2021

If You Don't Care, Who Will?

Chad J. Pomeroy
St. Mary's University School of Law, cpomeroy@stmarytx.edu

IF YOU DON'T CARE, WHO WILL?

*Chad J. Pomeroy**

You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every moment scrutinized.[1]

I. INTRODUCTION

As a property law professor, I have lately found myself thinking a lot about privacy rights. Initially, the two topics (property and privacy) perhaps do not seem closely related, but I think they are—or, at least, I think the tie between the two is becoming much more pronounced and important, as modern life becomes ever more techno-centric.[2] I have previously written about a particular aspect of this intersectionality,[3] but I think the relationship is broader and stronger than I suspected at the time, given the ubiquity of electronic communication in contemporaneous society and the concomitant deprivation of privacy.[4]

More specifically, I think that privacy rights are, at this point, essentially an outgrowth of property rights. That is, one's right to privacy is dependent on what we traditionally view as one's property rights.[5] At least, I think this is the current state of the law, given the extent to which behemoth tech companies have created and dominated modern communication—and the ability and right to profit from that communication—and have almost wholly eliminated all traditional

---

* Turcotte R.C. Professor of Law, St. Mary's University School of Law.

1. GEORGE ORWELL, NINETEEN EIGHTY-FOUR 3 (1949).

2. *See* Emily A. Vogels, *Millennials Stand Out for Their Technology Use, but Older Generations Also Embrace Digital Life*, PEW RSCH. CTR. (Sept. 9, 2019), https://www.pewresearch.org/fact-tank/2019/09/09/us-generations-technology-use.

3. *See* Chad J. Pomeroy, *All Your Air Right Are Belong to Us*, 13 NW. J. TECH. & INTELL. PROP. 277, 283-84, 293 (2015).

4. *See* Patricia Sánchez Abril et al., *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 AM. BUS. L.J. 63, 96-97, 111 (2012) (stating that millennials do not hesitate much when it comes to sharing information that some might consider private, as indicated by their "copious digital dossiers").

5. *See* Chad J. Pomeroy, *Why Is Property So Hard?*, 65 RUTGERS L. REV. 505, 521 (2013).

concepts of privacy and rights thereto.[6] In gross, this loss of privacy is fairly momentous and overt. In practice, though, it is almost insidious. While we understand and perceive it on a broad scale, it seems almost accidental or inevitable, as applied to our emails, texts, posts, searches, and so on—to all the various pieces that make up one's life in the current moment.[7] I perceive in this disconnect between what has happened to our privacy rights and how little we seem to have noted the loss, as it was happening, the solidification of the connection between privacy and property.

That is, we can only have suffered such a massive loss of traditional rights by *giving* them away.[8] We look at our current lives—every internet search noted and studied, every photograph analyzed and sold, every word overheard by Alexa or Siri—in amazement, perhaps. But none of this is a surprise. None of this is not volitional. None of this involves some company taking something from us—it is, all of it, an abandonment of rights.[9] And it is in this abandonment that we see the firm foundation between privacy rights and property rights, as filtered by the standard of reasonable expectations.

This connection may have ever been thus. However, I do not think it has always been very well understood, as the concept of privacy rights has traditionally been a little hard to pin down.[10] This Article seeks to clarify modern privacy rights by making the connection between property and privacy clear.[11] It also seeks to use that connection to make some related predictions and suggestions about how to remediate some of the current social losses of privacy, should society decide that is desirable.[12]

It starts, in Part II, by setting the foundation for this discussion by noting just a few of the ways in which privacy has eroded over the last

---

6. *See* Allum Bokhari, *Who Is in Control? The Need to Rein in Big Tech*, IMPRIMIS (Jan. 2021), https://imprimis.hillsdale.edu/control-need-rein-big-tech.

7. The analogy that springs to mind, of course, is that of the boiling frog. If a frog is thrown into boiling water, it will jump out—but if the same frog is put into mild water, which is then slowly brought to a boil, it tepidly accepts its fate unto death. Eugene Volokh, *The Mechanisms of the Slippery Slope*, 116 HARV. L. REV. 1026, 1105 (2003). Ask yourself: if someone had told you, twenty years ago, that you would grant ownership rights of the pictures, videos, and stories you write of your lover, spouse, kids, and friends to a multi-billion-dollar conglomerate based out of California, what would you have said?

8. *See* JESSE DUKEMINIER ET AL., PROPERTY 223, 226 (9th ed. 2018).

9. *See id.* ("The common law elements of abandonment are (1) the owner must intend to relinquish all interests in the property, with no intention that it be acquired by any particular person, and (2) there must be a voluntary act by the owner effectuating that intent.").

10. *See* DECKLE MCLEAN, PRIVACY AND ITS INVASION 3-6 (1995) ("Because the word 'privacy' is used so widely and so loosely, the concept remains inexact.").

11. *See infra* Part IV.

12. *See infra* Part V.

couple of decades.[13] Though not anywhere near comprehensive, this demonstrates the extent to which our current lives are not really our own.[14] Part III places that destruction of privacy in a broader cultural and historical context.[15] These rights traditionally relied less on a purely property-rights view, and more on a multi-faceted and subjective basis tied to the ephemeral need to be left alone.[16] The seeds for a property-rights based conception of privacy were always present, but were not clear.[17]

Part IV attempts to tie Parts II and III together, and to explain why modern privacy issues are not really protected by historical standards.[18] In particular, it argues that privacy has always been a property right but one that was easily dealt with elliptically.[19] That is, people have always had protectible interests in being left alone or having their intimate acts and communications kept private—but there was never a real need to ground that right in an actual property right.[20] "Property" is a complicated designation, arising organically over time, and not really defined by any single right or obligation.[21] As such, it is not terribly surprising that privacy was never centrally set within the ambit of property law or property rights—traditionally, violations of privacy were (relatively) rare, usually stemming from the socially unacceptable actions and behaviors of other people.[22] Those actions became the understandable loci of analysis, instead of focusing on the inherent right that was being violated.[23] That arguably no longer suffices in a world where privacy violations have become a norm and a background against which most communications occur.[24] More than that, though, it misses the underlying right that has really always been at the core of the law's recognition of privacy: a settled expectation to be left alone, within context.[25] That expectation sounds in property, as variable as that area of law is, recognizing this is an important and significant step in restoring historical measures of privacy.[26]

---

13. *See infra* Part II.
14. *See infra* Part II.
15. *See infra* Part III.
16. *See infra* Part III.
17. *See infra* Part III.
18. *See infra* Part IV.
19. *See infra* Part IV.
20. *See infra* Part IV.
21. *See infra* notes 117-24 and accompanying text.
22. *See infra* Part III.
23. *See infra* Part III.
24. *See infra* notes 141-47 and accompanying text.
25. *See infra* Part III.
26. *See infra* Part IV.

Part V makes this importance clear by discussing how casting privacy in this way means that people have a greater right to privacy because, in essence, the reasonable expectations of the violated party can be used as the basis for disallowing tech titans from profiting off the acts and communications of others.[27] However, that does not *necessarily* mean that we will enjoy more privacy.[28] A property right of this kind will depend on people's expectations—and a survey of students performed in 2019 indicated that people do not necessarily expect privacy.[29] The erosion of our rights, then, can feasibly be used to justify the continued erosion of those very rights.[30] As such, Part V concludes with a general conversation about some statutory or regulatory measures that could conceivably empower people enough to again stimulate expectations of privacy sufficient, hopefully, to clarify the right to not be spied upon for profit anymore.[31]

II. CURRENT PRIVACY ISSUES

I suppose it has become *de rigueur* to note just how little privacy we have in today's world. To me, the most amazing example of this is Amazon's Alexa product and its ilk.[32] The brazenness of this device's spying is matched only by its breadth: it literally listens to every single word said within earshot, never pausing, never stopping.[33] Its sole purpose, in fact, is to listen in on you at all times, ostensibly awaiting some command related to the current weather or a favorite song.[34] People put these in their kitchens, in their bathrooms, next to their showers, even in their kids' rooms.[35] And can anyone really say how much it overhears? What it does with what it hears? How many lists it compiles and to whom it sells those lists? Does anyone know? Does

27. *See infra* Part V.

28. *See infra* Part V.

29. *See infra* Part V.A.

30. *See infra* Part V.A.

31. *See infra* Part V.B.

32. *See What Is Alexa?*, AMAZON ALEXA, https://developer.amazon.com/en-US/alexa (last visited Aug. 1, 2021) ("Alexa is Amazon's cloud-based voice service available on hundreds of millions of devices from Amazon and third-party device manufacturers. With Alexa, you can build natural voice experiences that offer customers a more intuitive way to interact with the technology they use every day.").

33. Grant Clauser, *Amazon's Alexa Never Stops Listening to You. Should You Worry?*, WIRECUTTER (Aug. 8, 2019), https://www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you.

34. *See id.*

35. *See id.*

anyone care? It seems not, given the ubiquity of these devices.[36] Can anyone honestly imagine that you would have permitted one of the world's largest companies to plant literal listening devices throughout your home without any explicit constraint on how that company uses what it hears (or perhaps, who knows, even sees)?[37] I think not. And, yet, here we are—daily, hourly, moment-to-moment actively welcoming the destruction of a level of intimate privacy that was thought sacrosanct virtually minutes ago, it seems.

And, of course, the list goes on. In the case of *Conditi v. Instagram, LLC*, a consumer filed a class action suit against Instagram, a subsidiary of Facebook, alleging violations of the California Consumer Privacy Act, the California Unfair Competition Law, and the federal Wiretap Act—Title 1 of the Electronic Communications Privacy Act ("ECPA").[38] Her complaint alleged that Instagram, since 2010, had accessed the cameras on users' phones even when the app was not in use.[39] Instagram terms and conditions only give the company limited access, particularly, while the app is in use.[40] The company, without user consent, captured information through the camera and transmitted it to the company for business uses, including targeted advertisements.[41] This camera access intercepted the oral communications occurring when users were not in the Instagram app, without consent.[42]

In *Campbell v. Facebook, Inc.*,[43] Matthew Campbell sued Facebook over its use of Facebook private messages to gain information from users, information which was compiled and sold to advertisers for

---

36. An analysis done by Consumer Intelligence Research Partners, LLC "indicates that the US installed base of smart speaker devices is 76 million units," as of August 2019. Michael R. Levin & Joshua N. Lowitz, *Smart Speaker Market Shows Continued Growth*, CONSUMER INTEL. RSCH. PARTNERS (Aug. 8, 2019), https://46ba123xc93a357lc11tqhds-wpengine.netdna-ssl.com/wp-content/uploads/2019/08/cirp-news-release-2019-08-08-smart-speakers.pdf. And it only gets better. In February 2021,

> Amazon announced Alexa Custom Assistant, a new service that lets device makers, auto makers, and service providers create custom-branded voice assistants that are powered by and work in cooperation with Alexa. The Alexa Custom Assistant can be built into automobiles and consumer electronics, including smart displays, speakers, set top boxes, fitness devices, and more . . . .

