms and remedied them "'not because they [were] wrong, but because they [were] *harms*.'"[144] Holmes sought to strike a balance between the social interests in preventing the infliction of harm and in protecting freedom of action.[145]

In categorizing the privacy torts, Prosser emulated Holmes's focus on specific injuries caused by particular conduct. As Diane Zimmerman observed, Prosser's privacy taxonomy conformed to the Holmesian model of focusing on law's compensatory function.[146] But, in doing so, Prosser identified the injuries suffered quite narrowly. He envisioned the privacy torts' legally protected interest as a person's freedom from emotional distress, damaged reputation, and proprietary harm caused by the four types of privacy-invasive activities that became his privacy taxonomy.[147] For instance, he explained that a defendant's

---

137. WHITE, *supra* note 21, at 173.

138. WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS § 3, at 15 (1st ed. 1941) [hereinafter PROSSER, HANDBOOK 1st].

139. *Id.* at 17.

140. *Id.* at 15, 17.

141. WHITE, *supra* note 21, at 176. As Richard Markovits observed, Prosser believed that judges should operate as goal-oriented policymakers rather than identifying "unique answers that are right as a matter of law." Richard S. Markovits, *Liberalism and Tort Law: On the Content of the Corrective-Justice-Securing Tort Law of a Liberal, Rights-Based Society*, 2006 U. ILL. L. REV. 243, 293 (describing important contemporary tort scholars and judges, such as Fleming James, Roger Traynor, and William Prosser, as moral skeptics interested in social engineering).

142. LOUIS MENAND, THE METAPHYSICAL CLUB 339 (2001). Torts scholar Thomas C. Grey vividly describes Holmes's harm-based approach in his article *Accidental Torts*, 54 VAND. L. REV. 1225 (2001).

143. OLIVER WENDELL HOLMES, THE COMMON LAW 64 (1881, reissued 1963).

144. Thomas C. Grey, *Accidental Torts*, 54 VAND. L. REV. 1225, 1272 (2001) (quoting Holmes, *supra* note 143, at 144) (emphasis added).

145. *Id.* at 1272. Grey categorized ordinary activities warranting negligence and extra hazardous ones warranting strict liability. DAVID ROSENBERG, THE HIDDEN HOLMES: HIS THEORY OF TORTS IN HISTORY 128 (1995).

146. Diane Leenheer Zimmerman, *Musings on a Famous Law Review Article: The Shadow of Substance*, 41 CASE W. RES. L. REV. 823, 825 (1991).

147. *Id.* Reviewing Prosser's 1941 treatise, Laurence Eldredge explains that while Prosser treated mental distress claims separately from privacy claims, the "interest invaded in the privacy

intrusion on another's seclusion interfered with that person's interest in being free from emotional distress.[148] For "publicity of private facts" and "false light" claims, "[t]he interest protected is that of reputation, with the same overtones of mental distress that are present in libel and slander."[149]

Prosser based privacy tort law's legally protected interest on his analysis of precedent. In that sense, his approach owed much to his doctrinal instincts.[150] Prosser classified, catalogued, and synthesized reported decisions to reveal general rules.[151] Based on the cases, Prosser identified four types of privacy-impairing activities: (1) unreasonable intrusion upon a person's seclusion, (2) appropriation of someone's name or likeness, (3) unreasonably giving publicity to a person's private life, and (4) publicizing someone in a false light.[152] He based those rules on well-established precedent because, in his view, judges take comfort in steering according to the "magnetic needle of stare decisis."[153]

G. Edward White aptly described Prosser's methodology as "Consensus Thought."[154] While Prosser collected cases, rationalized results, and stated general rules, he balanced the interests at stake and focused on injuries worthy of prevention and compensation.[155] As Craig Joyce explained, Prosser acknowledged and identified the "various interests to be balanced, while relentlessly asserting (and, by copious citations and deceptively simple illustrations, seeming to prove) that the results of the cases, on proper analysis, were but multiple, somewhat varied yet ultimately consistent examples of

---

cases is the interest in freedom from mental distress." Book Review, 90 U. PA. L. REV. 505, 506 (1942).

148. Prosser, *supra* note 8, at 392 (explaining that the "interest protected by [the intrusion] tort is primarily a mental one" useful to fill the gaps left by trespass, nuisance, and the intentional infliction of mental distress and whatever remedies there may be for the invasion of constitutional rights).

149. *Id.* at 398. Prosser's view of the injuries that the privacy torts protected against developed over time. In 1941, Prosser saw the tort of privacy as part "of the larger problem of the protection of the plaintiff's peace of mind against unreasonable disturbance." PROSSER, HANDBOOK 1st, *supra* note 138 § 107, at 1053–54. Indeed, Prosser suggested that if the "'new tort' of the intentional infliction of mental suffering receives general recognition, the great majority of the privacy cases may be expected to be absorbed into it." *Id.* In his *Privacy* article and as the Reporter on the *Second Restatement of Torts*, Prosser expanded his description of privacy injuries to include reputational and proprietary harms. Prosser, supra note 8, at 400-01; RESTATEMENT (SECOND) OF TORTS § 652H (1977).

150. *See* Neil Richards & Daniel Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010) [hereinafter Richards & Solove, *Prosser's Privacy Law*] (discussing Prosser's doctrinalism).

151. WHITE, *supra* note 21, at 158; Craig Joyce, *Keepers of the Flame: Prosser and Keeton on the Law of Torts (Fifth Edition) and the Prosser Legacy*, 39 VAND. L. REV. 851, 860 (1986).

152. Prosser, *supra* note 8; Prosser, HANDBOOK 3d, *supra* note 136, at 829–42.

153. William L. Prosser, Book Review, 16 MINN. L. REV. 222, 223 (1932) (reviewing LEON GREEN, JUDGE AND JURY (1927)).

154. WHITE, *supra* note 21, at 176.

155. Joyce, *supra* note 151, at 892.

Prosser's own general rules."[156] In this way, Prosser fused the insights of instrumentalists, who emphasized the possibilities of social engineering, with the "countervailing demands" of doctrinally oriented scholars who sought predictability in the law.[157]

Anita Bernstein argues that Prosser's blend of doctrine and policymaking was crucial to his privacy taxonomy's success.[158] According to Bernstein, Prosser's reform-minded agenda needed precedent to thrive.[159] While Prosser's focus on the remedy and prevention of harm gave the privacy torts "intellectual legitimacy," his reliance on case law "reassured onlookers that their measure would not go out of control."[160] Bernstein contends that because tort innovations had long been treated with suspicion and panic, Prosser wisely invoked doctrine to make a case for the privacy torts.[161] Bernstein described Prosser as "better than anyone at the job of making a new tort look conservative."[162] The "combination of two opposing jurisprudential postures permitted new torts to form" without being labeled as such.[163]

Prosser's privacy taxonomy now permeates case law.[164] Its classifications have taken on the status of doctrine.[165] The 1971 edition of the Prosser hornbook proudly noted that "as yet no decided case allowing recovery" in privacy had occurred "which does not fall fairly within one of the four categories."[166] This remains true today: Prosser's taxonomy now "supplant[s] Warren and Brandeis's work as the touchstone of privacy jurisprudence."[167]

C. The Legacy of Prosser's Privacy Taxonomy

In spite of its dominance in tort law, Prosser's privacy taxonomy is a double-edged sword. Although it provided a pragmatic response to twentieth-century privacy intrusions, it leaves many contemporary privacy injuries uncompensated.[168]

---

156. *Id.*
157. *Id.*
158. Anita Bernstein, *The New-Tort Centrifuge*, 49 DEPAUL L. REV. 413, 418–20 (1999).
159. *Id.* at 418.
160. *Id.*
161. *Id.* at 419.
162. *Id.* at 423.
163. *Id.* at 420.
164. WHITE, *supra* note 21, at 430.
165. *Id.* at 158. Aside from Prosser's contribution in getting judges to recognize the four privacy torts, his other lasting accomplishments include his support for, and clarification of, the tort of intentional infliction of emotional distress as well as strict products liability. *See* William L. Prosser, *Intentional Infliction of Mental Suffering: A New Tort*, 37 MICH. L. REV. 874 (1939).
166. WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS § 117 at 816 (4th ed. 1971) [hereinafter PROSSER, HANDBOOK 4th].
167. Jonathan Kahn, *Bringing Dignity Back to Light: Publicity Rights and the Eclipse of the Tort of Appropriation of Identity*, 17 CARDOZO ARTS & ENT. L.J. 213, 223 (1999).
168. Richards & Solove, *Prosser's Privacy Law*, *supra* note 150, at 1918 (discussing the failure of privacy tort law to "adapt[] to new privacy problems such as the extensive collection,

Part of the problem can be attributed to Prosser's restrictive conception of the privacy torts' legally protected interest. Whereas Warren and Brandeis sought to protect an individual's right to be "let alone" from unwanted disclosure and intrusion, Prosser saw privacy tort law as protecting a person from emotional, reputational, and proprietary harm caused by specific activities. This narrowed the reach of the privacy torts from an approach that could adapt to changing circumstances to one that addressed four narrow types of privacy-invasive activities and their accompanying injuries. Importantly, it stopped courts from fleshing out the contours of the "right to be let alone" protected by tort privacy.

Courts adopted Prosser's privacy taxonomy with such rigidity that privacy tort law is now locked into a "writ system."[169] Courts recognize the four privacy torts but *only* those privacy torts.[170] Legal forms naturally tend to shape our thinking,[171] and Prosser's prestige and work on the *Second Restatement of Torts* additionally ensured the adoption of this constricted approach.[172] Privacy torts have taken on a "quasi-legislative prescription of the bounds of future liability for invasions of privacy."[173] At the same time, courts have narrowly construed the elements of the four privacy torts, further limiting their reach. This is surely due to the concern that privacy claimants could recover for trivialities given the ethereal nature of the alleged harm.[174]

In its current state, Prosser's privacy taxonomy plays a limited role in tackling many contemporary privacy injuries.[175] As this Part shows, some

---

use, and disclosure of personal information by businesses").

169. David W. Leebron, The Right to Privacy's *Place in the Intellectual History of Tort Law*, 41 CASE W. RES. L. REV. 808 (1991); White, *supra* note 21, at 176.

170. HARPER ET AL., HARPER, JAMES & GRAY ON TORTS § 9.6A (3d ed. 2006).

171. Nancy Levit, *Ethereal Torts*, 61 GEO. WASH. L. REV. 136 (1992); Jay M. Feinman, *The Jurisprudence of Classification*, 41 STAN. L. REV. 661 (1989).

172. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 153 (2008) [hereinafter Richards & Solove, *Privacy's Other Path*]. As Harry Kalven presciently noted in 1966: "given the deserved Prosser prestige, it is a safe prediction that the fourfold view will come to dominate whatever thinking is done about the right of privacy in the future." Kalven, *supra* note 24, at 332.

173. HARPER ET AL., *supra* note 170, § 9.6A (3d ed. 2006).

174. *See* Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 324 (1983) (arguing that recovery in privacy tort based solely or largely on claimed psychological harm "hardly rests on firm legal ground" because injuries are difficult to measure); Lyrissa Barnett Lidsky, *Prying, Spying, and Lying: Intrusive Newsgathering and What the Law Should Do About It*, 73 TUL. L. REV. 173, 211 (1998) (attributing plaintiffs' limited success in bringing intrusion on seclusion claims to courts' hostility to dignitary torts).

175. *See, e.g.*, Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1304 (2000) ("[A]s the literature has made very clear, the invasion of privacy tort is too narrowly defined to serve."); Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1634 (1999) ("Although the most likely place to begin a search for legal safeguards is the tort law of privacy, it is of little help in cyberspace."); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1231 (1998) ("[T]he common law tort of invasion of privacy has thus far provided no effective constraints on the sort of information

privacy problems fall outside the four privacy torts. And while others may be covered by the torts, their restrictive elements may preclude recovery.

1. Privacy Problems Falling Outside the Reach of the Privacy Torts

When Prosser constructed his taxonomy, privacy intrusions typically involved information collected directly from individuals.[176] Government and businesses stored personal data in paper records, posing a limited threat to individual privacy.[177] By contrast, today's privacy problems often emerge from the way that public and private entities handle and maintain personal data.[178] Because Prosser's taxonomy addressed privacy invasions characteristic of prior eras, and because courts applied it rigidly, privacy torts often do not prevent or redress many contemporary privacy injuries involving the collection and disclosure of personal information.

For example, privacy torts may not redress injuries resulting from insecure databases of sensitive personal information.[179] In public disclosure suits, plaintiffs must show that the defendants widely publicized the personal information:[180] communication of data to a single individual or a small group of people is insufficient.[181] Courts likely would not recognize public disclosure claims for the leaking of sensitive information to identity thieves, or for the release of distorted digital dossiers to employers, because only a small number of people—hackers—sees the sensitive personal information.[182]

---

flows depicted above.").

176. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 15, at 189.

177. The first federal agencies to use mainframe computers for storage and computation purposes—the Social Security Administration, the Census Bureau, and the Internal Revenue Service—began doing so in the mid-to-late 1950s. LANE, *supra* note 39, at 138. When Prosser wrote his seminal article *Privacy* and worked on the Second Restatement of Torts in the early 1960s, computers still had not replaced paper files for general government recordkeeping. *Id.* at 138–39. The migration to computerized files began in earnest in the late 1960s. *Id.*

178. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 15, at 189.

179. *See* Richards & Solove, *Privacy's Other Path*, *supra* note 172, at 155 (discussing the various ways that the privacy torts fail to address problems related to the collection, processing, and disclosure of information); *see also* SOLOVE, DIGITAL PERSON, *supra* note 81; Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087 (2006); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001). Michael Rustad and Thomas Koenig note a variety of areas where courts have failed to address twenty-first century privacy problems, including the online publication of disciplinary actions where the information is part of a public record and the widespread surveillance of employees' Internet use in the workplace. Michael L. Rustad & Thomas H. Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77, 129–30 (2004).

180. RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (1977) ("it is not an invasion of the right of privacy . . . to communicate a fact concerning the plaintiff's private life to a single person or even to a small group of persons").

181. Swinton Creek Nursery v. Edisto Farm Credit, 514 S.E.2d 126, 132 (1999).

182. *See* Bodah v. Lakeville Motor Express, Inc., 663 N.W.2d 550 (Minn. 2003) (finding no publicity under disclosure tort, where defendant gave plaintiffs' Social Security numbers to sixteen of its managers, because disclosure needs to be to the public at large). Disclosures of

Moreover, plaintiffs probably cannot sue database operators for intrusion on seclusion under current case law. To prevail in an intrusion suit, a plaintiff must show that a defendant invaded his physical solitude or seclusion, such as by entering his home, in a manner that would be highly offensive to the reasonable person.[183] Database operators and data brokers, however, never intrude upon a plaintiff's private space. They do not gather information directly from individuals and, to the extent that they do, the privacy problem involves the failure to secure personal information, not its collection.[184]

Those harmed by database operators' failure to keep private information secure likely do not have a false light claim either. False light claims require proof of a plaintiff's placement in a false light.[185] These claims do not apply when, as here, leaked information causes mischief because it is true.[186]

Finally, appropriation claims are also insufficient to protect the rights of individuals harmed by database leaks. Appropriation claims arise when a defendant uses for his own benefit the name or likeness of another.[187] In leaking sensitive personal information, database operators do not use plaintiffs' name or image for their commercial advantage. Instead, database operators fail to secure sensitive personal information from criminals.[188] Appropriation claims simply have no application to database operators who leak sensitive personal information to identity thieves.

Other modern privacy problems also fall outside of the scope of Prosser's taxonomy. Privacy tort law does not address website operators' display of individuals' home addresses in ways that make them vulnerable to physical

---

personal data by data brokers also might not be considered "highly offensive to the reasonable person" as one's home address, finances, and shopping habits might not strike many as deeply embarrassing or humiliating. SOLOVE, DIGITAL PERSON, *supra* note 81, at 60.

183. PROSSER, HANDBOOK 4th, *supra* note 166, at 833.

184. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 15, at 189; *see, e.g.*, Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995) (dismissing intrusion on seclusion claim where defendant rented lists of consumer behavior because defendant compiled the information about plaintiffs from their own records and because plaintiffs freely gave that information to defendant). To be sure, database operators may collect information from individuals at the outset—businesses collect SSNs for a variety of reasons. The harm is not the collection here but instead the failure to secure the information from criminals.

185. PROSSER, HANDBOOK 4th, *supra* note 166, at 837.

186. False light claims could be invoked where data brokers reveal false or distorting information to prospective employers as in the ChoicePoint matter discussed in Part I, if courts found such activities highly offensive to the reasonable person. Because false light claims raise free speech concerns, many courts refuse to recognize them. Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998).

187. RESTATEMENT (SECOND) OF TORTS § 652C (1977); *see* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 218 (3d ed. 2008) (explaining that appropriation protects against the "commercial" exploitation of one's name or likeness).

188. *See, e.g.*, Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1010 (N.H. 2003) (dismissing appropriation claim against data broker who sold personal information to stalker because data broker did not seek to take advantage of person's good will or reputation in using the information).

attack. For instance, plaintiffs cannot bring intrusion on seclusion claims in this situation because online postings do not involve invasions of a place or information that society recognizes as private. Website operators often cannot be said to have used someone's image for their own commercial advantage or to have put targeted individuals in a false light.[189] Because postings often reveal publicly available information such as a person's home address, courts likely would not uphold disclosure claims against website operators on the grounds that the disclosed information is not private.[190]

2. Precluding Recovery for Injuries Covered by the Privacy Torts

Prosser's taxonomy may also have limited value in cases that are covered by the privacy torts. Generally speaking, plaintiffs have difficulty pursuing privacy claims.[191] A study found that from 1974 to 1984, plaintiffs prevailed in 2.8% of cases involving public disclosure claims against the media and in twelve percent of cases involving non-media defendants.[192] In intrusion actions, plaintiffs succeeded in ten percent of cases against non-media defendants and in three-eights of cases against media defendants.[193] Plaintiffs recovered in one-third of cases where plaintiffs sued media and non-media defendants for appropriation.[194]

Privacy tort claims' restrictive elements play a role in this disappointing track record. Courts have long demanded considerable proof in privacy cases to prevent recovery for trivialities.[195] They routinely require plaintiffs to show that defendant's conduct was "highly offensive to the reasonable person."[196] Courts

189. Website postings involving impersonations would implicate false light claims against the posters themselves.

190. Richards & Solove, *Prosser's Privacy Law*, *supra* note 150, at 1919 (explaining that disclosures of a person's home address would not satisfy the "highly offensive to the reasonable person" requirement of disclosure privacy tort). A small number of courts have, however, found that individuals have a privacy interest in their home addresses. *See, e.g.*, Nat'l Ass'n of Retired Fed. Emps. v. Horner, 879 F.2d 873 (D.C. Cir. 1989) (finding that individuals had privacy interest in avoiding unlimited disclosure of their names and addresses); *see also* Benz v. Wash. Newspaper Publ'g Co., 2006 WL 2844896, at *8 (D.D.C. Sept. 29, 2006) (refusing to dismiss public disclosure claim where defendant published plaintiff's home address, alongside her suggested interest in sex, online because her home address was a private fact given that it was not published elsewhere). Moreover, as the next Part addresses, section 230 of the Communications Decency Act (CDA) affords website operators broad immunity for publishing the content of other websites. *See infra* Part III.

191. RANDALL P. BEZANSON, GILBERT CRANBERG & JOHN SOLOSKI, LIBEL LAW AND THE PRESS: MYTH AND REALITY 116 (1987).

192. *Id.*

193. *Id.* Aside from the study discussed in the Bezanson book, I know of no other contemporary studies regarding the success rates of privacy claims.

194. *Id.*

195. Kalven, *supra* note 24 at 328.

196. Notably, the *Restatement of Torts* only required evidence that the defendant's actions were "offensive to persons of ordinary sensibilities." § 867 cmt. d (1939). The *Restatement (Second) of Torts* elevated it to "highly offensive to a reasonable person." § 652B (1977). Prosser

insist upon proof of intentional conduct[197] and regularly adopt a restrictive view of what constitutes private information worthy of protection.[198]

Free speech concerns impact the efficacy of privacy torts as well. Courts dismiss public disclosure claims where information addresses a newsworthy matter, in other words, one of public concern.[199] They often defer to the media's judgment, all but guaranteeing the demise of plaintiffs' claims.[200] The Supreme Court has recognized the constitutional status of the newsworthiness test, requiring heightened scrutiny for restrictions on certain disclosures of public concern.[201] For instance, in *Cox Broadcasting Corp. v. Cohn*,[202] the Supreme Court held that the press could not be sanctioned for publicizing true information obtained from court documents open to public inspection.[203] In *Florida Star v. B.J.F.*,[204] the Court reiterated this rule, concluding that the First Amendment prohibited liability when a newspaper published the name of a rape victim obtained from a police report.[205] A recent Supreme Court decision, however, recognized the possibility that privacy could trump newsworthiness concerns in certain contexts, signaling a turn in favor of privacy against press freedoms.[206]

On top of these obstacles, plaintiffs have difficulty recovering for their emotional and reputational harm due to the privacy torts' restrictive

---

surely had something to do with this. In *Privacy*, he expressed dismay that privacy tort law did not require proof of extreme outrage and serious mental harm as did intentional infliction of emotional distress claims. Prosser, *supra* note 8, at 422. He argued that because privacy tort claims often sought recovery for emotional distress, they should demand the same proof as intentional infliction of emotional distress claims. *Id.*

197. RESTATEMENT (SECOND) OF TORTS § 652B (1977); Yoder v. Ingersoll-Rand Co., 31 F. Supp. 2d 565 (N.D. Ohio 1997) (dismissing privacy claim arising from disclosure of plaintiff's HIV status because the disclosure was not intentional).

198. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005).

199. Richards & Solove, *Privacy's Other Path*, *supra* note 172.

200. *Id.*

201. Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 988–89 (2003).

202. 420 U.S. 469 (1975).

203. *Id.* at 469–97. In a subsequent decision, the Court held that "[i]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order." Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979).

204. 491 U.S. 524 (1989).

205. *Id.* at 533–37 (1989). The Supreme Court has also held that the First Amendment required proof of actual malice in false light cases. *See* Time, Inc. v. Hill, 385 U.S. 374 (1967).

206. Gajda, *supra* note 5, at 1079–80 (discussing Bartnicki v. Vopper, 532 U.S. 514, 532 (2001), which cautioned that privacy concerns might trump the public's interest in newsworthy matters in cases involving disclosures of "domestic gossip or other information of purely private concern"). In her important work, Amy Gajda has explored how courts now defer less to the media on questions of newsworthiness in a manner that poses serious free speech concerns. Gajda, *supra* note 5, at 1072–76.

elements.[207] In the pre-Internet era, courts deemed disclosures of a person's unflattering or unusual behavior as falling short of the "highly offensive to a reasonable person" standard. A court, for instance, found the revelation of a body surfer's proclivity to put cigarettes out on his tongue and eat insects "unflattering and perhaps embarrassing" but not sufficiently "morbid and sensational" to satisfy the "very high level of offensiveness" required.[208] Another court held that although publicity of a person's illegal parking in a handicapped spot was "unflattering," it would not be "highly offensive to the reasonable person" because parking violations are an "everyday occurrence with which every driver must contend."[209]

Although those disclosures have failed to warrant redress in the past, perhaps they should in the present. In our networked age, unflattering information posted online can cause significant harm. What if someone today posted information about a person's parking violations? Under current case law, courts likely would not find such disclosure, if true, "highly offensive to the reasonable person" because it involves the ordinary, rather than the sensational.[210] Nonetheless, this disclosure, when repeatedly revealed to professional and personal contacts, could produce emotional and reputational damage equivalent to the harm experienced by those satisfying the "highly offensive" standard in the pre-Internet age. Revelations of people's unusual or unappealing conduct may prominently appear in searches of their names, and their explanations, if any, may be buried in less prominent posts. Prospective employers and clients would see the embarrassing information without any context.[211] Online postings perpetuate a person's emotional suffering, muting concerns that plaintiffs might recover for trivialities. This warrants reconsideration of the privacy torts.[212]

In a similar vein, courts have narrowly interpreted the meaning of private information in the public disclosure tort. As noted above, courts have refused to

---

207. Privacy tort law might have some success in cases resembling Erin Andrews' struggles. No doubt, the intrusions on Ms. Andrews's seclusion would be deemed "highly offensive to the reasonable person." *See supra* text accompanying notes 54–59.

208. Virgil v. Sports Illustrated, 424 F. Supp. 1286, 1289 (S.D. Cal. 1976). The court explained that because the article included plaintiff's "retrospective, more mature, perception and explanation" of the facts "any negative impression" of the plaintiff was tempered by his own remarks. *Id.*

209. Joyce v. Nextmedia Grp., Inc., No. 12617-2003, 13133-2003, 2004 WL 1932742, at *6 (Pa. Ct. Com. Pl. Mar. 12, 2004).

210. This may be particularly true in cases where the disclosures involve private facts that other courts have determined fall short of the "highly offensive" standard. *See* Cole v. CSC Applied Tech., LLC, 2008 WL 2705458, at *2 (W.D. Okla. 2008).

211. This may be especially true of lurid postings, such as information about a person's sexual habits, because they tend to attract attention from other sites and thus would appear prominently in searches of a person's name.

212. Any potential solutions would not impact the free speech concerns that animate the newsworthiness element of public disclosure claims. *See supra* notes 198–205 and accompanying text.

recognize privacy claims where defendants publicized a person's home address.[213] Nonetheless, the publication of a person's home address poses serious risks. A restrictive approach to the disclosure tort seems unjustified in light of the dangers facilitated by our networked environment as discussed in Part I of this article. In short, the privacy torts often cannot properly redress contemporary privacy injuries. The next part explores how mainstream tort remedies can supply a means to protect important privacy interests.

III.
UPDATING PRIVACY TORT LAW FOR THE TWENTY-FIRST CENTURY

This Part offers potential strategies for ensuring privacy tort law's efficacy in the information age.[214] A promising approach is to update privacy tort law to protect the broader set of interests that Warren and Brandeis identified in *The Right to Privacy*. In so doing, courts could invoke mainstream tort tools to address contemporary privacy problems.[215] As Prosser understood with great success, second-best solutions can be preferable to first-order ones that have little chance of adoption.

This Part considers an extension of enablement and breach of confidence law as well as the adoption of strict liability for abnormally dangerous activities. This Part also contemplates strategies for ensuring the privacy torts' prevention and remedy of serious emotional and reputational injuries caused by

213. *See supra* note 187 and accompanying text (discussing how courts often do not recognize public disclosure claims based on the release of home addresses because that information is already in the public domain).

214. Either legislatures or courts could lead this effort. The question of which institution is better suited to do so is beyond the scope of this Article. For thoughtful discussion of the comparative competence of the legislature and judiciary to address emerging privacy problems, see Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 806 (2004) (arguing that "the legislative branch rather than the judiciary should create the primary investigative rules when technology is changing"); *see also* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747 (2005) (positing that the judiciary is no less competent to address privacy problems raised by emerging technologies than the legislature).

215. Recently proposed federal legislation does not offer support for the torts-focused agenda articulated here. In June 2010, Representative Rick Boucher submitted for comment a draft consumer privacy bill that proposed a "notice and choice" regime for much of the private sector's online and offline collection, use, and disclosure of personal information. Staff Discussion Draft, May 3, 2010, http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf; *see* Danielle Citron, *The Boucher Privacy Bill: A Little Something For Everyone yet Nothing for All?*, CONCURRING OPINIONS BLOG (June 13, 2010, 11:37 AM), http://www.concurringopinions.com/archives/2010/06/the-boucher-privacy-bill-a-little-something-for-everyone-yet-nothing-for-all.html (summarizing the key features of the Boucher bill). While providing notice and opt-out consent for the collection, use, and sharing of information in certain instances, and notice and opt-in consent in others, the bill would preempt state law on the collection, use, or disclosure of covered information and bar private rights of action as well. Omnibus privacy bills akin to the Boucher proposal would cut off state-level innovation, including tort claims, without sufficient privacy protections for consumers. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009).

networked technologies.

A. Mainstreaming Privacy Tort Law for the Twenty-First Century

The privacy torts' intellectual lineage provides important insights that may be crucial to their future. Warren and Brandeis set forth the broader set of interests protected by privacy tort law while Prosser demonstrated the wisdom of combining theory and practice. Heeding both could help privacy tort law adapt to meet the privacy problems of the digital age.

Our conception of privacy harm should include the interests addressed in *The Right to Privacy*. Warren and Brandeis identified a normative idea of privacy based on individuals' interest in constructing their identities and personalities free from unwanted interference.[216] They envisioned privacy tort law as protecting a person's right to be "let alone," whether that meant preventing someone from interfering with a person's solitude or precluding the revelation of personal information to others.[217] Their understanding of privacy included a person's right to control the release of information about his person.[218]

Warren and Brandeis did not detail the precise contours of this interest. But they did provide an important foundation for appreciating tort law's role in protecting individuals' interest in privacy. For seventy years after *The Right to Privacy*, courts developed the interests protected by tort privacy in greater detail, signaling when privacy mattered and when it deserved protection. Prosser's taxonomy, and narrow judicial interpretations of it, halted those efforts, but we could continue them now.

Why should we consider returning privacy tort law to a focus on the protection of a person's right to be "let alone"?[219] As Warren and Brandeis underscored, privacy honors human dignity by conferring "respect for individual choice" and "respect for individuals because they have the capacity for choice."[220] It encourages creativity[221] and self-development.[222] Privacy

---

216. Randall P. Bezanson, *Privacy, Personality, and Social Norms*, 41 CASE W. L. REV. 681, 682 (1991). *See* Solove, *Conceptualizing Privacy*, *supra* note 7, at 1101–02 (suggesting that Warren and Brandeis's use of the phrase "'inviolate personality' . . . could be viewed as describing the content of the private sphere").

217. Bloustein, *supra* note 128, at 1003.

218. *Id.*; *see also* U.S. Dep't of Justice v. Reporters Comm., 489 U.S. 749, 763 (1989) (explaining that "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person").

219. In answering this question, I draw upon a vast literature on the value of privacy, one spearheaded by Warren and Brandeis and developed in rich detail by thoughtful scholars. *See generally* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 15 (exploring the differing conceptions of the value of privacy). This Article does not attempt to create anew this important discussion; instead, it highlights the instrumental and moral value of privacy.

220. Leslie Meltzer Henry, Spheres of Dignity 20 (Sept. 10, 2009) (unpublished manuscript) (on file with author). As Leslie Meltzer Henry elegantly develops in her work, people have dignity insofar as they can make autonomous choices. *See* Bloustein, *supra* note 128, at 981–

provides a space for people to "make up [their] minds and to develop new ideas"[223] and fosters social relationships.[224] Permitting individuals to form their personalities free from unwanted interference promotes selfhood and human relations, furthering a free society.[225] In his dissent in *Olmstead v. United States*, Justice Brandeis noted that "the right to be let alone [is] the most comprehensive of rights and the right most valued by civilized men."[226]

Many contemporary privacy problems implicate the right to privacy. For instance, online postings revealing personal information to potential assailants interfere with the "right to be let alone." As Warren and Brandeis argued, the media's publication of private facts denied people the ability to live anonymously, free from prying eyes. When the media published a picture of a couple's deceased conjoined twins, the couple's lives became a public spectacle.[227] After the media published a surgical patient's before-and-after pictures, she experienced so much shame that she refused to go to work.[228]

Postings encouraging assailants to rape or kill people similarly expose

---

82 (arguing that the legally protected interest at the heart of the tort suggested by Warren and Brandeis was a person's individuality and human dignity). For important discussions of privacy's role in protecting individuals' dignity, see JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000); Robert Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 973–75 (1989).

221. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1424–28 (2000); *see also* ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 48 (1988); C. Edwin Baker, *Autonomy and Informational Privacy, or Gossip: The Central Meaning of the First Amendment*, 21 SOC. PHIL. & POL'Y, Jul. 2004, at 215, 221 ("The claim that meaningful autonomy requires privacy often involves assertions that for development, experimentation, and repose, individuals need the capacity to shield themselves, at various times and places and to varying degrees, from exposure to the critical eyes of the world.").

222. As Cohen and Schwartz develop in their work, privacy promotes self-development that is essential to public discourse. *Compare* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1424–28 (2000) (explaining that information privacy yields collective benefits because it promotes individual autonomy and self-development, which are central to robust public debate), *with* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1651–52 (1999) (arguing that information privacy rules are a precondition for deliberative autonomy and deliberative democracy). *See also* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights*, 44 FED. COMM. L.J. 195 (1992).

223. Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008) ("The ability to freely make up our minds and to develop new ideas thus depends upon a substantial measure of intellectual privacy."); *see also* Joel R. Reidenberg, *Setting Standards For Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 497 (1995) (arguing that "adequate standards for the treatment of personal information are a necessary condition for citizen participation in a democracy").

224. *See generally* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 15 (exploring the differing conceptions of the value of privacy).

225. Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423–24 (1980).

226. 277 U.S. 438, 478 (1927) (Brandeis, J., dissenting).

227. Bloustein, *supra* note 128, at 979 (explaining that when a newspaper publishes a picture of a newborn deformed child, its parents are mortified and insulted that the world should be witness to their private tragedy).

228. *See supra* notes 40–42 and accompanying text.

peoples' lives in ways that impact their life choices. Such postings draw unwanted attention to individuals, making them vulnerable to assailants who otherwise likely would not know about them. Mindful of this exposure, individuals refuse to leave their homes and change their jobs, just as the surgical patient refused to go to work after the publication of her pictures.[229] Doctors listed on the *Nuremberg Files* site wore bulletproof vests to work; many likely stopped performing abortions. Targeted individuals have explained that because online postings told assailants where to find them, they purchased alarm systems for their homes and carried baseball bats when going to their cars.[230]

Such exposure of individuals can be even more harmful than privacy invasions of the past. Whereas individuals in the past faced with public disclosures of stigmatizing private facts withdrew from society, those facing online revelations of their personal information now have been wounded and killed. Targeted individuals endure rape and assault, not just feelings that prevent them from going to work or leaving their homes.[231]

Leaking databases of information also impair people's ability to develop their inviolate personalities and shape how others see them. In releasing sensitive information to criminals, database operators prevent individuals from developing their credit histories, giving identity thieves that privilege. Just as a newspaper story of a woman's plastic surgery or of a person's debt changed how others saw them, credit scores—distorted by identity theft—impact people's reputations by impacting individuals' ability to get loans and jobs. Similarly, medical identity theft undermines people's ability to get insurance. Free from insecure databases, individuals' *own* choices would instead determine their employability, creditworthiness, and insurability.

The legal community's growing conception of the above practices as impeding privacy interests is a crucial step toward remedying their effects. Commentators have proposed innovative privacy torts to address contemporary privacy problems. Sarah Ludington, for instance, has called for a new tort of information misuse to address data leaks based on the Fair Information Practice Principles.[232] Natalie Regoli has proposed an "Internet Profiling Tort" that

229. Citron, *Law's Expressive Value*, *supra* note 23, at 385 (2009).

230. Tracy L.M. Kennedy, *An Exploratory Study of Feminist Experiences in Cyberspace*, 3 CYBERPSYCHOL. & BEHAV. 707, 716 (2000).

231. In some respects, these exposures have much in common with the gendered nature of Warren and Brandeis's approach. Just as Samuel Warren saw tort privacy as a crucial means to protect his wife from unwanted publicity, here, too, tort privacy could protect women from postings that turn them into public spectacles.

232. Sarah Ludington, *Reigning in the Data Traders: A New Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 146 (2006) (arguing that the tort would target "insecure data practices" and "the use of personal information data for purposes extraneous to the original transaction"); *see also* Jonathan Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1419, 1430 (proposing a "tort of commercial dissemination of private information").

would hold a commercial entity liable for its collection, use, or sale of personal information without informed consent.[233]

Although these proposals are creative, they might be impractical.[234] New torts can amount to unattainable first-best[235] solutions.[236] Judges may refuse to adopt new causes of action due to concerns about legitimacy[237] and reversal.[238] They may also find it hard to support new torts that require them to mark out the law's contours with little or no precedential support.

Calls for new privacy torts could eclipse second-best solutions, such as applying mainstream tort concepts to developing privacy issues.[239] According to David Hyman, "perfection is not the appropriate standard for judging real world policies and institutions. To believe otherwise is to indulge in the nirvana fallacy."[240] Just as Prosser looked to existing law to construct the four privacy

---

233. Natalie L. Regoli, Comment, *A Tort for Prying E-Eyes*, 2001 J.L. TECH. & POL'Y 267, 284; *cf*. Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L. J. 877, 892–93 (2003).

234. This is not to say that that courts or legislatures should not adopt them. Mainstream tort claims could, of course, complement these new torts in the event that legislatures or courts adopted them.

235. In economics, the defining characteristic of a first-best solution is the "attainment of a Paretian optimum" with "simultaneous fulfillment of all the optimum conditions." R.G. Lipsey & Kevin Lancaster, *The General Theory of Second Best*, 24 REV. ECON. STUD. 11, 13, 11 (1956). Put simply, first-best solutions are ones that are ideal in a perfect environment whereas second-best solutions work within environmental constraints and variables. "First-best solutions are (by definition) the most attractive, but second-best solutions fare well if they are much more realistic and give us much of what we want." Stuart Minor Benjamin and Arti K. Rai, *Who's Afraid of the APA? What the Patent System Can Learn from Administrative Law*, 95 GEO. L.J. 269, 335 (2007).

236. Lipsey & Lancaster, *supra* note 235. As Pierre Schlag explained, a realist "understands that law is always in negotiation with the world. Law is thus nearly always a second-best enterprise operating in a second-best world." Pierre Schlag, *Formalism and Realism in Ruins (Mapping the Logics of Collapse)*, 95 IOWA L. REV. 195, 210 (2009). I thank my colleague Max Stearns for his insights on this point.

237. Anita Bernstein, *How To Make a New Tort: Three Paradoxes*, 75 TEX. L. REV. 1539, 1546, 1557 (1997) (noting that proposals for a hate speech tort fell flat in part because it seemed radical and too incompatible with free speech doctrine).

238. MENAND, *supra* note 142, at 341.

239. Some scholars have already begun looking to traditional tort concepts to address the new privacy injuries. *See, e.g.*, Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 69 (2003) (arguing "that collecting and selling or leasing an extensive consumer data profile without consumer consent should be actionable under the privacy tort known as appropriation"); Litman, *supra* note 175, at 1311 (suggesting a tort-based "breach of trust approach" for data privacy protection because "[a] relational approach . . . carries significant intuitive appeal" and "its scope can easily be limited by confining the definition of a qualifying relationship"). Some scholars have also suggested borrowing from existing statutory law to prevent violations of data privacy. *See, e.g.*, Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305, 1320 (2001) (arguing that the Federal Trade Commission Act, which prohibits unfair and deceptive trade practices, "could in fact offer more informational privacy protection than the privacy torts because of the extraordinary scope given its language").

240. David A. Hyman, *Employment-Based Health Insurance and Universal Coverage: Four Things People Know That Aren't So*, 9 YALE J. HEALTH POL'Y L. & ETHICS 435, 451 (2009).

torts, courts could look to mainstream tort concepts to tackle contemporary privacy injuries. Invoking those claims would appear as "new wrinkles" on established rules rather than as radical changes in law.[241] They would permit the redress and prevention of privacy injuries while assuring courts that they were not venturing too far from precedent.[242]

Invoking traditional tort claims is a promising means to harness law's coercive and expressive value in combating privacy invasions. Although not originally designed to protect privacy interests, mainstream tort claims could evolve to do so. Courts could make clear to juries that the torts' legally protected interests include the right to privacy. As juries assessed whether defendants' interfered-with interests were protected by traditional torts, they would also consider whether and to what extent plaintiffs deserved compensation for interferences with their "right to be let alone."

In such cases, jury instructions and favorable verdicts would say to the public that a defendant's activities not only violated interests protected by traditional tort law, but those covered by privacy tort law as well. As discussed below, database operators would see that their failure to keep sensitive personal information from release into the hands of identity thieves not only constituted ultrahazardous activity, warranting strict liability and possibly a breach of confidence, but also a privacy invasion. Certain website operators—those publishing personal information alongside suggestions that individuals should be hurt—would understand their actions as interfering with those individuals' right to be "let alone" while also enabling criminal activity.

The next Sections will discuss mainstream tort claims that might be effective in deterring and remedying contemporary privacy injuries, including enablement, strict liability, and breach of confidence claims.

1. Tortious Enablement of Criminal Conduct

Certain plaintiffs should, and could, bring enablement torts against website operators whose postings of personal information interfered with the plaintiffs' right to be free from unwanted publicity. Tort law recognizes claims against actors who engage in "risk-generating behavior leading to harms caused by third-party intervening conduct."[243] Courts permit recovery in such cases because the defendant paved the way for the third party to injure another. They justify imposing liability on the enabling actor due to the deterrence gaps—the difficulty of finding and punishing the criminal in order to deter would-be

241. Bernstein, *supra* note 158, at 433.

242. Applying mainstream tort concepts has another attractive feature. It might break down the artificial wall that has separated privacy torts from the main body of tort law. This would help free privacy tort law from its neglected doctrinal niche. In turn, privacy claims might have the opportunity to take advantage of developments occurring in traditional areas of tort law.

