University of Richmond Law Review

Volume 55 | Issue 2 Article 3

1-1-2021

Trade Secrets and Personal Secrets

Lital Helman
Ono Academic College

TRADE SECRETS AND PERSONAL SECRETS

Lital Helman *

Two separate systems of law govern secrets. The first one concerns trade secrets: confidential business information that provides an enterprise with a competitive edge. The unauthorized use of a trade secret by persons other than the holder is regarded as an unfair practice and a violation of the trade secret. The second system protects personal secrets. This system is information privacy law. Information privacy law deals with the regulation, storing, and use of personal information of individuals. While both systems concern secrets, the laws that govern them comprise entirely different regimes, and have almost nothing in common.

This Article aims to examine the different ways in which the law protects commercial and private secrets. The most fundamental difference is that the trade secrets regime forbids the unauthorized use of a business's confidential information, while privacy law does not forbid the unauthorized use of a person's confidential information. If a firm takes measures to protect information of value, the law forbids the use of this information. Yet, as to personal secrets, the mere fact that someone has taken measures to protect their privacy does not create an obligation to avoid misappropriation of their information.

This asymmetry of protection is especially troubling when these two systems collide. For example, certain information can be subject to a trade secret of a company, while at the same time strongly 'belong' to an individual. Trade secret laws often prevent individuals from learning about uses that firms conduct with their own private information.

* Assistant Professor (Senior Lecturer in Law), Ono Academic College. The author is grateful to Michael Birnhack, Rochelle Dreyfuss, Daniel Gervais, Sonya Katyal, Gideon Parchomovsky, Joel Reidenberg of blessed memory, Michael Risch, Sharon Sandeen, Ofer Tur Sinai, Deepa Varadarajan, Felix Wu, and Tal Zarsky, for helpful insights and advice. The author is also thankful for input received in the 2020 Intellectual Property Scholars Conference and in the Ono Faculty Workshop.

This Article explores the extent to which the distinction between the two laws is justified, and analyzes whether the law of information privacy can be modified to resemble trade secrecy more closely. This exploration is particularly relevant under today's climate of commodification of private information, where both users and companies make transactional use of personal data on a regular basis.

INTRODUCTION

Two separate systems of law govern secrets.[1] The first one concerns trade secrets: confidential business information that provides an enterprise with a competitive edge.[2] The unauthorized use of a trade secret is regarded as an unfair practice and a violation of trade secret law.[3] The second system protects personal secrets. This system is information privacy law.[4] Information privacy law deals with the regulation, storing, and use of personal information of individuals.[5] While both systems concern secrets, the laws that govern them comprise entirely different regimes, and have almost nothing in common.[6]

The fundamental difference between the regimes is that trade secret law forbids the unauthorized use of a business's confidential information, while privacy law does not forbid the unauthorized use of a person's confidential information.[7] If a firm takes measures to protect information of value, the law forbids the use of this information.[8] Yet, as to personal secrets, the mere fact that someone has taken measures to protect their privacy does not create an obligation to avoid misappropriation of their information.[9]

1. There are, of course, other laws that concern confidentiality in particular contexts, such as contract law, criminal law, etc. *See, e.g.*, Richard A. Posner, *Blackmail, Privacy, and Freedom of Contract*, 141 U. PA. L. REV. 1817, 1818 (1993) (discussing the criminal offense of blackmail).

2. *See* UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985); *see also infra* section II.A.1.

3. *See* UNIF. TRADE SECRETS ACT § 1(2)*; see also infra* section II.A.1.

4. *See infra* section I.B.

5. *See infra* section I.B.

6. *See infra* section I.B.

7. *See infra* Part I.

8. *See infra* section I.A.

9. *See infra* section I.B.

This Article explores the extent to which the distinction between the two regimes is justified and analyzes whether privacy law can be modified to resemble that of trade secrecy more closely. My main thesis is that adoption of relevant trade secrecy doctrines can encourage both responsible sharing and responsible use of information in the context of information privacy law. Despite obvious differences, trade secret law forms an equivalent regime to information privacy law, with a solid set of caselaw, robust policy justifications, and relevant experience in how to protect secrets under the law. While the analogy between trade secrecy and information privacy laws has its limits, it is nonetheless a useful framework with which to rethink information privacy.

The first contribution of this Article to the literature is the uncovering of the doctrinal differences between trade secrecy and information privacy law. I show that trade secret law offers more robust protection in five critical areas. First, trade secret protection attaches to *any* valuable information that the owner of which treats as secret. In contrast, privacy law denotes a categorical, objective view of sensitive information, regardless of individual attitudes or preferences of the information subjects.[10] Second, trade secret protection is triggered when firms take reasonable efforts to maintain secrecy.[11] Yet, precautions that individuals take when sharing information have no legal effect in the privacy arena.[12] Third, while trade secrecy protects against downstream, conscious use of misappropriated secrets, privacy protection does not extend against third parties.[13] Fourth, privacy remedies pale in comparison to the remedies available for trade secret owners.[14] Finally, trade secret law is well enforced in court, while privacy law is increasingly the domain of administrative enforcement at the Federal Trade Commission.[15]

The result of these differences is a robust trade secret law alongside a weak and equivocal privacy protection. This asymmetry of protection is especially troubling when these two systems collide.[16] An example of collisions includes cases where certain information