Amazon.com Announces Financial Results and CEO Transition, BUS. WIRE (Feb. 2, 2021), https://s2.q4cdn.com/299287126/files/doc_financials/2020/q4/Amazon-Q4-2020-Earnings-Release.pdf.

37. *See* Clauser, *supra* note 33.

38. Class Action Complaint & Jury Trial Demanded, Conditi v. Instagram, LLC., No. 3:20-cv-06534-AGT, at 4, 9-10, 22, 24 (N.D. Cal. Sept. 17, 2020).

39. *Id.* at 3-7.

40. *Id.* at 1-2.

41. *Id.* at 6-8.

42. *Id.* at 25.

43. 77 F. Supp. 3d 836 (N.D. Cal. 2014).

production of "targeted ads."[44] Plaintiff alleged that Facebook intercepted the messages and took scans of them, searching for URLs to understand a user's preferences.[45] Facebook private messages, as described on the website, were purportedly meant to protect private conversations, and the only ones to know of the contents were the sender and receiver.[46] Facebook and plaintiffs settled the case.[47]

In yet another case dealing with the Facebook Empire, *Davis v. Facebook, Inc. (In re Facebook, Inc. Internet Tracking Litigation)*,[48] plaintiffs (Facebook users) alleged violations of various federal statutes, claiming that the company continued to track users' personal information even after they had logged off the social media platform, using plug-ins to track users' browsing histories when they visited other websites.[49] This was done without users' knowledge or consent, meaning Facebook intercepted the communications between the user and first party website (the URL request from the user to the website) and could examine what type of content the website contained and how long a user stayed there.[50] This also meant that Facebook had access to users' browsing history, using this information to compile personal profiles for sale to the highest bidders.[51]

Albeit focusing on a different evil empire, the case of *Brown v. Google, LLC*,[52] sounds much the same. Google has a private browsing option that purports to prevent the company from tracking browsing history, IP addresses, what a user is viewing, and details about a user's hardware.[53] Plaintiffs filed a class action complaint alleging, however, that Google continued intercepting users' private personal data including URL requests, webpage browsing history, search queries, and

---

44. *Id.* at 838-39. "Targeted advertising is a form of online advertising" that is directed to the individual based on his "specific traits, interests, and preferences." *What Is Targeted Advertising?*, GCFGLOBAL, https://edu.gcfglobal.org/en/thenow/what-is-targeted-advertising/1 (last visited Aug. 1, 2021). Advertisers acquire consumers' information by tracking their activity on the internet, which can be done by viewing saved cookies that are associated with online searches, checking search engine history, and finding personal information on social media. *See id.*

45. *Campbell*, 77 F. Supp. 3d at 840.

46. *See id.* at 838-39.

47. Ashwini Bharatkumar, Campbell v. Facebook*: California District Judge Approves Final Class Action Settlement Over Facebook's Use of URL Data*, JOLT DIG. (Mar. 7, 2018), https://jolt.law.harvard.edu/digest/campbell-v-facebook-california-district-judge-approves-final-class-action-settlement-over-facebooks-use-of-url-data.

48. 956 F.3d 589 (9th Cir. 2020).

49. *Id.* at 596-97.

50. *Id.* at 596.

51. *Id.* at 596, 601.

52. No. 20-CV-03664-LHK, 2021 WL 949372 (N.D. Cal. Mar. 12, 2021).

53. *Id.* at *3-4.

geolocation, without their consent.[54] While the search engine would not track the data, Google Analytics, Google Ad Manager, and other apps and plug-ins continued recording the data.[55] After intercepting the communications between a user and a website, Google then used the data acquired by violating the ECPA.[56]

Apparently not content with that kind of behavior, Google's subsidiary, YouTube, was the subject of a civil action in *Federal Trade Commission v. Google, LLC*.[57] There, the Federal Trade Commission brought a Children's Online Privacy Protection Act ("COPPA") complaint against the company, alleging that, beginning in 2016, YouTube gave content creators on their platform the option to use behavioral advertising.[58] YouTube collected data to conduct its behavioral advertising to target ads based in part on the type of video content a YouTube user searched and viewed.[59] YouTube hosted several child-directed channels, with content popular among children relating to toys, movies, and cartoons.[60] As an owner of a website classified as "child directed," YouTube had a duty under COPPA to obtain parental permission before collecting personal information from children, but it failed to adequately ensure the children's parents gave verifiable consent and failed to give notice that the information was used to target advertisements to children based on the personal information and communications gathered.[61]

Of course, it is not just the tech colossi that violate you (and your children's) privacy. In the case of *Ducharme v. Madewell Concrete, LLC*,[62] for example, an employee brought a complaint against his company alleging violations of the Stored Communications Act.[63] As part of his employment, the company provided an iPad for work, which he occasionally used to log into his personal email account.[64] The company filed suit against the employee after he left its employ, using a screenshot from the iPad in the case against him.[65] That screenshot, however, showed an email from plaintiff's personal email account,

54. *Id.* at *1-2.
55. *Id.*
56. *Id.* at *14.
57. Complaint for Permanent Injunction, Civil Penalties, & Other Equitable Relief, Fed. Trade Comm'n v. Google, L.L.C., No. 1:19-cv-02642 (D.D.C. Sept. 4, 2019).
58. *Id.* at 1, 7.
59. *Id.* at 7-10.
60. *Id.* at 10-11.
61. *See id.* at 14-16.
62. No. 6:20-1620-HMH, 2020 WL 4043646 (D.S.C. July 17, 2020).
63. *Id.* at *1.
64. *Id.*
65. *Id.*

meaning the company had accessed his stored electronic information without his knowledge or consent.[66]

It is also not just companies who can take advantage of our online lives and activities to violate our privacy in ways that would have been unimaginable just a few years ago. In *A Vast Web of Vengeance*, author Kashmir Hill details the extent to which an individual armed with nothing more than spite and access to publicly available computers can ruin the reputations and lives of countless people.[67] Therein, Ms. Hill details the activities of a Canadian woman named Nadire Atas, who has posted about numerous individuals with whom she has been in conflict.[68] These posts—alleging fraud, illegal activity, and pedophilia—once online, seemingly exist forever.[69] Whether posted on "reputation websites" like the Ripoff Report or simply available as random blog posts, these claims and descriptions seep into the background structure of the internet, difficult-to-impossible to remove, and forever stain the reputation and privacy of its targets.[70] Though not as direct as some of the above examples, this is no less a terrifying example of how little control we have over formerly private aspects of personhood like reputation and community perception.[71]

And when we say "privacy," it is not just our photos and secrets and innermost thoughts at issue. We also mean the right to participate in an open and free democratic system that is not lorded over by secret gate-keepers utilizing unknowable algorithms and formulae to decide who gets to speak out and who does not.[72] This was made explicit when the same old group of tech companies banned President Trump, in unison, in January 2021.[73] This provoked a wide variety of world

---

66. *See id.* For a discussion on the dangers of employers violating the Wiretap Act and the Stored Communications Act, see Kara K. Trowell, *Monitoring Employee Electronic Communications: A Potentially Risky Business Decision?*, DAVIS WRIGHT TREMAINE LLP (July 2, 2020), https://www.dwt.com/blogs/privacy—security-law-blog/2020/07/privacy-concerns-monitoring-employee-communication. In this blog post, Ms. Trowell notes employers should craft company policies requiring employees to consent to electronic monitoring to circumvent the Wiretap Act. *Id.* For the Stored Communications Act, she suggests either exclusively using employer provided communication services coupled with a disclosure of data retention policy or employees' consent to obtain communications from their private sources. *Id.*

67. Kashmir Hill, *A Vast Web of Vengeance*, N.Y. TIMES (Feb. 2, 2021), https://www.nytimes.com/2021/01/30/technology/change-my-google-results.html.

68. *Id.*

69. *See id.*

70. *See id.*

71. *See id.* The author Kashmir Hill notes, at the end of her article, that Ms. Atas, having become confrontational during conversations, apparently began to post online demeaning and false things about Hill and her husband. *Id.*

72. *See* Bokhari, *supra* note 6.

73. *Id.*

leaders—many (maybe most) of whom did not agree with Trump's policies—to speak out.[74]

None of them liked "the idea that a pack of American hipsters in Silicon Valley can, at any moment, cut off their digital lines of communication."[75] The Web was set up, initially, to accommodate a free flow of ideas and to permit unshackled speech, owned by no one.[76] But that has now been subverted, given the incredible power and reach of a relatively small number of companies, which has monetized and capitalized speech, which monitors thoughts and trends, and which openly manipulates public behavior and electoral processes.[77] Whatever you think of the politics involved, this is ultimately a deep intrusion into a normal public discourse. By intercepting in between open speech and open behavior, these companies have, yet again, lessened the ability of people to speak openly and freely and chipped away, ever more, at privacy rights and norms.[78]

Again, these are simply a few random samples and thoughts regarding the increasing destruction of privacy. With a few days looking by a research assistant, this list could easily be expanded in terms of breadth and type.[79] The overarching point is that our lives are online and they are no longer our own.

III. HISTORICAL CONCEPTS OF PRIVACY RIGHTS[80]

This loss of privacy does not exist in a vacuum. The right to privacy is a longstanding human concern.[81] Indeed, it is not too strong to say that

---

74. *See id.* ("Socialists, conservatives, nationalists, neoliberals, autocrats, and anti-autocrats may not agree on much, but they all recognize that the tech giants have accumulated far too much power."). It is appropriate, I suppose, that this condemnation came from outside America, given that the core remedial scheme I will ultimately recommend also comes from other shores. *See infra* Part IV.B. There is apparently a relatively high level of acceptance of online violation or technocratic control incipient in American culture and society. Whether that is due to America's position as the source of much of the technology at issue or some aspect of our national psyche (perhaps echoed by endless reality television shows), I do not know. But it seems rather stark, and, indeed, I do not think this Article would be necessary if American citizens maintained an even remotely historical sense of self, privacy, and distance.

75. Bokhari, *supra* note 6.

76. *Id.*

77. *See id.*

78. *See id.*

79. *See, e.g.*, Merrill v. Curry, No. 05-19-01229-CV, 2020 WL 6498983, at *1 (Tex. App. Nov. 5, 2020) ("Merrill sued McKinney Independent School District administrators . . . alleging they improperly used unauthorized nude photographs of her that were posted and sent to them by her ex-fiancé to force her to resign her position as teacher.").

80. Much of the material herein is taken from an earlier Article of mine, Pomeroy, *supra* note 3, at 279-82.

privacy is a core part of who we all are.[82] Historically, it was not so difficult or challenging a concept, given how little exposure most people had to other people.[83] But, of course, this has changed over time and is now a very important concern and issue.

Before focusing on the issue itself, though, it is perhaps helpful to take a moment to examine and think about the protections the legal system has traditionally provided when it comes to privacy. From there, given the content of this Article, it is helpful to analyze those traditional protections in the context of our contemporary tech-centric problems and to think about the extent to which the old matches up with the challenges of the new. This should, in theory, aid us in understanding how it is that we have ended up in our current privacy desert.