243. Robert L. Rabin, *Enabling Torts*, 49 DEPAUL L. REV. 435, 437 n.14 (1999). Rabin argues there is little difference between inciting misconduct and enabling it. *Id.*

tortfeasors.[244] As Robert Rabin explains, negligence law's deterrence rationale would be defeated if those enabling wrongdoing can escape judgment by shifting liability to individuals who cannot be caught and thus deterred.[245]

Courts have recognized enabling torts in premises liability cases. For instance, in *Kline v. 1500 Massachusetts Avenue Apartment Corp.*,[246] the plaintiff was attacked and robbed in the hallway just outside her apartment. The landlord left the building unguarded in the face of increasing assaults and robberies perpetrated against the tenants in the apartment building's common hallways.[247] The court held that residential apartment owners had a duty to exercise reasonable care to protect tenants from third party violence.[248] It explained that the landlord had a "duty . . . to take those measures of protection which are within his power and capacity to take, and which can reasonably be expected to mitigate the risk of intruders assaulting and robbing tenants."[249] The court underscored the preventative value of creating a duty to protect against third-party violence, noting that the landlord was in a better position than the tenant to adopt precautionary measures and better situated than the police to diminish the risk of criminal assault on its premises.[250]

According to Meiring de Villiers, courts are more likely to impose liability for enabling torts when defendants create an opportunity for tortious conduct that does not exist for the wrongdoer in the "normal background of incitements and opportunities."[251] For example, in *Sun Trust Banks, Inc. v. Killebrew*, a robber shot the plaintiff at the defendant's automated teller machine (ATM) at night.[252] The court accepted the plaintiff's argument that the defendant failed to exercise due care to keep the premises safe.[253] In a concurrence, Judge Sears noted that the defendant should have foreseen the possibility of criminal activity because of the unique opportunity for such conduct that ATMs present, given their weak security and assurance of victims with money.[254]

---

244. *Id.* at 444.
245. *Id.*
246. 439 F.2d 477 (D.C. Cir. 1970).
247. *Id.* at 479.
248. *Id.* at 487.
249. *Id.*
250. *Id.* at 480. Courts have extended premises liability for a third party's criminal acts in cases involving owners of residential property, hospitals, colleges, day care centers, and shopping centers. Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1582 (2005) (arguing in favor of recognition of negligent enablement of cybercrime claims against software manufacturers for insecure software that facilitates conversion of credit card numbers, invasion of privacy, identity theft, or misappropriation of trade secrets).
251. Meiring de Villiers, *Reasonable Foreseeability in Information Security Law: A Forensic Analysis*, 30 HASTINGS COMM. & ENT. L.J. 419, 450 (2008).
252. *Id.*
253. *Id.*
254. *Id.* at 450–51.

Courts have also recognized theories of liability against those who gather or communicate information on the theory that their actions negligently, recklessly, knowingly, or purposefully facilitated criminal conduct.[255] Thus, in *Remsburg v. Docusearch*, a stalker killed a woman after obtaining the woman's work address from the defendant, a data broker.[256] The court found that the broker had a duty to exercise reasonable care in releasing information to third parties, due to the risk of criminal misconduct.[257] It held that a "where the defendant's conduct has created an unreasonable risk of criminal misconduct, a duty is owed to those foreseeably endangered."[258] The court explained that "threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client."[259] According to the court, information brokers should know that stalkers often use their services to obtain personal information about victims and that identity theft is an increasingly common risk associated with the disclosure of personal information such as an SSN.[260]

In certain instances, enablement claims ought to vindicate plaintiffs' privacy interests. In cases akin to *Nuremberg Files*, site operators should be required to compensate individuals, like the targeted doctors, for denying them their right to remain anonymous from extremists bent on murder.[261] Enablement claims could thus be used to deter site operators from disclosing personal information in ways that interfere with individuals' life choices.[262]

In such circumstances, enablement liability would also satisfy the enablement tort's traditional rationales. Website operators are the most realistic candidates for deterrence pressure as it can be difficult to find or pursue the posters.[263] Enablement liability would help deter operators, like the group

255. *See, e.g.*, Rice v. Paladin Enters., Inc., 128 F.3d 233 (4th Cir. 1997) (concluding that the publisher of a book on how to commit a contract murder could be held liable on the grounds that the book's purpose was to facilitate crime).

256. 816 A.2d 1001 (N.H. 2003).

257. *Id.* at 1007.

258. *Id.*

259. *Id.* at 1007.

260. *Id.* at 1008.

261. *See supra* notes 231–236 and accompanying text (exploring how online postings revealing personal information to potential assailants interfere with individuals' right to be let alone).

262. *Id.*

263. Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 118 (2009). As Jack Balkin explains, much speech on the Internet is anonymous and thus it may be difficult to locate the speakers. Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 434 (2009). David Robinson explains, however, that advances in computer science may help plaintiffs and prosecutors find anonymous posters. David Robinson, *Identifying John Doe: It Might Be Easier than You Think*, FREEDOM TO TINKER (Feb. 8, 2010, 8:45 AM), http://www.freedom-to-tinker.com/blog/dgr/identifying-john-doe-it-might-be-easier-you-think. Nonetheless, posters may be a poor source of deterrence as they may be judgment-proof or be difficult to find. Balkin, *supra* at 434.

running the *Nuremberg Files* website, from hosting posts encouraging and facilitating assaults on individuals. It might provide incentive for operators to remove postings once they receive notice that imposters have used their site to facilitate physical assaults. Website operators are in a better position to address the problem than the targeted individuals, who may not know about the postings and cannot take the postings down themselves.[264]

Enablement claims may, however, have limited application to privacy violations. Courts deciding these claims might require proof that website operators knew about the risk of third-party criminal conduct.[265] Website operators responsible for postings, as in the *Nuremburg Files* case, would meet this standard—they orchestrated the postings themselves.

Plaintiffs in more difficult cases might be able to satisfy this requirement by presenting evidence of similar, prior impersonations of individuals, as in the Craigslist incidents.[266] This may not go far enough, however. Because the First Amendment might require proof of intentional conduct, some courts will insist upon evidence that the website operators created the online forum with the intent to facilitate criminal conduct.[267]

Additionally, tortious enablement claims against website operators will face important statutory and constitutional obstacles. Website operators enjoy immunity from tort liability under section 230(c)(1) of the Communications Decency Act, which states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[268] Section 230 generally frees online service providers from liability related to the postings of others.[269] This safe harbor is inapplicable, however, if the website operator helps create the content enabling the criminal activity. The anti-abortion group running the *Nuremberg Files* site exemplifies a party with no immunity under section 230.

---

264. In enabling torts, the third party has not superseded causation, as that is the whole point of the tort. *See* Bell v. Bd. of Educ., 687 N.E.2d 1325 (N.Y. 1997).

265. Rustad & Koenig, *supra* note 179, at 1583.

266. A court might question whether website operators can reasonably distinguish an impersonation of a person interested in rape fantasies from someone with such a genuine interest, even if the site experienced prior incidents. For instance, a court might ask whether a heavily trafficked site such as Craigslist could readily determine if a woman posted a genuine interest in rape fantasies or if an imposter did so to encourage third parties to stalk and rape her. To address this problem, courts could examine the surrounding circumstances—such as whether the targeted individual or police contacted the website operator to take down the posting—to assess if the website operator should have foreseen its enablement of criminal activity. *See, e.g.*, Isaacs v. Huntington Mem'l Hosp., 695 P.2d 653 (Cal. 1985) (upholding a premises liability claim, where a doctor was shot in a hospital parking lot, because the attack was foreseeable given the totality of the circumstances—the high crime rate in the area, evidence of previous assaults, and the absence of security at the time of the shooting).

267. *See* notes 286–305 and accompanying text (discussing First Amendment implications of enablement claims).

268. 47 U.S.C. § 230(c)(1) (2006).

269. *Id.*

It is possible that courts will alter their interpretation to require less involvement by the website operators in creating the offending content. Recently, the Ninth Circuit refused to extend the immunity under section 230 to website operators who played some role in unlawful activity.[270] *Fair Housing Council of San Fernando Valley v. Roommates.com*[271] addressed whether the defendant, a website, lost its section 230 immunity by inducing others to violate antidiscrimination law. As part of its sign-up process, the defendant required individuals to answer questions about their gender, race, and sexual orientation.[272] The site created user profiles based on this information.[273] It also allowed users to search by various categories and to receive emails containing profiles meeting their criteria.[274] Plaintiffs argued that those questions, if asked offline, would violate antidiscrimination laws.[275]

The Ninth Circuit found that section 230 failed to immunize the defendant from liability because the defendant created the questions and choice of answers and thus became the "information content provider."[276] The court also ruled that since the site allowed users answering the defendant's questions to choose from a list of possible responses, the defendant was "the developer, at least in part, of that information."[277] The court explained that each user's profile page was partially the defendant's responsibility "because every such page is a collaborative effort between [the site] and the subscriber."[278] The court reasoned that section 230 does not grant immunity for helping third parties develop unlawful conduct.[279]

The *Roommates.com* decision could be used to extend tort liability to website operators who ask posters to detail the names and addresses of women who ought to be raped (or are interested in anonymous sex) or who urge individuals to post SSNs of others. In such cases, site operators would not enjoy immunity from enablement liability.

Most of the examples referred to in Part I do not, however, fall in this category. Website operators, such as Craigslist, would enjoy immunity under section 230 because they merely provide a space for others to post information and do not prompt posters to reveal specific information. Although courts could extend the *Roommates.com* approach to cover website operators who knowingly display posts that induce criminal conduct, none have done so to

270. Fair Hous. Council v. Roommates.com, 521 F.3d 1157 (9th Cir. 2008).
271. *Id.* at 1161–62.
272. *Id.* at 1161.
273. *Id.* at 1162.
274. *Id.*
275. *Id.* at 1167.
276. *Id.* at 1165.
277. *Id.* at 1166.
278. *Id.* at 1167.
279. *Id.* at 1167–68.

date.[280]

The recognition of enablement claims as a protection against privacy invasion also raises free speech concerns. The First Amendment, like section 230, would immunize some website owners against enablement claims. In *Brandenberg v. Ohio*,[281] the Supreme Court held that abstract advocacy of lawlessness is protected speech under the First Amendment unless it is intended to, and is likely to produce, specific imminent lawless action.[282] There, the Court deemed Ku Klux Klan speech "mere advocacy" because it never targeted a specific group at a specific time but instead expressed generalized ill will toward various groups.[283] Applying this standard, the Court, in *NAACP v. Claiborne Hardware Co.*, held that even though the Field Secretary of the National NAACP stated in a speech that "[i]f we catch you going in any of them racist stores, we're gonna break your . . . neck," [284] the NAACP was not liable for acts done by "enforcers" of a boycott in Claiborne County, Mississippi. The Court reasoned that, in context, the statement constituted hyperbole.[285] Some speech found on websites may fall under this same protection.