This historical review is more difficult than it initially seems, though, because the American judiciary has historically struggled to define "privacy" and to specify what "right to privacy" each individual possesses.[84] So, it is certainly true that "[t]hroughout history, human

---

81. *See, e.g.*, TERRY HALBERT & ELAINE INGULLI, LAW & ETHICS IN THE BUSINESS ENVIRONMENT 87-93 (8th ed. 2015) (discussing the value of privacy and the tension between that value and the modern workplace). "In democratic societies there is a fundamental belief in the uniqueness of the individual, in his basic dignity and worth as a creature of God and a human being, and in the need to maintain social processes that safeguard his sacred individuality." ALAN F. WESTIN, PRIVACY AND FREEDOM 33 (1967). There is a "core self" that can be pictured as an inner circle encompassed by larger circles. *See id.* These circles represent an inner core that shelters one's "hopes, fears, and prayers," radiating out to less personal—but nevertheless important—aspects of one's self that we all desire to keep private. *See id.* "The most serious threat," in fact, "to the individual's autonomy is the possibility that someone may penetrate the inner zone and learn his ultimate secrets, either by physical or psychological means." *Id.* This is so important because

> [e]ach person is aware of the gap between what he wants to be and what he actually is, between what the world sees of him and what he knows to be his much more complex reality. In addition, there are aspects of himself that the individual does not fully understand but is slowly exploring and shaping as he develops. Every individual lives behind a mask in this manner . . . .

Id.

82. Or, at least, the right to privacy is a core part of who we are. It is the ability, it seems to me, to decide how much of oneself to reveal that is so important, so intrinsic to our personhood. Obviously, you will reveal more of yourself to a spouse, a child, or a close friend than to a stranger. And, of course, you will reveal different parts of yourself even to different parts of your inner circle, and even to the same person at different times. That is really what privacy is—the dynamic, variable ability to decide who gets to know certain things about you. It is no less than self-determination.

83. The number of people you know or have come into contact with, for instance, is likely vastly higher than that of your grandparents or great grandparents, particularly if you define contact as the people you are exposed to (or who are exposed to you) online.

84. *See* Lance E. Rothenberg, Comment, *Re-thinking Privacy: Peeping Toms, Video Voyeurs, and the Failure of Criminal Law to Recognize a Reasonable Expectation of Privacy in the Public Space*, 49 AM. U. L. REV. 1127, 1132-33 (2000).

beings have always recognized a concept of privacy,"[85] but just what that means has not always been clear.[86]

Some clarity was provided in 1890 "when Samuel Warren and Louis Brandeis drafted the blueprints for a new tort."[87] This newly articulated tort protecting a legal right to privacy, protecting against an invasion of privacy, went beyond trust, contract, and property theories and instead stood alone, stemming from an individual's "inviolate personality."[88]

Part of the difficulty in understanding these sorts of rights, though, is that the very concept of privacy is relative, so the definition of privacy must fit within the ambit of what society is willing to condone.[89] There is, after all, a very big difference between saying that you have a right to exclude paparazzi from your shower and saying that you have a right to exclude the police from your basement drug-cooking operations. And, of course, this is where much of the theoretical heft of this Article is directed—in thinking through why it is that historical privacy norms (whether perfect or not, presumably they covered a significant chunk of important activity) have, more or less, failed entirely to cover contemporary privacy needs.[90]

---

85. *Id.* at 1132 (citing MCLEAN, *supra* note 10, at 3, 9).

86. For many years, the "right to be let alone" seemed to vaguely encapsulate the concept. *Id.* at 1132-33; *see also* THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (2d ed. 1890) (contextualizing the right "to be let alone" in terms of tort law); Peter P. Swire, *Peeping*, 24 BERKELEY TECH. L.J. 1167, 1176 n.49 (2009) (setting forth numerous sources discussing the protections afforded to privacy rights under the English common law).

87. Rothenberg, *supra* note 84, at 1133 (citing Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 219 (1890)). Prior to this, "Peeping Tom crimes were unknown" under the common law. Lisa F. Wu, *Peeping Tom Crimes*, 28 PAC. L.J. 705, 705 (1997). The Article by Warren and Brandeis marked the American beginning of legal protection from various types of intrusion on a person's seclusion. *See id.* at 707. Interestingly, their interest in a tort for invasion of privacy allegedly stemmed from embarrassing press coverage of the wedding party of one of Warren's daughters. *Id.* at 707 (citing William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 383 (1960)).

88. Rothenberg, *supra* note 84, at 1133-34 (quoting Warren & Brandeis, *supra* note 87, at 205). This ideal of an "inviolate personality" has been described "as a condition and right that is essentially tied to human dignity, the principle of equal respect for persons, and the notion of personhood itself." Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479, 484 (1990). *But see* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1343 (1992) (indicating that the "[b]asic kernels of privacy" relate back to the common law crimes of trespass, assault, and battery).

89. "Since the latter part of the twentieth century, the critical determinant of whether a person has a right to privacy is whether that person has a reasonable expectation of privacy in the situation at hand." Robert Sprague, *Orwell Was an Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83, 133 (2008).

90. *See infra* notes 151-55 and accompanying text.

That said, privacy needs to be deconstructed to really be understood or critiqued. Fortunately, "[s]eventy years [after Warren and Brandeis's Article], this concept of invasion of privacy was broken down into four separate torts by Dean William L. Prosser."[91] The four areas of protection "consist of the following: (1) [i]ntrusion upon one's seclusion, (2) public disclosure of private facts, (3) publicity placing a person in false light, and (4) misappropriation of a person's name or likeness."[92]

This list is as interesting for what it is not as for what it is. What it is not is a list that even contemplates an online world.[93] That said, I do think the first area of protection, regarding observing people where they expect not to be observed, or intruding upon their seclusion, is perhaps the most potentially relevant.[94] Looking at people when they wish to remain unseen is a kind of "peeping" not generally permitted under the law, and "[t]he simplest form of peeping is merely to look."[95] "Just looking" is a deceptively innocuous action that has long had significant legal and cultural implications, and the tort of intrusion grows out of this concern.[96] This tort includes three elements: first, there is an intrusion; second, that intrusion is offensive to a reasonable person; and third, the plaintiff had a reasonable expectation of privacy.[97]

These elements probably seem fairly intuitive to most of us: most of us probably think that the law should protect us against unreasonable, impermissible observation. And several early examples seem to confirm this intuition.[98] These examples include "an instance where one looked into windows through elevated railways, and also one in which a detective spied into windows."[99] Most of us would expect privacy while in our own homes, and that is what these cases protect.[100]

Of course, as technology changes, so do society's requirements and the pressures put upon traditional rights.[101] Almost immediately upon

---

91. Wu, *supra* note 87, at 707.

92. *Id.* (citing Prosser, *supra* note 87, at 389).

93. Of course, that is not surprising, given when it was developed—but it is striking, nonetheless, given the extent to which human interaction now revolves around online fora.

94. *See Elements of an Intrusion Claim*, DIGIT. MEDIA L. PROJECT (Jan. 22, 2021), https://www.dmlp.org/legal-guide/elements-intrusion-claim ("An intrusion on seclusion claim is a special form of invasion of privacy. It applies when someone intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another.").

95. Swire, *supra* note 86, at 1173-74.

96. *See id.* at 1174-75.

97. Wu, *supra* note 87, at 707.

98. *See id.* at 708.

99. *Id.* (citing Moore v. N.Y. Elevated R.R., 29 N.E. 997, 998 (N.Y. 1892); Souder v. Pendleton Detectives, Inc., 88 So. 2d 716, 718 (La. Ct. App. 1956)).

100. *See id.*

101. *See id.*

their invention and widespread adoption, for instance, videotaping and photographing became a means to intrude upon privacy.[102] Courts adapted quickly, and, though they have been reluctant to rule that videotaping and photographing constitute intrusions of privacy when they occur in a public place, they have not hesitated to do so when such observation occurs where the person has a reasonable expectation of privacy.[103]

Courts have not, however, similarly adapted to online voyeurism.[104] Though one can make the argument that following someone's online activities, selling their private information, or monitoring their purchases is a kind of "peeping," we have not seen great strides in expanding the tort of intrusion to online activity.[105]

I think this is due to the logical and intuitive heft of the latter two elements of intrusion, mentioned above (that the intrusion must be offensive to a reasonable person and that the plaintiff must have had a reasonable expectation of privacy).[106] The focus on reasonableness and expectations is similar to many torts and, being tort-based, is reflexively focused on one's perceptions of circumstance and the behavior of others.[107] That is, the extent to which conduct is ultimately found to meet

---

102. *See id.*

103. Many cases have so held, and a few examples quickly make the point. *See, e.g.*, Miller v. Nat'l Broad. Co., 232 Cal. Rptr. 668, 678-79 (Cal. Ct. App. 1986). In that case, a TV news crew filmed a man in his home as he was having a heart attack. *Id.* at 670. The court found liability, based upon intrusion. *Id.* at 679. In another case, several underaged fashion models who were secretly videotaped in their dressing area by security guards later recovered against the guards' employer under a cause of action for invasion of privacy. Doe v. B.P.S. Guard Servs., Inc., 945 F.2d 1422, 1423 (8th Cir. 1991). Finally, in a different case, a woman who had been taped while using a tanning bed ultimately recovered punitive damages. Miller v. Willis, No. 92AP-1410, 1993 WL 76303, at *1, *3 (Ohio Ct. App. Feb. 16, 1993). In this context, then, the courts have not had any difficulty understanding the advancements in surveillance made available due to video technology and how those advancements affect historical concepts of privacy.

104. *See* Rothenberg, *supra* note 84, at 1135-38 ("[T]he video voyeur blatantly defies . . . [the] legitimate desire for privacy by utilizing technology to observe, record, and often to disseminate images of the very acts and body parts that were never intended or reasonably assumed to be open to public inspection.").

105. *See id.*

106. *See supra* note 97 and accompanying text.

107. This includes, without limitation, the torts of negligence, Univ. of Tex. M.D. Anderson Cancer Ctr. v. McKenzie, 578 S.W.3d 506, 518-19 (Tex. 2019) (stating that, in a negligence action, foreseeability means that "the actor should have reasonably anticipated the dangers that his negligent conduct created for others"); nuisance, Crosstex N. Tex. Pipeline, L.P. v. Gardiner, 505 S.W.3d 580, 596 n.9 (Tex. 2016) (stating that in a nuisance action, the relevant question is whether the defendant's actions unreasonably hindered the plaintiff's use and enjoyment); assault, Sanchez v. Striever, 614 S.W.3d 233, 239 (Tex. App. 2020) (stating that a person commits an assault if "the person intentionally or knowingly causes physical contact with another when the person knows or should reasonably believe that the other will regard the contact as offensive or provocative"); defamation, Diocese of Lubbock v. Guerrero, 591 S.W.3d 244, 250-51 (Tex. App. 2019) (stating

these elements (and so constitute the tort of intrusion) is driven primarily by the extent to which the conduct seems objectively objectionable.[108] Courts—and society—ask whether something seems strange, bizarre, or weird.[109] We look outside ourselves and ask how society views our inner life or personal actions. This is, then, a fundamentally outward facing view of rights, dependent on what society, as a whole, thinks is reasonable or normal, and the behavior of others within the context of that normality (or lack thereof).[110]

This is in contrast to an inward looking, inherent view of rights.[111] Under this kind of view, a right is a more concrete thing, less subject to the vagaries of social views or pressures.[112] It is a legal ability or power that is broadcast to the world and to which the world must react. In this sense, it is possibly more subjective, as it is not as variable, and can, in some ways, be defined by the individual because, once so defined, it exists and must be reacted to.[113]

I think that privacy has historically been viewed through the lens of the former because most privacy-violating acts have historically been easily understood as observably outrageous, or weird, behavior.[114] Ultimately, though, I think the latter view of privacy is more correct and healthy and would cover a wider variety of activity that, though historically not bizarre, would likely be viewed by most reasonable people as a violation of what most of us understand as our privacy rights.

---

that whether a publication is defamatory depends on a reasonable person's view of the publication as a whole"); negligent infliction of emotional distress, Carrol v. Allstate Ins. Co., 815 A.2d 119, 128 (Conn. 2003) (stating that a person negligently inflicts emotional distress if the fear experienced by the plaintiffs is reasonable compared to the acts of the defendants); and professional malpractice, Rogers v. Zanetti, 518 S.W.3d 394, 406 (Tex. 2017) (stating that in a malpractice action, "the risk associated with a trial tactic speaks to what a reasonably prudent lawyer would do under similar circumstances"). It does not appear too strong a claim to state that tort law is substantially constructed upon the concept of reasonableness.

108. *See* Prosser, *supra* note 87, at 390-91.

109. *See, e.g.*, Wood v. Hustler Mag., Inc., 736 F.2d 1084, 1085-86 (5th Cir. 1984) (finding an invasion of privacy when neighbors broke into Wood's home, stole a nude photo, and forged a consent form for Hustler Magazine to publish); Patel v. Hussain, 485 S.W.3d 153, 176-77 (Tex. App. 2016) (stating that Patel not only sent Nadia a text message threatening to play Nadia's private video during a mutual friend's wedding, but also frequently sent offensive messages, hacked into her accounts, and uploaded the secretly recorded videos to the web); Merrill v. Curry, No. 05-19-01229-CV, 2020 WL 6498983, at *1-2 (Tex. App. Nov. 5, 2020) (involving public school administrators who took a nude photo from emails and enlarged the photo on an oversized computer monitor during a private employment meeting).

110. *See* Prosser, *supra* note 87, at 390-91.

111. *See* Nicholas Wolterstorff, *Justice as Inherent Rights: A Response to My Commentators*, 37 J. RELIGIOUS ETHICS 261, 263 (2009).

112. *See id.*

113. *See id.*

114. *See supra* notes 108-09 and accompanying text.

In essence, what I am arguing is that privacy really is an *in rem* right—and that, ultimately, it is one we are actively abandoning.[115] Viewing privacy in this fashion squares the circle of why we have an invasion of privacy tort, but live in a world where virtually anything we do or say (most of which occurs online) does not belong to us and is fair game for companies and third parties to pilfer and profit from.

IV. PRIVACY AS PROPERTY[116]

As indicated above, property law focuses on the *thing* and the rights flowing from that thing.[117] This means that third parties have to expend time and resources to learn the attributes of these rights, rather than requiring the rights-claimant to advertise or take on the burden of informing others of their right.[118] Because it focuses on the corporeal thing, this theory of cost can be said to flow from the *in rem*, as opposed to the *in personam*, nature of property.[119] This is inherent in

115. I am largely focusing on the common law, though I think the same can be said of statutory and regulatory law, as well, though there are a number of (again) arguably relevant statutes out there. "The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986," for example. *Electronic Communications Privacy Act of 1986 (ECPA)*, BJA, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 (last visited Aug. 1, 2021). According to the United States Department of Justice, the Electronic Communications Privacy Act ("ECPA") applies to "wire, oral, and electronic communications" that are transmitted or stored in a computer. *Id.* These include emails, phone calls, and electronically stored data. *Id.* Title I of the ECPA, also known as the Wiretap Act, prohibits intentional actual or attempted interception, use, disclosure, or procurement of any wire, oral, or electronic communication. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511. The Wiretap Act has exceptions for operators and service providers for uses in the ordinary course of business necessary to providing the service. *Id.* Title II of the ECPA, also known as the Stored Communications Act, protects the contents of electronically stored information when the information is stored by service providers. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2701–2702. The contents protected include subscriber name, billing records, or IP addresses. *Electronic Communications Privacy Act of 1986 (ECPA)*, *supra*. These federal provisions represent the backbone of electronic privacy claims, but, again, they do not apply squarely to the kinds of issues at hand. Similarly, the Children's Online Privacy Protection Act, specifically focused on children, protects the private personal information of children under the age of thirteen. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6502. The Act requires companies to acquire the consent of parents to collect this type of personal information from their children. *Id.* § 6502. Personal information includes name, address, IP address, and browsing history. *See id.* § 6501. This statute seems relatively muscular, in this context, but irredeemably narrow.

116. Much of the material herein is taken from an earlier article of mine, Chad J. Pomeroy, *The Shape of Property*, 44 SETON HALL L. REV. 797, 806-10 (2014).

117. Thomas W. Merrill & Henry E. Smith, *What Happened to Property in Law and Economics?*, 111 YALE L.J. 357, 360 (2001).

118. Unusual property rights increase the cost of doing this. I have previously written about this view of property, in the context of the numerus, on a number of occasions. *See, e.g.*, Pomeroy, *supra* note 5, at 525-30.

119. Merrill & Smith, *supra* note 117, at 360.

Blackstone's famous definition of property: "that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe."[120]

This view of property rights focusing upon the thing itself means that rights are defined with respect to an actual, concrete thing that is possessed or owned (as opposed to being defined with respect to the actors or individuals involved).[121] This, in turn, means that property effectively broadcasts the rights and obligations inherent therein to "the world."[122] And that acts to create a duty in "everyone else" to understand what is being broadcast.[123]

> In order to avoid violating another's property rights, [individuals] . . . must ascertain what those rights are. In order to acquire property rights, [individuals] must measure various attributes, ranging from the physical boundaries of a parcel, to use rights, to the attendant liabilities of the owner to others (such as adjacent owners).[124]

I think this would be a much healthier approach to something like privacy rights in our modern world. Ironically, perhaps, I think this is so because privacy is so innately ephemeral.[125] Corporeal things are, obviously, identifiable—a box is a box, a car is a car, your property book is your property book, and Blackacre is Blackacre.[126] There is no disconnect between how I see a car and how you see a car (at least, not in the context of recognizing it as a thing that is ownable). And yet, even in that overt context, property law still functions in terms of *in rem* rights.[127] Privacy obviously is not a corporeal thing[128]—but, rather than

---

120. 2 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 2 (1992).

121. This is a traditional view of property, also relied on by Adam Smith and Jeremy Bentham, which is in contrast with a more recent view of property rights as a malleable "bundle of rights." *Compare* ADAM SMITH, LECTURES ON JURISPRUDENCE 9-10 (R. L. Meek et al. eds., 1978) (viewing property rights as being focused upon the thing itself), *and* 2 JEREMY BENTHAM, THE LIMITS OF JURISPRUDENCE DEFINED 164-65 (Greenwood Press Publishers 1970) (1945) (analyzing property rights as being defined with respect to an actual, concrete thing), *with* Felix S. Cohen, *Dialogue on Private Property*, 9 RUTGERS L. REV. 357, 370-71 (1954) (examining property rights with respect to other individuals involved).

122. Merrill & Smith, *supra* note 117, at 360.

123. *Id.* at 359.

124. *See* Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The* Numerus Clausus *Principle*, 110 YALE L.J. 1, 26 (2000).

125. MCLEAN, *supra* note 10, at 3-5.

126. Blackacre is "a fictitious piece of real property . . . used in the study of property law." *Legal Definition of Blackacre*, MERRIAM-WEBSTER, https://www.merriam-webster.com/legal/blackacre (last visited Aug. 1, 2021).

127. Merrill & Smith, *supra* note 124, at 32.

128. *See* MCLEAN, *supra* note 10, at 5.

make an *in rem* view less important, I think it makes it more important: privacy is less clear, less explicit. My view of what I want to happen to pictures of my kids on vacation likely differs a lot from your view of what you want to happen to pictures of your kids on vacation—much more than our views of the cars we drove on that vacation would differ. That said—even though we would differ on the precise contours of the protections we want afforded to those pictures—most people would certainly want some protections to attach. There are broadly acceptable contours of privacy rights that most people can agree on, but even these will not flourish if every manifestation of privacy depends upon interpreting the acts of third parties on an ad hoc basis.[129] In other words, permitting an inherently variegated right like privacy to exist solely as it is viewed by society at large is bound to end in its virtual elimination.[130]

An *in rem* kind of focus will result, then, in a far more secure recognition of rights than a third-party or facts-and-circumstances focus would.[131] Now, one legitimate objection here is that doing so will result in enormous burdens on third persons ("third persons," here, being "everyone else").[132] The problem, of course, is that an *in rem* focus imposes burdens on everyone to know and understand others' rights (indeed, that is the feature for which I am lauding it).[133] Merrill and Smith focused in on this informational burden in theorizing why the American property law system has the numerus clausus.[134] They claim

---

129. *See* Thomas W. Merrill & Henry E. Smith, *The Property/Contract Interface*, 101 COLUM. L. REV. 773, 793-94 (2001) (explaining that in complex circumstances with many parties and competing interests, an *in rem* strategy is necessary to avoid a "break down" of the regulatory system).

130. A fairly clear parallel is the designation of intellectual property as "property." Ideas, words, creative works—these are intangible things, as well, but are recognized as property, and so bestowed with property rights. Of course, these did not much exist at common law either (with a few exceptions) and so, the absence of "privacy rights" from the "property rights" realm is not particularly surprising. *See* Pomeroy, *supra* note 5, at 526 (explaining that courts are resistant to creating "different types of property" or "new interests" because "property law recognizes only a limited number of property forms or types").

131. Merrill & Smith, *supra* note 129, at 792 (stating that an *in rem* strategy provides useful social functions, such as "a basis for security of expectation[s]").

132. *Id.* at 795-96.