Although speech that advocates lawlessness has enjoyed protection under the First Amendment, it is well established that "aiding and abetting" speech can be proscribed.[286] In *Rice v. Palladin Press Enterprises*,[287] for instance, the defendant published *Hit Man*, a book purporting to instruct would-be assassins.[288] The publisher was sued after one of its readers killed three individuals following the book's instructions.[289] The Fourth Circuit found that the publisher could be held civilly liable for "aiding and abetting" a crime.[290] It ruled that the book constituted "instructional speech" that differed from abstract

280. *See* Note, *Badging: Section 230 Immunity in a Web 2.0 World*, 123 HARV. L. REV. 981, 986 (2010) (noting that decisions after *Roommates.com* have preserved section 230 immunity and limited *Roommates.com* to its facts). Scholars argue that Congress ought to amend section 230 to deny website operators immunity if they enable criminal activity, such as cyber harassment. *See, e.g.*, Nancy S. Kim, *Web Site Proprietorship and Online Harassment*, 2009 UTAH L. REV. 993. John Palfrey and Urs Gasser contend that there is no reason why a social network site "should be protected from liability related to the safety of young people simply because its business operates online." JOHN PALFREY & URS GASSER, BORN DIGITAL 107 (2008). Any change in section 230 would, of course, come at a price to free expression online. Balkin, *supra* note 263, at 434–35 (explaining that intermediary liability would produce a phenomenon called collateral censorship); Eric Goldman, *Unregulating Online Harassment*, 87 DENV. U. L. REV. 59 (2010).

281. 395 U.S. 444 (1969) (per curiam).

282. *Id.* at 447–48.

283. *Id.* at 448–49.

284. 458 U.S. 886, 902, *reh'g denied*, 459 U.S. 898 (1982).

285. *Id.* at 931.

286. Randall P. Bezanson & Gilbert Cranberg, *Institutional Reckless Disregard for Truth in Public Defamation Actions Against the Press*, 90 IOWA L. REV. 887, 910 (2005).

287. 128 F.3d 233 (4th Cir. 1997).

288. *Id.* at 239–40.

289. *Id.* at 241.

290. *Id.* at 244.

incitement of lawlessness protected by the First Amendment.[291] The court reasoned that because the manual directly assisted the hit man, the criminal activity and expression could not be separated. In essence, the writing was used as an integral part of a crime sufficient to find the author liable.[292]

The court in *Rice* explained that the First Amendment may, in some circumstances, impose a heightened intent requirement to prevent the punishment of innocent, lawfully useful speech.[293] It suggested that the First Amendment might bar liability based on "mere foreseeability or knowledge that the information one imparts could be misused for an impermissible purpose."[294] For the court, such a limitation "would meet the quite legitimate, if not compelling, concern of those who publish, broadcast, or distribute to large, undifferentiated audiences, that the exposure to suit under lesser standards would be intolerable."[295] The court reasoned that "it would not relieve from liability those who would, for profit or other motive, intentionally assist and encourage crime and then shamelessly seek refuge in the sanctuary of the First Amendment."[296] It hypothesized that the First Amendment would not protect the publication on the Internet of "the necessary plans and instructions for assassinating the President" with the specific, indeed even the admitted, purpose of assisting such crimes.[297]

As Eugene Volokh explains, several courts have held that speech that intentionally facilitates crime is constitutionally unprotected.[298] Three courts have ruled that speech that knowingly facilitates crimes is constitutionally unprotected.[299] Meanwhile, three others have found that a newspaper does not have a First Amendment right to publish a witness's name where such publication might facilitate crimes against the witness. Apparently, these courts would find this way even if no evidence suggested that the newspaper intended to facilitate such crime.[300] Two other courts would only find liability for such claims if the *Brandenberg* incitement test was satisfied.[301]

Much like the result under section 230, website operators like the one running the *Nuremberg Files* would not enjoy immunity from liability on free

291. *Id.* at 244–45.
292. *Id.* at 246–47.
293. *Id.* at 247.
294. *Id.*
295. *Id.*
296. *Id.* at 248.
297. *Id.*
298. Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095, 1129 (2005). I am grateful to Eugene Volokh for discussing with me the First Amendment concerns that these cases raise.
299. *Id.*
300. *Id.* at 1130; Brandenberg v. Ohio, 395 U.S. 444, 447–48 (1969) (finding that abstract advocacy of lawlessness is protected speech under the First Amendment unless it is intended to, and is likely to produce, specific imminent lawless action).
301. *Id.*; *see also Brandenberg*, 395 U.S. 444.

speech grounds. Although the Ninth Circuit upheld a lawsuit against the *Nuremberg Files* operators because the site's postings constituted unprotected threats,[302] it might have done so on the grounds that the site operator intended to facilitate violence against the abortion providers. Given the majority's finding that that the postings sent the message that "You're Wanted or You're Guilty; You'll be shot or killed"[303] in light of the prior murders of doctors appearing in Wanted posters, it might have found not just an intent to threaten, but also an intent to facilitate murder.[304]

On the other hand, courts may immunize from liability website operators like Craigslist who do not intentionally "aid and abet" crimes such as impersonation, rape, assault, and stalking. They might find, as did the *Rice* court in dicta, that upholding enablement claims on negligent, reckless, or knowing conduct would chill legitimate speech by encouraging operators to take down genuine assertions by individuals interested in "rape fantasies" and the like. Thus, enablement claims premised on theories of negligence or recklessness may be invalid on the grounds of both free speech and section 230.[305]

---

302. As the Supreme Court held in *Virginia v. Black*, threats fall outside the First Amendment's protection if speakers mean to communicate a serious intention to commit an act of unlawful violence against particular individuals. 538 U.S. 343 (2003). "The speaker need not actually intend" to commit a violent act because the prohibition of threats "'protect[s] individuals from the fear of violence' and 'from the disruption that fear engenders.'" *Id.* at 359–60 (quoting *R.A.V. v. City of St. Paul*, 505 U.S. 377, 388 (1992)). In *Planned Parenthood of Columbia/Willamette v. American Coalition of Life Activists*, the Ninth Circuit found that the First Amendment did not bar abortion providers' lawsuit against the *Nuremberg Files* website operators because the portion of the site listing abortion doctors' home addresses went "well beyond the political message." 290 F.3d 1058, 1079 (9th Cir. 2002) (en banc). The court determined that the site constituted unprotected threats because, even though it contained no explicitly threatening language, it sent the implied message: "You're Wanted or You're Guilty; You'll be shot or killed" given the prior murders of doctors appearing in Wanted posters. *Id.* The *Planned Parenthood* court was strongly divided, with the majority emphasizing the difference between intimidation by threat and general advocacy of lawlessness. *Id.* at 1071–72.

303. *Planned Parenthood*, 290 F.3d at 1085.

304. *Id.* at 1079–80. Eugene Volokh has argued that some speakers do not have the "conscious object" or the "aim" of producing crime. Volokh, *supra* note 298, at 1182. The "deeper motive . . . is generally ideological, at least setting aside speech said to a few confederates in a criminal scheme." *Id.* Speakers, in his view, "rarely want unknown strangers to commit a crime unless the crime furthers the speaker's political agenda." *Id.*

305. Volokh has generally opposed legal liability for crime-facilitating speech. Although such information can be used to commit crimes, it provides information that can be used for lawful purposes. Volokh, *supra* note 298, at 1146. In his view, liability for crime-facilitating speech should be permitted only in a few instances, such as where the speech communicates facts that have very few lawful uses, such as the publication of SSNs and computer passwords, because it is both crime-facilitating and has nearly no value beyond its facilitation of a crime. *Id.* Any valuable use of such information—alerting others of a security problem—can be accomplished in less harm-facilitating ways, such as releasing parts of passwords. *Id.* Under Volokh's analysis, websites hosting SSNs would not be immune from enablement liability, yet sites such as Craigslist would be protected from liability given the risk that legitimate posts about people's sexual fantasies could be chilled.

2. Strict Liability

The strict-liability rule of *Rylands v. Fletcher* also offers a promising means to address privacy invasions resulting from databases leaking sensitive personal information. *Rylands* involved an industrial accident: the flooding of plaintiff's coal mines after water escaped the reservoir of the neighboring textile mill, which had been built by a contractor.[306] The operator of the coal mine sued the reservoir owner in the Court of the Exchequer and lost.[307] On appeal, the Exchequer Chamber judges found the reservoir owner liable without fault.[308] The House of Lords affirmed. The rule that emerged from *Rylands* is that a person who "brings on his land and collects and keeps there anything likely to do mischief if it escapes" must pay for all of the damage that is "the natural consequence of its escape."[309]

Strict liability claims would require database operators to provide redress for privacy invasions resulting from the unwanted "escape" of people's sensitive personal information into the hands of identity thieves. Leaking databases deny people the right to limit who has access to their SSNs, birth dates, medical insurance information, and the like. They interfere with people's ability to develop their inviolate personalities free from identity theft and insurance fraud.[310]

Moreover, insecure databases impact people's sense of self.[311] Rather than seeing themselves as self-directing agents, victims of database leaks perceive themselves as ends to others' means. This is surely true for the countless individuals who are denied work and loans due to compromised credit histories caused by identity theft.[312] Strict liability claims could potentially provide compensation for such interference with individuals' right to privacy.

A *Rylands v. Fletcher* strict-liability approach would also address traditional tort goals of deterrence. In my previous work, I have argued that

306. Rylands v. Fletcher, [1865] 159 Eng. Rep. 737, 739–40 (L.R. Exch.).

307. *Id.* at 744.

308. Fletcher v. Rylands, [1866] 1 L.R. Exch. 265, 278.

309. Rylands v. Fletcher, [1868] 3 L.R.E. & I. App. 330, 339, 340 (H.L.).

310. *See supra* p. 230 (discussing how leaking databases of personal information interfere with individuals' right to privacy).

311. *See* Henry, *supra* note 220 (proposing that being treated in an undignified manner damages a person's self respect).

312. *See infra* text accompanying notes (discussing ChoicePoint incident). Courts have recognized individuals' privacy interest in their Social Security numbers. *See, e.g.*, Greidinger v. Davis, 988 F.2d 1344, 1353 (4th Cir. 1993) ("[A]rmed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain the person's paycheck"). Congress, too, has recognized that the disclosure of SSNs raises serious privacy concerns. *See* Freedom of Information Act, 5 U.S.C. § 552(b)(6) (2006) (interpreting Exemption 6 of FOIA to forbid the disclosure of SSNs); Driver Privacy Protection Act, 18 U.S.C. §§ 2721–23 (barring states from disclosing "personal information," including SSNs, contained in motor vehicle licensing records).