133. Merrill & Smith, *supra* note 124, at 26.

134. *Id.* at 24-26. Merrill and Smith make the point that what the numerus clausus is really doing is making it easier on others to understand what is being broadcast about the ownership rights of others in a particular thing:

> There can be no harm in allowing the fullest latitude to men in binding themselves and their representatives, that is, their assets real and personal, to answer in damages for breach of their obligations. This tends to no mischief, and is a reasonable liberty to bestow; but great detriment would arise and much confusion of rights if parties were allowed to invent new modes of holding and enjoying real property, and to impress upon their lands and tenements a peculiar character, which should follow them into all hands,

that courts are concerned that new property interests will create information costs for those third parties that are required by our *in rem* system to perceive the rights being broadcast from all property.[135]

This is a significant concern for a number of reasons. The first reason is inherent in communication—one must expend resources (incur cost) in order to receive and correctly interpret communication, and expanding the type or range of information being communicated (i.e., changing what rights are possible or potentially present by creating new types of property) will necessarily increase that cost.[136]

The second is the universality described above: the duty to understand is not personal—it attaches to "everyone else" and is necessary in order to permit people to clearly and efficiently perceive property rights and obligations and to economically arrange their plans accordingly.[137] Unfortunately, this universality, while helpful and necessary, greatly amplifies the costs of communication because those costs end up being applied both to interested parties and to third parties who presumably have no need to understand the rights and responsibilities of a given property owner or relating to a given piece of real property.[138]

Property owners and those directly interested in a given piece of property will not take adequate account of these third-party costs, so the informational burden identified herein is only possible so long as

---

> however remote. Every close, every messuage, might thus be held in several fashion; and it would hardly be possible to know what rights the acquisition of any parcel conferred, or what obligations it imposed.

Id. at 25-26 (quoting Keppell v. Bailey, 39 Eng. Rep. 1042, 1049 (Ch. 1834)).

135. *See id.* at 26.

136. *See id.* at 26-27.

137. *See* Cohen, *supra* note 121, at 359; Merrill & Smith, *supra* note 117, at 359.

138. *See* Cohen, *supra* note 121, at 359-61. Merrill and Smith posit a helpful example, which seems to have been based, at least in part, on a more complex hypothetical set forth by Henry Hansmann and Reinier Kraakman. *See* Merrill & Smith, *supra* note 124, at 27 (referencing Henry Hansmann & Reinier Kraakman, *Property, Contract, and Verification: The* Numerus Clausus *Problem and the Divisibility of Rights*, 31 J. LEGAL STUDIES S373, S416-17 (2002)). Suppose that many people own watches. *Id.* One of these people is A, who is the sole owner of one of the watches and who wants to transfer some of his rights to use the watch to B. *Id.* The law permits the creation of various types of estate in property: A could sell a fee, a life estate, or some sort of concurrent interest. *Id.* But, instead of this, assume that A wants to create a time-share type of interest in the watch, which would allow B to use the watch only on the 15th of each month. *Id.* If this sort of "fancy" property right were permitted, then everyone else interested in buying a watch (whether from A or from any other owner) would have to continually be on the lookout as to whether or not the watch they were interested in had been carved up in this manner or in some other unique manner. *Id.* Neither A nor B would care about this, as they would have accomplished their purpose and would presumably have accounted for any marginal cost associated with a future sale. *Id.* By foreclosing anything other than a standardized set of forms, then, property law forces parties to effectively moderate the costs ultimately borne by "everyone else." *Id.*

property remains simple and standardized, such that "everyone else" can understand the broadcast easily and with little cost.[139] This standardization lowers the cost of determining the nature of the property rights at issue and so economically benefits society as a whole.[140]

Those seem like huge concerns in my suggestion that we view privacy through an *in rem* lens. I think, however, that such concerns and concepts actually run, counterintuitively, in the opposite direction—that is, that they support the useability of such a focus, in this context. For, while it is true that it is very difficult and costly to understand all rights and obligations associated with all possible kinds of "property," when that requirement to understand is imposed on everyone, our modern privacy issues do not really revolve around "everyone."[141] Instead, they

---

139. *See id.* at 33. This point about third parties is central to Merrill and Smith's view of the numerus clausus. *See id.* at 28. They focus on the informational asymmetry that arises due to the fact that third parties have no connection with, or exposure to, the transaction wherein the unique property interest is created. *See id.* Those connected with the transaction (that is, those who fall within the "zone of privity") are able to account for the increased informational costs by incorporating them (or an expectation of them) into the price they receive or pay, and such immediate parties (or those within the "zone of privity" of the decision to create the fancy right) could perhaps be just as effectively (and more easily) controlled or affected by a contractarian approach with default rules that can be opted out of. *See id.* at 30-31. Those not so connected to the transaction, however, do not have the knowledge or ability necessary to act in an informed manner. *See id.* at 31. And it is that disconnect upon which Merrill and Smith focus—that fundamental asymmetry of information that drives the numerus clausus as a mandatory rule of prohibition. *See id.* Interestingly, that may well be (particularly given the amount of interest generated by Merrill and Smith's writings on this matter), but that is not directly relevant to the point made by this Article. The relevant point here is that, at least in the view of some, the numerus clausus exists in order to counteract informational burdens created by new or unique property types. *See id.* at 38. The extent to which those costs are borne by those outside the zone of privity is partially analogous, but it is not necessary and does not directly drive the application of the numerus clausus to the heterogeneity of vesting documents. *Compare id.* at 38, *with* Pomeroy, *supra* note 116, at 811-19. In fact, taking it even a step further, the numerus clausus is arguably applicable here, regardless of whether or not it directly turns on informational burdens. *See* Michael A. Heller, *The Boundaries of Private Property*, 108 YALE L.J. 1163, 1176-78 (1999). Heller argues that the purpose of the numerus clausus is to limit fragmentation of ownership and thus promote the easy transferability of property rights. *See id.* This is not an informational burden and so is not as similar to the heterogeneity cost identified above as is Merrill and Smith's cost. The numerus clausus would still apply, however, as it still posits that property law should limit newness or uniqueness when doing so would further an underlying goal of property law. Merrill & Smith, *supra* note 124, at 40.

140. *See* Merrill & Smith, *supra* note 124, at 33. This may lead to the conclusion that there is a preferred balance as to the economically appropriate number of recognizable property forms. *See id.* at 39-40. Some costs would be lowest in a fixed system that only recognizes a single type of property interest. *See id.* "On the other hand, by grandfathering in existing forms of property, and permitting legislative creation of new forms, the *numerus clausus* permits some positive level of diversification in the recognized forms of property." *Id.* at 40. *But see* Pomeroy, *supra* note 116, at 807-19 (arguing that, perhaps, property law is not as much shaped by the type of informational burden analysis propounded by Merrill and Smith as some have argued).

141. *See supra* Part II.

really only revolve around the technology whales of our day.[142] It is true that, as much of our life has migrated online, the privacy ramifications have multiplied exponentially and that these ramifications are felt, to some degree, by everyone.[143] We all, as individuals, have choices to make regarding others' online information and lives. However, by far, the most pressing concerns really stem from the activities of a relatively small number of companies.[144] I do not purport to know the exact number, but the basic oligarchy of tech titans is well known: Facebook, Google, Amazon, Apple, Microsoft.[145] These companies have an enormous level of connection to each of us—we communicate via them, we share photos via them, we purchase via them, we invite them into our homes to listen in on us at all times (literally), we use them to access the internet and much of the outside world.[146] Just read through Part II again, even briefly—almost every privacy issue raised there (and almost every issue you can think of that is likely to present a legitimate threat to your privacy) surrounds these (and perhaps a relatively modest number of other) companies.[147]

This is, in fact, excellent news. Without anticipating the solutions discussed in Part V too much,[148] it suffices here to say that our privacy can be protected if we all take a greater, more proprietary view of those rights and that this, in turn, can be instigated by imposing some basic obligations on the tech companies that have so much access to so much private data.[149] Given that this access is so concentrated in the hands of so few, this is a feasible and workable idea. But it must start with convincing people that they do, in fact, own *something*.[150]

V. PRIVACY AS *ABANDONED* PROPERTY

The sum suggestion, to this point, then, is that privacy rights have traditionally been viewed as an issue of tort, revolving around the acts of others, but that this view is not equal to the task of protecting privacy in

142. *See supra* Part II.

143. *See* Bokhari, *supra* note 6.

144. *Tech Giants Do Not Face Enough Competition, New Report Says*, PRIV. INT'L (Mar. 13, 2019), https://privacyinternational.org/news-analysis/3736/tech-giants-do-not-face-enough-competition-new-report-says.

145. *Id.*

146. *See* John Herrman, *We're Stuck with the Tech Giants. But They're Stuck with Each Other*, N.Y. TIMES (Nov. 13, 2019), https://www.nytimes.com/interactive/2019/11/13/magazine/internet-platform.html.

147. *See supra* Part II.

148. *See infra* Part V.

149. *See* Bokhari, *supra* note 6.

150. *See infra* Part V.A.

the modern age.[151] Instead, privacy should be viewed as an *in rem* right, as something we own that others must acknowledge and of which they must take stock.[152] This will only help,[153] though, if people recognize these *in rem* rights and view them as valuable property worth protecting. That is clearly not the case now, as a small survey, discussed below, that I put out to my students makes clear.[154] There is, however, a solution to this problem that can provoke a more proprietary view of privacy and so usher in a better era of protection and rights.[155]

A. The Abandoned Birthright

If we reconceptualize privacy as a property-type right that radiates outward and must be understood and respected by others, then we go a long way toward "fixing" the current status quo, wherein nobody seemingly cares a whit for our inner selves or private thoughts. However, what good is a property right if it is abandoned?

Abandonment of property is possible, within limits.[156] In order to establish abandonment, the owner must intend to relinquish all ownership (with no intent that it go to a particular person) and there must be a voluntary, affirmative act effectuating that intent.[157] This is an analogous concept here because, even if you conceive of privacy rights as property rights, it very much appears they have been abandoned.[158]

In Fall 2019, I asked over 100 students to complete a questionnaire attempting to assess their online behavior, their views on social media, and their expectations of privacy.[159] Ninety-three completed the survey. The results are generally depressing.

First—in a surprise to no one—almost everyone uses the internet a lot. Most people use social media multiple times per day, most people use email multiple times per day, most people conduct internet searches

151. *See supra* Part III.

152. *See supra* Part IV.

153. By "help," I mean, encourage the acknowledgment and vitality of privacy rights in our culture, at large.

154. *See infra* notes 160-66 and accompanying text.

155. *See infra* Part V.B.

156. Real property cannot be abandoned. *See* DUKEMINIER ET AL., *supra* note 8, at 226, 229.

157. *Id.* at 225-26. (citing Hawkins v. Mahoney, 990 P.2d 776, 781 (Mont. 1999)).

158. Completing the analogy, abandoned property can be claimed by anyone. *Id.* at 225 (citing *Hawkins*, 990 P.2d at 779). It is not too much a stretch to say that Facebook and its ilk have simply come along and claimed the private information and data belonging to the millions (or billions) of people who have abandoned it.

159. For the questions asked, and the responses received, see *infra* Appendix A.

multiple times per day, and most people utilize a Global Positioning System ("GPS") on a regular basis.[160]

Second, most people have no real expectation of privacy when it comes to this online activity. Three-quarters of the respondents expect that the relevant service providers will be able to access the content that they put online, and nearly as many (two-thirds) expect that even third parties will be able to access the content that they put online.[161] And, not only do people expect providers and strangers to access that content, about 40% expect that those providers will be able to sell that content to third parties.[162]

So, if you conceive of privacy rights as an *in rem*-type of property interest—that is, something that you own and that broadcasts out obligations to third parties—then it is a property interest that has been abandoned. People expect their online behavior to be observed and monetized.[163] They do not expect or demand that their property be respected or that the value that flows from it stay with them—they know that providers and third parties are taking that data, using it, selling it, and yet they continue to use these media on a near-constant basis.[164] They have rights, but willingly give them up.

There is, perhaps, a slight silver lining in the survey. And that is the last question.[165] Nearly 80% of the respondents indicated that they had altered their privacy settings, based upon their belief that their privacy was being invaded.[166] That is good, in that it indicates that people do care—which is enough, I think, to serve as a foundation for viewing privacy as the property right it ought to be viewed as, and all of the benefits that radiate out from that: if people care, then they will possibly demand that others respect that about which they care. It is particularly good news, too, in that it suggests a way to let people actively protect their rights: by giving them simple tools to do so. If I can toggle a button and prevent Facebook from selling photos of my kids to third-party vendors, then I will do so—and so, apparently, will most people.

---

160. *See infra* Appendix A. If I were to repeat this survey, I think I would drill down on which applications/websites people use the most and on the difference between people's perceptions of email privacy and social media privacy. I suspect that people expect, and desire, more privacy when it comes to email than to, say, Twitter. Given what I discuss below regarding how to inculcate a sense of ownership in privacy rights, I think that existing expectation could perhaps serve as useful information and perhaps as a sort of guidepost. *See infra* notes 163-66 and accompanying text.

161. *See infra* Appendix A.

162. *See infra* Appendix A.

163. *See infra* Appendix A.

164. *See infra* Appendix A. I say "they," but I do this, too. Nearly everyone does.

165. *See infra* Appendix A.

166. *See infra* Appendix A.

Unfortunately, we have seen the results of relying on this sort of ad hoc, bit-by-bit approach to privacy, wherein every company comes up with its own privacy standards and its own ways to permit consumers to opt in or out of various violations.[167] The internet is just too all encompassing, and the companies that effectively run it are just too omnipresent[168]—even if consumers begin to view privacy as *theirs*, a random approach tucked at the end of a long list of terms and conditions will not result in the kind of systemically protective approach to privacy rights that we ought to have. Instead, what is needed is a silver bullet—an all-in-one ability to force internet service providers to pay attention to our rights and to respond to them. Fortunately, there is such a bullet—and it has been used elsewhere with real results.[169]

B. Giving People the Tools to Protect Themselves

The key, I think, is to allow people to fully protect themselves. If they had this ability, easily exercised, they would feel empowered and entitled to their privacy rights—they would no longer shrug their shoulders in collective apathy in the face of technological encroachment if they knew it was within their power, and their right, to stop it. And the way to do this is already well established, though not in our country.[170]

In the United States, the publication of truthful information is generally protected by the First Amendment[171] even when that information is potentially embarrassing for the person it covers[172] or otherwise imposes on their privacy.[173] Significantly, the United States extends this protection to online platforms like YouTube and Google, as well.[174] Other countries do not, instead prioritizing an individual's right to be forgotten or right to erasure.[175]

---

167. *See* Alfred Ng, *Default Settings for Privacy -- We Need to Talk*, CNET (Dec. 21, 2019, 5:00 AM), https://www.cnet.com/news/default-settings-for-privacy-we-need-to-talk.

168. *See* Bokhari, *supra* note 6.

169. *See infra* notes 176-81 and accompanying text.

170. *See infra* notes 176-81 and accompanying text.

171. *See* Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979) ("[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.").

172. *See* Fla. Star v. B.J.F., 491 U.S. 524, 532-33 (1989) (holding state law criminalizing the publication of sexual offense victims' names unconstitutional).

173. *See* Judith Haydel, *Privacy*, MIDDLE TENN. STATE UNIV., https://www.mtsu.edu/first-amendment/article/1141/privacy (last visited Aug. 1, 2021).

174. *See* Garcia v. Google, Inc., 786 F.3d 733, 745-47 (9th Cir. 2015) (noting that, while one may wish to have certain information "forgotten and stripped" from an online platform, there is no "right to be forgotten" in the United States).

175. *See id.* at 745.

The European Union—and, therefore, its twenty-seven member countries—recognizes such a right.[176] In adopting this position, the European Union addresses the difficulty many face when trying to escape or conceal unpleasant personal information—and, thus, gives people the ability and prerogative to take care of themselves.[177] "[T]he right to be forgotten addresses an urgent problem in the digital age: it is very hard to escape your past on the Internet now that every photo, status update, and tweet lives forever in the cloud."[178]

The concept actually originates in a much narrower "right of oblivion" under French law, which allows an individual with a criminal history to object when someone publishes facts surrounding his conviction after he has served his time for the crime and has been rehabilitated.[179] The European Union's "right to be forgotten" doctrine builds upon that idea and is much broader—it extends well beyond information relating to criminal convictions.[180] It applies to the processing of any information that is "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes" for its processing.[181]

This sweeping definition raises many questions that are still being thought through and settled.[182] In *Google Inc. v. González*,[183] for example, González sought to have Google remove newspaper articles mentioning "a real-estate auction connected with attachment proceedings for the recovery of social security debts" from the list of results appearing when his name was entered into the website's search engine.[184] The Court of Justice of the European Union held that a search engine operator like Google is a "data processor" required to grant valid requests to have information erased under the European Union-recognized right to be forgotten.[185]

---

176. 1995 O.J. (L 281) 31; *see also* Case C-131/12, Google Inc. v. González, ECLI:EU:C:2014:317, ¶ 2 (May 13, 2014); Court of Justice of the European Union Press Release 70/14, An Internet Search Engine Operator Is Responsible for the Processing that It Carries Out of Personal Data Which Appear on Web Pages Published by Third Parties (May 13, 2014).

177. *See* Jeffrey Rosen, *The Right to be Forgotten*, 64 STAN. L. REV. ONLINE 88, 89 (2012).

178. *Id.* at 88.

179. *Id.*

180. *See* Court of Justice of the European Union Press Release 70/14, *supra* note 176.

181. *Id.*

182. Inadequate to accomplish what, exactly? Irrelevant or no longer relevant to what issue? And who decides what the purpose for a particular data processing instance is or was? *See, e.g.*, FED. R. EVID. 401 (defining evidence as relevant if it "make[s] a fact [at issue] more or less probable than it would be without the evidence").

183. Case C-131/12, ECLI:EU:C:2014:317 (May 13, 2014).

184. *Id.* at ¶¶ 14-15.

185. Court of Justice of the European Union Press Release 70/14, *supra* note 176.

In addition to the undeniably broad substantive nature of the right to be forgotten, the *González* decision seemed to grant a geographically broad (possibly global) reach, as well.[186] There, the court held that where the search engine operator has some establishment in a member state, the requirements apply even if the organization "has its seat in a non-member [s]tate."[187] It therefore held the requirements applicable to Google Inc., even though Google asserted that the data processing itself happened in a non-member state.[188] The court later limited its holding, finding that processors were only required to block or "de-reference" affected search results in *member* states.[189] In other words, the search results may remain on versions of the search engine serving non-member states, like the United States.[190]

Of course, this right to be forgotten does create burdens on the right to free speech.[191] After all, at its core, the regulation allows one person to initiate the suppression of another's speech.[192] And the likelihood of suppression is compounded by the burden the right to be forgotten places on data processors, like Google, should they choose to refute the right in any given situation because, while the procedure for submitting a request to have your information erased is remarkably simple,[193] the requirements for denying that request is not.[194] If the organization receiving the request for erasure chooses to deny the request, it bears the burden of justifying its decision by proving its interest in processing the data overrides the requestor's right to be forgotten, which requires showing the request was "unfounded or excessive."[195] If, on the other hand, the data processor chooses to grant the request, it merely has to take reasonable steps to verify the identity of the person submitting the

186. *See id.*

187. *Id.*

188. *Id.*

189. Court of Justice of the European Union Press Release 112/19, The Operator of a Search Engine Is Not Required to Carry Out a De-Referencing on All Versions of Its Search Engine (Sept. 24, 2014).

190. *Id.* (noting that, while processors are not *required* to de-reference the affected information on all versions of their search engines, they are nevertheless free to do so).

191. Rosen, *supra* note 177, at 88, 90.

192. *See id.* at 88-91 (noting the risks of extending the right to be forgotten beyond just rescinding something one person said about himself to what someone else lawfully said about him).

193. *Everything You Need to Know About the "Right to Be Forgotten,"* GDPR.EU, https://gdpr.eu/right-to-be-forgotten (last visited Aug. 1, 2021) (noting there is no specified format for an erasure request—such a request may be made either verbally or in writing and need not contain the words "request for erasure" or "right to be forgotten" or reference the particular authorities which apply).

194. *See id.*

195. *Id.* (listing the acceptable justifications for denying an individual's request for erasure).

request and then erase the information "without undue delay."[196] Because such a substantially greater burden accompanies a decision to deny, it seems likely many platforms will grant more requests than they deny—thus, suppressing more speech than they fight to protect.[197]

However, the import of this Article is really that such a burden must be balanced against what is gained by granting this right to individuals. This is not a one-sided analysis involving a naked loss of rights. The loss of speech, on the one hand, is countered by the gain of privacy rights on the other—a gain, I think, that will enable people to enjoy rights that they already have and that have been widely forgotten or abandoned.[198] Doing this will go a long way to righting the imbalance we are all currently experiencing in the modern era, where we all have less and less privacy, as the big technology companies become more and more powerful.[199]

Indeed, righting this imbalance is so important that the scale should be tipped even further, I think. The European Union's General Data Protection Regulation ("GDPR") does permit damages, but I do not think it goes far enough.[200] Under the GDPR scheme, should a data processor fail to timely remove information after a data subject submits a valid removal request, the processor may face a number of financial consequences.[201]

First, there is provision for administrative fines.[202] Second, the processor may be held liable to individual data subjects for any "material or non-material" damages suffered because of the delay.[203] However, this seems somewhat toothless, given the difficulty of calculating non-material damages, such as discrimination or damage to reputation. These sorts of things are extremely difficult to quantify,[204] and, as always, one has to remember that the state of play is a single individual against a large corporation with virtually limitless resources. This is all the more true, given that the European Union member state courts require those alleging such damages to prove that actual non-material

196. *Id.* (quoting 2016 O.J. (L 1119) 1) ("'Undue delay' is considered to be about a month.").

197. *See* Rosen, *supra* note 177, at 88-92.

198. *See supra* Part V.A.

199. *See supra* Part II.

200. *Everything You Need to Know About the "Right to Be Forgotten," supra* note 193.