Rylands v. Fletcher provides a powerful metaphor for understanding economically valuable, yet risky, technologies—like databases of sensitive personal information.[313] Metaphors have long had a profound impact on the way scholars and judges conceptualize problems.[314] Although *Rylands* responded to the damage caused by bursting dams and other similar hazards at the dawn of the industrial age, it also produced a metaphor for economically valuable, yet risky, technologies—a dynamic reservoir, amassing enormous power that provides great value if kept in check, but, if let loose (as is inevitable), could wreak havoc on innocent people not involved in the enterprise.[315]

Rylands provides a potent metaphor to conceptualize the characteristic risks of new technologies at the dawn of the information age. Just as water in a reservoir is safe inside its confines, sensitive personal information inside computer databases is harmless if it remains inert. Now, as then, it is the uncontrolled release of the collected material—in this instance, personal identifying data—that wreaks havoc on innocent people not involved in the enterprise.[316] Moreover, recognizing *Rylands* strict-liability claims against database operators would comport with noted contemporary tort theories.[317] Notably, the efficient deterrence theory of Guido Calabresi[318] and the fairness theory of Gregory Keating both support a strict liability approach to leaking databases of sensitive personal information.[319]

313. Citron, *Reservoirs of Danger*, *supra* note 19, at 283–94 (2007). Because my previous work provided a detailed analysis of the importance of using *Rylands* as a metaphor and how contemporary tort theories might support a strict-liability approach to data leaks, I provide a brief summary of some of my main points, hoping that interested readers turn to that piece for my fully developed arguments on the matter.

314. *Id.* at 278.

315. *Id.*

316. *Id.*

317. *Id.* at 283–92.

318. Calabresi's efficient deterrence theory argues that tort law should minimize the costs of accidents, including the costs of avoiding accidents. GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 26 (1970). It would attach liability to the "cheapest cost avoider"—the party best suited to make the cost-benefit analysis between accident costs and accident avoidance costs and to act on that analysis. *Id.* at 26–29. Under this theory, database operators constitute the cheapest cost avoiders as compared to individuals whose information sits in a private entity's database. Because database operators have distinct informational advantages about vulnerabilities in their computer networks, they sit in the best position to make decisions about the costs and benefits of their information collection practices.

319. Gregory Keating's fairness theory also supports a strict-liability solution to leaking databases. Fairness theory provides the "moral logic" for treating strict enterprise liability as the modern default rule for tort law. Gregory C. Keating, *Distributive and Corrective Justice in the Tort Law of Accidents*, 74 S. CAL. L. REV. 193, 202 (2000). It requires an enterprise to compensate individuals injured by its risky, yet profitable, activities if the victim does not benefit from those activities to the same extent that the enterprise does. *Id.* Strict liability exacts a "just price" for an enterprise's freedom to engage in profitable activities where the victim did not similarly enjoy such a liberty but nonetheless suffered injury. *See* Gregory C. Keating, *Rawlsian Fairness and Regime Choice in the Law of Accidents*, 72 FORDHAM L. REV. 1857, 1891 (2004).

It is not clear whether Prosser would have approved the application of a strict liability approach to leaking databases of personal information. But his work as the Reporter for the *Second Restatement of Torts* provides important clues to that answer. Section 520 of the *Second Restatement* addressed the strict liability standard for abnormally dangerous activities.[320] It identified several factors that suggest the existence of abnormally dangerous activities, including: the high degree of risk of some harm to people, land, or chattels of others; the inability to eliminate the risk by the exercise of reasonable care; and the extent to which the activity's value to the community is outweighed by its dangerous attributes.[321] The essential question was "whether the risk created is so unusual, either because of its magnitude or because of the circumstances surrounding it, as to justify the imposition of strict liability for the harm that results from it, even though it is carried on with reasonable care."[322] The *Second Restatement* did not limit strict liability to cases involving land.[323]

Leaking cyber-reservoirs arguably constitute an abnormally dangerous activity under Prosser's standard. They constitute high-utility activities with significant residual risk regardless of the care taken by database operators.[324] Security breaches are an inevitable byproduct of collecting sensitive personal information in computer databases.[325] No amount of due care will prevent a significant amount of sensitive data from escaping into the hands of cyber-criminals.[326] Such cyber reservoirs are also abnormally dangerous due to the magnitude of the risk involved. A single data leak can involve the release of millions of Social Security numbers and other personal information into the hands of identity thieves.[327]

Under Keating's fairness theory, private entities enjoy appreciable profit-making freedoms, such as gains from the sale of personal information, enhanced workplace efficiency, and a means to solicit customers in collecting personal data. On balance, the degree of benefit to individuals whose information is collected is not matched by the detriment they suffer upon the release of their information. Placing liability on the database operator would fairly distribute the costs of the release of sensitive data and equalize the burdens and benefits of profitable cyber reservoirs of information.

320. RESTATEMENT (SECOND) OF TORTS §§ 519, 520 (1977).

321. *Id.* § 520.

322. *Id.* § 520 cmt. f.

323. *Id.* § 520 cmt. e. The *Third Restatement of Torts* defines abnormally dangerous activity as creating a foreseeable and highly significant risk of physical harm even when reasonable care is exercised by all actors and the activity is not one of common usage. RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL HARM § 20 (2005). Although cyber reservoirs fall outside this definition because they do not cause physical harm, they nonetheless share defining characteristics of abnormally dangerous activities like blasting and water reservoirs—high utility and high risk.

324. Citron, *Reservoirs of Danger*, *supra* note 19, at 265.

325. LAWRENCE A. GORDON ET AL., COMPUTER SECURITY INSTITUTE, 2005 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 11 (2005), *available at* http://www.cppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf.

326. Citron, *Reservoirs of Danger*, *supra* note 19, at 265.

327. Prosser did note, in 1953, that *Rylands* should be restricted to activities that were

Prosser's response to the changing nature of injuries in the twentieth century also provides insight as to how he would have responded to today's cyber reservoirs. When the source of injuries shifted from industrial accidents to mass consumer harms, Prosser supported an extension of strict liability to products.[328] The source of injuries has again changed, this time from mass consumer harms to financial vulnerabilities connected to the release of sensitive personal data. Prosser might very well have responded to this shift as he did for strict products liability—by supporting the application of *Rylands v. Fletcher* to leaking databases of personal information.

As a practical matter, strict liability claims might be limited to cases where plaintiffs have suffered actual financial harm. Courts have dismissed negligence claims in cases involving data breaches where plaintiffs identify the *threat* of identity theft and the cost of credit monitoring as their injury on the grounds that the harm is too speculative.[329] Nonetheless, an important argument exists that the cost to monitor one's credit—combined with the emotional, physical, and financial harm associated with the mental distress accompanying the threat of identity theft—amounts to a tangible, compensable harm.[330] Credit monitoring damages share a similar rationale to awards of medical monitoring in toxic exposure cases.[331] Just as individuals exposed to toxins face the risk of

foreign to the community and inappropriate to its location. WILLIAM L. PROSSER, *The Principle of* Rylands v. Fletcher, *in* THE THOMAS M. COOLEY LECTURES: SELECTED TOPICS ON THE LAW OF TORTS 185, 187 (1953). He wrote that *Rylands* should apply only in cases resembling "a pig in the parlor"—something unexpected and inappropriate to the surrounding circumstances. *Id.* The *Second Restatement*, however, does not deem this factor as dispositive for abnormally dangerous activities, instead looking to an amalgam of concerns listed in section 520. RESTATEMENT (SECOND) OF TORTS § 520 (1977).

328. *See* John C.P. Goldberg, *The Constitutional Status of Tort Law: Due Process and the Right to a Law for the Redress of Wrongs*, 115 YALE L.J. 524, 582 (2006) (discussing Prosser's role in promoting strict products liability as Reporter of the Second Restatement of Torts).

329. Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 7–8 (D.D.C. 2007); *cf.* Kahle v. Litton Loan Servicing LP, 486 F. Supp. 2d 705, 709–10 (S.D. Ohio 2007) (ruling that plaintiffs lacked standing to sue in data breach cases due to lack of imminent or actual injury, such as identity theft). The economic loss rule likely would not bar recovery for the costs associated with identity theft and monitoring one's credit. As Robert Rhee explains, the economic loss rule applies where parties involved are strangers and the injury is not foreseeable. Robert J. Rhee, *A Production Theory of Pure Economic Loss*, 104 NW. U. L. REV. 49 (2010). It covers instances where liability would be too indeterminate and administratively difficult to sort out and where contracts would more efficiently address the issue. *Id.* In this vein, Vincent Johnson contends that economic loss principles do not apply to data breach cases because the expenses associated with identity theft and credit monitoring are susceptible to proof with a "high degree of certainty" and because rights related to the protection of personal data are not proper subjects of bargaining. Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 298–301 (2006). Moreover, it would be an absurdity to dismiss negligence claims in data breach cases due to the lack of actual economic injuries such as identity theft, as courts do and yet insist that the economic loss rule applies.

330. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 15, at 177.

331. Johnson, *supra* note 329, at 308.

future harm, so, too, do victims of data breaches.[332] Much like victims of toxic spills, those subject to a data breach are in a better position to address the risk of identity theft than the database operator.[333]

Some may raise concerns that a strict liability approach would bankrupt defendants as massive data leaks could involve enough individuals to put companies out of business. However, a system of fixed tort fines could be created to address leaking databases and keep damages from spiraling out of control.[334] Possible actions include a uniform act adopted by all of the states or congressional legislation—assuming leaks, at least in Internet databases, substantially affect interstate commerce. Congress could require that fines for such leaks hinge upon the size of the firm and the number of people affected. Such limitations might dispel concerns that a strict liability would force data collection firms into bankruptcy.

3. Duty of Confidence

Neil Richards and Daniel Solove make an important case for importing breach of confidence doctrine into privacy tort law.[335] They point to the common law's protection of the exchange of information in particular professional and contractual relationships.[336] Confidence law also applies to certain communications, such as mail and telegrams.[337]

Confidence law is an underutilized resource for today's privacy problems.[338] It should be invoked to remedy and deter defendants' interference with plaintiffs' right to be let alone in cases where parties have a relationship warranting confidence.[339] Breach of confidence claims could be used to provide compensation for unwanted disclosures of personal information. They could repair and deter invasions of privacy interests in much the same way that strict

---

332. *Id.*

333. *Id.*

334. Stanley Ingber, *Rethinking Intangible Injuries: A Focus on Remedy*, 73 CALIF. L. REV. 772, 852 (1985).

335. Richards & Solove, *Privacy's Other Path*, *supra* note 172; *see also* Susan M. Gilles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy*, 43 BUFF. L. REV. 1, 61 (1995) (discussing a "breach of confidence" tort that would "impose a duty of confidence on novel relationships without the need to explain why the other duties that typically attach to a true fiduciary relation are not triggered"), Randall P. Bezanson, *The Right To Privacy Revisited: Privacy, News, and Social Change, 1890–1990*, 80 CALIF. L. REV. 1133, 1174 (1992) ("I suggest that the privacy tort be formally interred, and that we look to the concept of breach of confidence to provide legally enforceable protection from dissemination of identified types of personal information.").

336. Richards & Solove, *Privacy's Other Path*, *supra* note 172, at 140–45.

337. *Id.*

338. *Id.* at 158. Richards and Solove point to English law for helpful developments in the breach of confidence tort. *Id.* at 162–73.

339. Courts would determine confidence law's applicability by assessing the nature of the relationship between parties and the norms by which they handle each other's personal information. *Id.* at 174.

liability claims would.[340]

The utility of the breach of confidence tort in protecting privacy can easily be demonstrated in the employment context. Suppose an employer failed to secure its information systems, permitting a hacker to obtain an employee's SSN and medical information. Because the employer interfered with the employee's interest in keeping her sensitive personal information from criminals in violation of a trusted relationship, the breach of confidence tort would both redress and prevent further violations of the interests protected by confidence law, as well as the employee's right to privacy.[341] It would provide compensation in cases that are all too common today—where estranged husbands and wives reveal online their spouses' sensitive personal information that might be known to their circle of family and friends but not to employers, future social contacts, and the like.[342] Breach of confidence claims would compensate and deter unwanted disclosures of personal information that interfere with individuals' ability to develop their inviolate personalities.

Breach of confidence law can vindicate privacy interests while offering significant practical advantages over the four privacy torts.[343] It does not require plaintiffs to demonstrate that information has been publicized or that the disclosure would be "'highly offensive to a reasonable person.'"[344] Whereas the public disclosure tort "focuses on the *content*, rather than the *source* of the information," the breach of confidence tort focuses on the source and protects confidential information "without regard to the degree of its offensiveness."[345] It can provide relief even when information is spread only to a few others.[346] The breach of confidence tort also does not raise free speech concerns in the same manner as the public disclosure tort.[347] According to Randall Bezanson, a confidentiality approach is preferable to privacy tort law because it is

340. *See supra* notes 318, 319 and accompanying text (discussing the ways that strict liability claims could provide compensation for and deter invasions of individuals' right to privacy).

341. In such a case, privacy tort law would not apply because the employer only disclosed the personal information to a few people. *See supra* notes 182, 190 (discussing limits of public disclosure tort).

342. *See* Leanne Italie, *Oversharing on Facebook a Boon to Divorce Lawyers*, HUFFINGTON POST, June 28, 2010, http://www.huffingtonpost.com/2010/06/29/facebook-overshares-a-boo_n_628940.html.

343. Richards & Solove, *Privacy's Other Path*, *supra* note 172, at 174.

344. *Id.* at 175 (quoting Restatement (Second) of Torts §§ 652B, 652D, 652E (1977)).

345. McCormick v. England, 494 S.E.2d 431, 438 (S.C. Ct. App. 1997) (emphasis in original).

346. Richards & Solove, *Privacy's Other Path*, *supra* note 172, at 176.

347. *Id.* As Richards and Solove have argued, because the gravamen of the breach of confidence tort is the violation of an established relationship, the tort does not raise free speech concerns in the same manner as do privacy torts, such as public disclosure of private fact. Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650, 1670 (2009).

susceptible to consistent and principled application.[348]

A confidentiality approach, however, has important limits. Because it requires the existence of a relationship to which it is reasonable to impose duties of confidence, it would likely not apply to data brokers and others who lack a relationship with individuals whose information they release.[349] For instance, it would not address privacy injuries caused by data brokers or website operators who have no relationship with the individuals whose information they collect or post.

B. Redressing Traditional Privacy Injuries in the Twenty-First Century

Aside from widening the sphere of Prosser's taxonomy to include mainstream torts, there are other ways in which privacy tort law could expand to meet the needs of today's exacerbated harms. This might involve altering Prosser's existing torts by changing the burden of proof. Privacy torts have long required demanding proof to ensure that plaintiffs cannot recover for the "merely unpleasant aspects of human interpersonal relationships."[350]

In important respects, today's privacy problems dispel concerns that plaintiffs would recover for trivialities. Public disclosures online are more lasting and destructive than ever before. They often create an "indelible blemish on a person's identity."[351] Although people may attempt to respond to damaging disclosures in other posts, many may not see them, leaving the destructive bits in the forefront.

Given the exacerbated nature of privacy injuries in our networked age, Erwin Chemerinsky has called for changes to revive the public disclosure tort.[352] A possibility in public disclosure cases would be to require proof that a defendant's conduct was "offensive to the reasonable person," instead of "highly offensive to the reasonable person." The *Restatement of Torts* only demanded that privacy plaintiffs demonstrate that a defendant's conduct would be "offensive" to the reasonable person.[353] Adopting one of these weaker

348. Bezanson, *supra* note 120, at 1174.

349. Richards & Solove, *Privacy's Other Path*, *supra* note 172, at 178.

350. Munley v. ISC Fin. House, Inc., 584 P.2d 1336, 1338 (Okla. 1978); Kalven, *supra* note 24, at 338 (viewing privacy plaintiffs as having "shabby, unseemly grievances and an interest in exploitation").

351. SOLOVE, THE FUTURE OF REPUTATION, *supra* note 20, at 94.

352. Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L.J. 645 (2007).

353. RESTATEMENT OF TORTS § 867 cmt. d (1939). Under that standard, courts routinely dismissed privacy actions on the grounds that the publicly released information would not offend the person of ordinary sensibilities. Gill v. Hearst Pub. Co., 253 P.2d 441, 445 (Cal. 1953). That approach got even more restrictive while Prosser served as the Reporter for the *Second Restatement of Torts*, which required proof that the conduct be "highly offensive to the reasonable person." RESTATEMENT (SECOND) OF TORTS § 652D (1977). This accorded with Prosser's criticism of the privacy tort law's failure to require proof of extreme outrage and serious mental harm attested by physical illness. Prosser, *supra* note 8, at 422. He argued that because privacy

standards of proof could enable recovery in cases that might otherwise not seem sufficiently embarrassing, even though they engender serious harm in our networked age.[354]

Such a move would, however, raise significant free speech concerns. A strong argument exists that even with the public disclosure tort's newsworthiness requirement, allowing liability for merely "offensive conduct" would prevent individuals from expressing legitimate criticism about others' personal lives. The "highly offensive" standard, when coupled with the newsworthiness inquiry, arguably secures an important amount of breathing space for discourse about facts in which the public has an interest.[355]

Perhaps courts could avoid rewriting the standard of proof required for privacy torts by considering the Internet's magnifying and distorting impact in assessing such claims. For instance, courts might find that the persistence of online disclosures would satisfy the "highly offensive to the reasonable person" standard. This would not be unusual: in the defamation context, law has recognized that the longevity of damaging information deepens its destructive power. For instance, plaintiffs asserting libel claims (defamation accomplished in writing) need not prove damages whereas those bringing slander claims (defamation accomplished in spoken word) do. Courts treat libel and slander differently based on the assumption that the more permanent the damaging statements, the more harmful they are.

Moreover, courts could apply the four privacy torts to privacy harms caused by newer technologies with an eye toward the goals sought by Warren and Brandeis. This might enable courts to shed some of the rigidity that has prevented privacy torts from tackling privacy injuries accomplished over digital networks. For instance, courts might move beyond their narrow conception of "private" information.[356] Rather than reflexively dismissing public disclosure claims on the grounds that plaintiffs revealed personal information to others, courts might consider such sharing in light of Warren and Brandeis's aim to

---

tort claims sought recovery for emotional distress, they ought to demand the same proof as intentional infliction of emotional distress claims. *Id.*

354. Another possibility would be to eliminate the intent requirement. As Warren and Brandeis suggested, "[t]he invasion of the privacy that is to be protected is equally complete and equally injurious, whether the motives by which the speaker or writer was actuated are, taken by themselves, culpable or not." Warren & Brandeis, *supra* note 1, at 218.

355. Eugene Volokh has argued that the public disclosure tort, in its current form, does not go far enough to protect free speech concerns. 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, 1091 (2000). He contends that "[e]ven offensive, outrageous, disrespectful, and dignity-assaulting speech is constitutionally protected." *Id.* at 1113. In his view, one's reputation should primarily be molded by truthful information, rather than shaped inaccurately through legal coercion to keep certain details from becoming public. *Id.* Daniel Solove offers a different view. *See* Solove, *The Virtues of Knowing Less*, *supra* note 201, at 1030.

356. *See* note 211 and accompanying text (discussing how narrow interpretation of the meaning of private information has precluded privacy claims despite significant risks faced by plaintiffs in a networked environment).

protect individuals' right to be "let alone." While courts should not ignore their past rulings on the scope of privacy tort law, they nonetheless could infuse their approach with contemporary expectations about privacy in an age when individuals share sensitive personal information with trusted social networks.[357]

Consider a hypothetical student who shares intimate information with a hundred friends on the popular social network site Facebook. The student has set the site's privacy settings so only friends can view his photographs, wall musings, and daily updates. The student suffers from a genetic disorder, which he often discusses with his Facebook friends. Quite unexpectedly, the student's Facebook friend blogs about the student's genetic disorder and reveals other personal information about him as well.[358] Under current law, the student likely could not sue for public disclosure as his sharing of the information with his Facebook friends meant it was no longer private. Yet if the court considered Warren and Brandeis's broader conception of the right to be "let alone" from unwanted disclosures, perhaps privacy tort law might consider contemporary expectations about information sharing within trusted networks online.

Of course, this is but one example. Privacy torts could be infused with the lessons of Warren and Brandeis's right to privacy in various ways. Doing so might allow privacy torts to adapt to the evolving challenges that we face in our networked age while honoring the legally protected interests at the heart of privacy tort law.

CONCLUSION

Although the modern privacy torts, as currently understood, often do not address many contemporary privacy injuries, it is fruitful to continue the project that Warren and Brandeis spearheaded and that Prosser developed. To that end, courts and legislatures could take cues from privacy tort law's intellectual history to ensure its continued vitality. They could employ Warren and Brandeis's conception of the privacy torts' legally protected interest—the protection of the individual's inviolate personality by limiting unwanted disclosures of personal information—while recognizing, as Prosser did, the persuasive power of precedent.

While I have discussed a number of mainstream tort remedies, my suggestions are preliminary. In the end, privacy tort law may need wholesale renovation to address privacy injuries in the information age. It remains, however, valuable to consider the ways that we can use existing tort remedies to redress and prevent privacy invasions and to consider the impact of digital networks on privacy harms in suits involving the four privacy torts.

---

357. In assessing the right to be let alone, courts would wisely look to Lior Strahelivitz's social network theory to determine if, in that context, plaintiffs should have expected that their confidantes would have told others. Strahilevitz, *supra* note 198.

358. For a superb analysis of privacy challenges posted by social media and suggestions to face them, see James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009).