201. 2016 O.J. (L 119) 82–83.

202. *Id.* (imposing "effective, proportionate[,] and dissuasive"-sized fines for General Data Protection Regulation ("GDPR") infringement).

203. *See* 2016 O.J. (L 119) 81–82 (imposing joint and several liability when more than one entity is at fault for the damages suffered).

204. Henrik Hanssen, *Germany: New Case-Law on Immaterial Damages for GDPR Infringements*, JDSUPRA (Oct. 26, 2020), https://www.jdsupra.com/legalnews/germany-new-case-law-on-immaterial-63954.

damages were suffered, it being insufficient to merely show a GDPR infringement and allege non-material damages without substantiating them.[205]

Perhaps because of these difficulties (attendant as they are to the lack of a substantial remedy), there seems to have been limited application of Article 82 of the GDPR itself in cases involving the right to be forgotten, specifically.[206] What is needed, then, is a robust method to accurately capture the damages inflicted, to ensure that the value thereof can be transferred back to the harmed party, and to ultimately incentivize individuals to take on the very large corporations that are reaping these profits by appropriating the property of individuals everywhere.

What is called for in this scheme, I think, is the ability to pursue American-style damages. Leaving up damaging information about individuals (or, really, any information about them) is a significant decision that dramatically affects those individuals—that, in the styling and import of this Article, affects their property rights. Thus, it should be treated as such, and that means that any damage resulting from such a decision should be compensable in a way that accurately drives at the damage done. To start, that means compensatory damages. Compensatory damages are awarded "to a person as compensation, indemnity or restitution for harm sustained,"[207] with the amount of damages intended to put the injured party in as good a position as they were before the injury.[208] "Compensatory damages do not include any amount 'in excess of the damages [the plaintiff] has suffered' because the 'plaintiff is entitled to be made whole and nothing more.'"[209] This has the effect of righting the wrong in that the wrong-doer has to bear (or

---

205. *Id.* It is currently unclear whether punitive damages are available under the General Data Protection Regulation. *Id.* However, given the tendency of many member state courts to require proof of actual damages, it seems unlikely punitive damages will be available in this context. *Id.*

206. However, some European Union ("EU") member courts have imposed liability based on pre-GDPR EU directives and caselaw; for example, the Court of Appeal of Barcelona considered a civil suit to recover damages for Google's untimely removal of offending web links. Giancarlo F. Frosio, *The Right to Be Forgotten: Much Ado About Nothing*, 15 COLO. TECH. L.J. 307, 323 (2017). In that case, the Spanish court found that Google was required to pay damages from the time it "obtained actual knowledge of the offending links" to when it eventually removed them. *Google Inc.*, ECLI:EU:C:2014:317, ¶ 2 (reaching decision on damages in reliance on Council Directive 1995 O.J. (L 281) 31). And in Germany, the District Court of Heidelberg referenced the Court of Justice of the European Union's *González* decision in awarding damages against Google because it failed to promptly remove the links at issue upon notification. Frosio, *supra* note 206, at 323.

207. RESTATEMENT (SECOND) OF TORTS § 903 (AM. L. INST. 1979).

208. Jill Wieber Lens, *Honest Confusion: The Purpose of Compensatory Damages in Tort and Fraudulent Misrepresentation*, 59 U. KAN. L. REV. 231, 235 (2011).

209. *Id.*

internalize) the consequences of the wrong done, an end that is broadly consistent with the primary purpose of tort law.[210]

Compensatory damages are private in nature, with the victim allowed a direct action against their injurer to achieve the cost-shifting end,[211] rather than force the state, or the general public, to bear the cost of returning the victim to a pre-injured position:

> To the extent tort law is a forum for vindicating claims to repair, the victim's connection to his injurer is fundamental and analytic, not tenuous or contingent. That his injurer acted towards him in a way that gives rise to [] legitimate [and just] claim[s] . . . to compensation is the heart of the victim's assertion. This assertion connects the victim and his injurer in an analytic way: they are connected to one another and to no one else, in a way that makes a kind of sense of the structure of tort law that economic analysis simply cannot.[212]

Thus, to the extent the cost-shifting function of compensatory damages is concerned, shifting the burden to the wrongdoing party forces the cost to them rather than the victim or society more generally.[213]

This seems to me a fantastic fit, here, given the enormous profit these tech companies are generating via the acts outlined herein. Again, conceptualize these companies as essentially amortizing the value and sanctity of our private lives. To say that they are monetizing our personal information is a truism at this point, but, in reality, it is more than that. They are actually transferring value from every individual to themselves—they are, in a way, appropriating our personal lives, amortizing that which is valuable to us, and shifting that reduction in value to themselves. They are stealing our property, and every such act of theft impoverishes each of us.

---

210. The "primary purpose of tort law is 'that wronged persons should be compensated for their injuries and . . . those responsible for the wrong should bear the cost of their tortious conduct.'" Jews for Jesus, Inc. v. Rapp, 997 So. 2d 1098, 1105 (2008) (quoting Clay Elec. Coop. v. Johnson, 873 So. 2d 1182, 1190 (Fla. 2003)); *see also* Esmond v. Liscio, 224 A.2d 793, 799 (Pa. 1967) (noting that while compensatory damages tend to discourage tortious conduct, "[t]he function of compensatory damages is primarily to shift the loss from a wholly innocent party to one who is at fault"); JEFFERY J. SHAMPO, AM JUR. 2D TORTS § 2 (2d ed. 2021); Rizzuto v. Ladders, 905 A.2d 1165, 1173 (Conn. 2006) (quoting Lodge v. Arett Sales Corp., 717 A.2d 215 (1998)) (indicating that compensatory damages shift the burden of the cost from the innocent party to the responsible party or distribute the loss among appropriate entities based on the amount of harm the responsible party has caused).

211. Alexandra Klass, *Tort Experiments in the Laboratories of Democracy*, WM. & MARY L. REV. 1501, 1509-10 (2009).

212. Jules L. Colman, *The Structure of Tort* Law, 97 YALE L.J. 1233, 1249 (1998).

213. Klass, *supra* note 211, at 1509-10.

There is a handy analogy to this: nuisance.[214] The tech companies create enormous internal value and profit but bear none of the costs—the true cost in loss of privacy, in loss of property value—associated with that profit endeavor. What we need to do, then, is to redirect these costs—to cause the companies that profit to internalize the externalities that they are creating. Nuisance does this by standing, essentially, for the maxim that every person should use his own property so as not to injure that of another.[215] Of course, when we talk of "injury" in this context, what we really mean is activity that does not match its external-facing cost with external-facing benefit.[216] Though not arising directly from the use of property, per se, the tech companies are doing this very thing: engaging in activity that creates enormous cost for society, but benefits only the company. An apt analogy would be pursuing a nuisance claim for carbon emissions.[217] Facebook and Google are spewing pollution every bit as much as ExxonMobil or Chevron—and profiting the same way.

Damages, then, would tether the revenue to the cost. If Facebook had to bear the cost associated with having the private photos of your grandkids data-analyzed and data-mined, or otherwise utilized by the company or a third party—if you had the right to quantify what level of damage that caused you and to have Facebook compensate you accordingly—then Facebook would presumably cease such activities.

Of course, that is a bit of a simplification. Facebook (or whatever other horrible corporation is at hand) would still data-mine the photos of your grandkids, even if it had to reimburse you for the damage caused by such privacy violations, if the revenue it generated exceeded the quantifiable cost to you. That is what nuisance is, obviously—an attempt to create "optimal activity levels."[218] If, however, we really want to empower people to control their own property, then we can move even further by going beyond compensatory damages and permit those whose

214. Keith N. Hylton, *The Economics of Public Nuisance Laws and the New Enforcement Actions*, 18 SUP. CT. ECON. REV. 43, 68 (2010).

215. A private nuisance exists when one makes an improper use of his own property and, in that way, injures the land or some other right of his neighbor. *Id.* "Strict nuisance liability is desirable because it discourages the scale of an activity with negative externalities." *Id.*

216. "If, as nuisance law implicitly assumes, normal risks are balanced off by positive externalities, then excluding liability for normal risk leads to optimal activity levels." *Id.* at 59-60.

217. *See* Gary Bryner, *The Rapid Evolution of Climate Change Law*, UTAH BAR J., March-Apr. 2007, at 22 (discussing Comer v. Nationwide Mut. Ins. Co., 2006 U.S. Dist. LEXIS 33123 (S.D. Miss. Sept. 20, 2005)); Connecticut v. Am. Elec. Power, Inc., 406 F. Supp. 2d 265 (S.D.N.Y. 2005)).

218. *See* Hanssen, *supra* note 204, at 59-60.

privacy property rights are violated to pursue punitive damages, as well.[219]

Punitive damages are generally awarded in excess of compensatory damages in order to punish and deter.[220] They deter future behavior—of both the defendant and others—by imposing significant damages on that kind of behavior and signaling to everyone involved that future, similar behavior will result in economic damages that may push such behavior well beyond the pale of economically justifiable activity.

When the deterrent effect of punitive damages is aimed at the defendant themselves, scholars refer to it as special deterrence, and when the deterrent effect is aimed at others who would consider acting in a manner similar to the defendant, scholars refer to it as general deterrence.[221] Much like compensatory damages, punitive damages achieve the deterrence function, in part, by forcing the tortfeasor to internalize the cost of their wrongful conduct.[222] But, as some scholars point out, this means that punitive damages only really serve a deterrence function when they factor in the damages of other victims, not party to the case, who either chose not to bring their claim or failed to make the required showing.[223] Proponents of this theory also advocate for taking into consideration instances where tortfeasors escape liability.

---

219. Thus, echoing the original need to go beyond the GDPR's original damage scheme.

220. The Restatement Second of Torts describes the purpose of awarding punitive damages "to deter him and others like him from similar conduct in the future." RESTATEMENT (SECOND) OF TORTS, *supra* note 207, at § 903. This was explicitly recognized by the United States Supreme Court in *Pacific Mutual Life Insurance Company v. Haslip.*, 499 U.S. 1, 19 (1991) ("[A]s under the law of most States, punitive damages are imposed for purposes of retribution and deterrence.").

221. JACOB A. STEIN, STEIN ON PERSONAL INJURY Damages § 4:4 (3d ed. 1997). Jurisdictions adopting the deterrence rationale recognize punitive damage awards satisfy both the general and special deterrence purposes simultaneously. *See* STUART M. SPEISER ET AL., AMERICAN LAW OF TORTS § 8:46 (2008) (quoting Ray Dodge, Inc. v. Moore, 479 S.W.2d 518, 523 (Ark. 1972)).

222. Kevin S. Marshall & Patrick Fitzgerald, *Punitive Damages and the Supreme Court's Reasonable Relationship Test: Ignoring the Economics of Deterrence*, 19 ST. JOHN'S J. LEGAL COMMENT. 237, 251 (2005).

223. Sheila B. Scheuerman, *Two Worlds Collide: How the Supreme Court's Recent Punitive Damages Decisions Affect Class Actions*, 60 BAYLOR L. REV. 880, 890-91 (2008) (stating that "Professors Polinsky and Shavell urge a cost internalization approach to punitive damages. Under this theory, a punitive damages award is imposed in order to make up for the number of times . . . a tortfeasor escapes liability"). It is true that some other scholars say the deterrence function is best served through a "gain elimination" theory, which values a punitive damage award based on the illicit gains to different people and businesses—similar to disgorgement of profits. *Id.* at 891-92. But proponents of this view still advocate taking into consideration instances where tortfeasors escape liability. "Instead of taking into account the total harm caused, the calculation 'requires the court to divide the defendant's gain by the probability of liability.' '[T]he penalty should be at least as large as the minimum of the illicit gain expected by the offender.'" Jill Wieber Lens, *Justice Holmes's Bad Man and the Depleted Purposes of Punitive Damages*, 101 KY. L.J. 789, 796 (2013).

It is true that the ability of punitive damages to shape behavior has been considerably limited because of recent Supreme Court decisions limiting the availability of punitive damages. In *BMW of North America, Inc. v. Gore*,[224] the United States Supreme Court reversed a two-million-dollar punitive damage award as unconstitutional in violation of due process.[225] The Court laid down three guides to determine the propriety of a punitive damage award including: (1) the reprehensibility of the conduct; (2) the relationship between the harm suffered and the damage award; and (3) the difference between comparable civil penalties and the punitive damage award.[226]

The Court refined its punitive damage jurisprudence in *State Farm Automobile Insurance Co. v. Campbell*,[227] where the Court followed the *Gore* guideposts, but further explained that "[a] State cannot punish a defendant for conduct that may have been lawful where it occurred," even though that conduct may be relevant to the case.[228] The Court further significantly noted "few awards exceeding a single-digit ratio between punitive and compensatory damages, to a significant degree will satisfy due process."[229] The Court added that when "compensatory damages are substantial, then a lesser ratio, perhaps only equal to compensatory damages, can reach the outermost limit of the due process guarantee."[230] Taken together, these limitations dull the potential effect a punitive damages award would have in deterring future conduct.[231]

Indeed, in analyzing the effects of the United States Supreme Court's punitive-damage jurisprudence in federal common law, some scholars directly argue limitations like the ratio limitation undermine the deterrence function:

> The Court also gave no explanation regarding how the damages might achieve deterrence and hurt the damages' ability to achieve any notion of deterrence by failing to acknowledge the effects of under-detection and under-enforcement. Without some consideration of the chances of

224. 517 U.S. 559 (1996).
225. *Id.* at 575.
226. *Id.*
227. 538 U.S. 408 (2003).
228. *Id.* at 421.
229. *Id.* at 425.
230. *Id.*
231. *Cf.* Mathias v. Accor Economy Lodging, Inc., 347 F.3d 672, 675-77 (7th Cir. 2003) (acknowledging that limiting the availability of punitive damages lessens the ability of courts to punish reprehensible conduct). Obviously, limiting punitive damage awards naturally decreases their deterrent effect.

> escaping liability, punitive damages have less ability to achieve whatever type of deterrence the state might seek.[232]

This perhaps seems overwrought. The United States Department of Justice conducted a study on punitive damages in 2005 and found that general civil cases awarded punitive damages in only 5% of the cases where plaintiffs prevailed.[233] Further, general trends revealed punitive damage awards were down by 33% in general tort cases from 2001 to 2005, 46.1% down in medical malpractice cases over the same period, and 70.4% in product liability cases, also over the same period.[234] The median punitive damage amount awarded in all the cases surveyed was only between $38,000 and $50,000.[235] Given the relatively low rates and amounts at which punitive damages are awarded, the deterrent effect of punitive damages is on the decline—after all, their function cannot be fulfilled if they are not issued.[236]

But, to the point at hand, it certainly seems reasonable to conclude that punitive damages, as an enforcement mechanism, could help force large tech companies to respect others' property. This seems particularly apt, given the extent to which punitive damages speak to attempting to lasso in the damages incurred by non-parties. Again, returning to the nuisance analogy or example, what we are trying to do is cause these companies to truly bear the actual costs associated with their activities—of course, in the case at hand, but also more broadly. This is the only way to re-appropriate the broad property rights we all used to enjoy but have now ceded to Facebook. In any event, it seems almost certain that a small (probably a vanishingly small) percentage of people will ever seek to validate these claims in court—the damages we are talking about, on an individual basis, are very difficult to conceive of, or prove, and are unlikely to be high enough to justify the individual effort for most people. But the damages, on a society-wide level, are massive. Permitting punitive damages as a bridge between individual plaintiffs and the calamity of culture-wide property theft seems reasonable and

---

232. Lens, *supra* note 223, at 834.

233. *Fact Sheet: Punitive Damages: Rare, Reasonable and Limited*, CTR. FOR JUST. & DEMOCRACY (Apr. 2011), https://centerjd.org/content/fact-sheet-punitive-damages-rare-reasonable-and-limited-2011. It also found that medical malpractice and products liability cases only resulted in punitive damages in approximately 1% of successful cases. *Id.*

234. *Id.*

235. *Id.*

236. Marshall & Fitzgerald, *supra* note 222, at 249 & n.41 (2005) (stating that punitive damages are awarded in 2% to 4% of cases in studies conducted, and in cases where punitive damages were awarded they were for low amounts); Michael Conklin, *Factors Affecting Punitive Damage Awards*, FLA. COASTAL L. REV. (Forthcoming 2020) ("[Punitive Damages] are rare, occurring in only 6% of civil cases that result in a monetary award.").

directly in line with what punitive damages are typically thought to be for.[237]

Speculation is, of course, difficult in assessing how effective punitive damages really are at deterring conduct: the amount of damages; the nature of the industry involved; whether the defendant is a private citizen, a small business, a corporation, or a multi-national corporation—these things could all have an effect.[238] But the concept, as an economic principle, seems beyond question: disincentivizing property theft results in less property theft. And tying that directly to the ability of individuals to pursue what we are arguing is a stolen property right—it seems the perfect fit of remedy and right.

The right to be forgotten, then, seems like an excellent scaffold upon which to shore up our flagging rights. This is well beyond what American courts and statutes currently recognize, but is broadly consistent with equating privacy as property, in that it merely couches control and power in the hands of the owner. It is simply, in other words, allowing us to control what is ours—to treat our castle as our own, as it were. But hanging American-style compensatory and punitive damages on that scaffolding would go even further and do even more to help us all protect what is ours.

---

237. An analogy would be the idea of permitting a property owner to sue for punitive damages for simple trespass, in certain situations. Imagine, for instance, somebody who owns a home on a very busy corner, favored by many, many passers-by. Every day, thousands of pedestrians cut across the property, damaging it badly. If the property owner can sue each one for their contribution to the damage to her home, that is good—it does, in fact, cause the defendant pedestrian to internalize the cost of the ten to fifteen seconds that he cuts off of his commute each day. However, the homeowner would have to sue thousands of people. Unless she can pursue punitive damages. If she could get a damages award of, say, $10,000 (or $100,000 or $1,000,000—or whatever number is needed), then each pedestrian will likely second-guess their trespass, for, while it is unlikely that any one of them will be sued, the consequences of being that unlucky defendant are too great to ignore. The analogy is not perfect, but it seems reasonably similar, and serves to demonstrate the concept, as applied to property theft or trespass.

238. The McDonald's coffee burn case serves to illustrate the inadequacies of punitive damages awards in shaping conduct. Liebeck v. McDonald's Restaurants, P.T.S., Inc., 1995 WL 360309, at *1 (D.N.M. Aug. 18, 1994); Allison Torres Burtka, Liebeck v. McDonald's: *The Hot Coffee Case,* AM. MUSEUM TORT L., https://www.tortmuseum.org/liebeck-v-mcdonalds (last visited Aug. 1, 2021). In the case, a 79-year-old woman was served coffee from McDonald's that, when spilled, was hot enough to cause third-degree burns on 16% of her body. *Liebeck*, 1995 WL 360309 at *1. The jury awarded the woman $160,000 in compensatory damages and originally $2.7 million in punitive damages. *See id.* The trial court reduced the punitive damage award to $480,000, but ultimately the case was settled while this award was on appeal. *See id.* Even after this case awarding punitive damages, and the over-700 similar instances of coffee burns, McDonald's did not change the temperature at which it kept its coffee in the wake of the McDonald's coffee case. *See id.*

VI. CONCLUSION

The law has shifted without us noticing much. Privacy rights, which seem at an all-time low ebb, are really a function of property law, rather than tort law.[239] Though traditionally conceived of as an outgrowth of the latter area of law, this is really an almost *in rem* right that speaks to others and warns them of how they have to interact with the *owner*.[240] Unfortunately, that shift has been accompanied by an almost wholesale abandonment of that property right.[241] Our legal system should acknowledge this and arm people with the tools they need to understand, appreciate, and protect their rights. Adopting a European-style right to be forgotten will go a long way in that direction and will ultimately do much to reverse the massive losses suffered by us all in the last one or two decades.[242] Only such a systemic change will set things right and allow us to live in our homes and enjoy our lives without the omnipresent concern that someone is watching over us and monetizing our lives.

APPENDIX A

Here are the questions and responses to the 2019 survey I gave to my students:

Question 1
How often do you use social media?

5+ times per day.....36.6% (34 respondents)
1-3 times per day.....43% (40 respondents)
1-3 times per week.....14% (13 respondents)
Never..... 6.5% (6 respondents)

Question 2
How often do you use email?

5+ times per day.....52.7% (49 respondents)
1-3 times per day.....41.9% (39 respondents)
1-3 times per week..... 5.4% (5 respondents)
Never..... 0% (0 respondents)

239. *See supra* Part IV.
240. *See supra* Part IV.
241. *See supra* Part V.A.
242. *See supra* Part V.B.

Question 3
How often do you conduct internet searches?

5+ times per day.....52.7% (49 respondents)
1-3 times per day.....41.9% (39 respondents)
1-3 times per week..... 5.4% (5 respondents)
Never..... 0% (0 respondents)

Question 4
How often do you use GPS?

Multiple times per day .....12% (11 respondents)
A few times per week.....60.9% (56 respondents)
Rarely.....26.1% (24 respondents)
Never..... 1.1% (1 respondent)

Question 5
Do you expect third parties to be able to access the content you post/communicate?

Yes .....64.1% (59 respondents)
No.....35.9% (33 respondents)

Question 6
Do you expect the providers of the services you're utilizing to be able to access the content you post/communicate?

Yes .....75% (69 respondents)
No.....25% (33 respondents)

Question 7
Do you expect the providers of the servicers you're utilizing to be able to sell, to third parties, the content you post/communicate?

Yes .....40.9% (38 respondents)
No.....59.1% (55 respondents)

Question 8
If you answered yes to [the above] questions, have you altered any privacy settings within the [relevant] apps?

Yes .....79.6% (74 respondents)
No.....20.4% (19 respondents)