10. *See infra* section I.C.1.
11. *See infra* section I.C.1.
12. *See infra* section I.C.2.
13. *See infra* section I.C.3.
14. *See infra* section I.C.4.
15. *See infra* section I.C.5.
16. *See infra* section II.A.2.

can be subject to a trade secret of a company, while at the same time strongly 'belong' to an individual. Trade secret law can, in such cases, limit individuals from accessing, correcting, or challenging uses of such information.[17]

The second contribution of this Article to the literature is in providing an analysis of the normative foundations that trade secret law and information privacy law have in common. This Article argues that these shared foundations—while not aiming to comprise the entire underpinnings of privacy protection—justify doctrinal borrowing from trade secret law. Indeed, it is broadly understood that the basic objective of trade secrecy is to encourage mindful information sharing in the market.[18] At its core, trade secret law, like other intellectual property law, answers Arrow's disclosure paradox—that without legal protection, information would not be shared.[19] To facilitate mindful information sharing while discouraging careless sharing, trade secret protection attaches to valuable information if the secret holder used safeguards while sharing the information.[20] In striking contrast, extant privacy law treats information disclosure like a fault. The governing standard for privacy protection is "expectations of privacy," and this standard typically leads courts to deny protection of information that was originally shared voluntarily.[21] Treating personal disclosure like a fault makes very little sense in an economy that is fueled by sharing personal information.[22] Privacy law should instead aim to encourage individuals to share information in a responsible manner, as trade secrecy does.

Trade secret law also aims to obviate investments by secret owners in wasteful self-help measures that firms can take to prevent the disclosure of their secrets.[23] But the law unjustly recognizes no such concern in the privacy context. Thus, the law grants no legal effect to safeguards that individuals may take to protect the information that they share. The result is that nothing in current law

17. *See infra* section II.A.2.
18. *See infra* section II.A.1.a.
19. *See infra* note 180 and accompanying text.
20. *See infra* section II.A.1.a.
21. *See infra* notes 78–83 and accompanying text.
22. *See, e.g.*, Sebastian Sevignani, *The Commodification of Privacy on the Internet*, 40 SCI. & PUB. POL'Y 733, 733–36 (2013).
23. *See infra* section II.A.1.b.

incentivizes users to use safeguards responsively. Individuals react to this reality in one of two ways. They either use no safeguards at all when sharing information or engage in information-obscuring methods that are not only wasteful but may also have negative externalities, such as interfering with law enforcement, slowing internet use, or generating other risks.[24]

Finally, in today's marketplace, where transactional use of private data is commonplace, even trade secret law's objective to further business ethics applies to information privacy. Indeed, the same concern that companies have—that misappropriators of their secrets will gain an unfair advantage over them based on their own information—is now shared by individuals. One of the most prevalent privacy complaints today is that privacy violators have used personal information to enhance their bargaining power against the information's subject, by engaging in price discrimination or by exploiting the individuals' vulnerabilities in various other ways.[25]

This normative analysis is important even though it does not—and does not aim to—capture the full theoretical and normative depth of privacy protection. This analysis is important because uncertainty around the underpinnings of privacy has prevented courts and other policy makers from effectively addressing contemporary privacy harms. Such uncertainty has also focused much of the privacy scholarship on theorizing, defining, contextualizing, categorizing, and justifying the right to privacy rather than developing its doctrines and remedying intrusions.[26] Indeed, exposing the underlying rationales of privacy law is an ongoing—and important—endeavor, and I myself have contributed to it.[27] Yet the stakes for privacy have increased exponentially in the information age, and workable conceptual frameworks that can address privacy

24. *See infra* notes 188–89 and accompanying text.

25. *See infra* note 191 and accompanying text.

26. *See, e.g.*, Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653, 657 n.21 (2019) ("One of the more common type of privacy article is the categorization article, that is, an article that seeks to impose order on privacy by defining and describing subcategories o[f] the phenomenon, usually drawing on nonlegal social science methods and perspectives in the process."); Anita Bernstein, *Real Remedies for Virtual Injuries*, 90 N.C. L. REV. 1457, 1462 (2012) ("[T]he causes of action available for virtual injuries probably do a better job of describing than remedying.").

27. *See generally* Lital Helman, *Pay for (Privacy) Performance: Holding Social Network Executives Accountable for Breaches in Data Privacy Protection*, 84 BROOK. L. REV. 523 (2019) (discussing the current data protection privacy laws in the United States and demonstrating an ongoing need for a legal framework that can accommodate the expansion of modern technology and social networking).

concerns are required in the academic literature alongside this endeavor.[28]

Let us now take the above analysis one step forward and demonstrate how doctrinal adoption from trade secret law can have positive normative payoffs in the privacy realm. One doctrine that privacy law can effectively borrow from trade secret law is *the reasonable precautions standard*. This standard means that firms can effectuate trade secrecy protection by taking reasonable measures to protect their valuable information.[29] Embracing this doctrine in the privacy context (with necessary adjustments) would allow users to show that they took reasonable precautions to safeguard their information even in cases where they shared the information voluntarily. Proving "reasonable precautions" would work to establish "expectations of privacy," and thus trigger privacy protection.[30] Such a standard in information privacy law could yield dramatic improvements over the current regime. First, it would enhance privacy protection and create certainty in the market and in courts. Second, it would generate incentives for users and businesses to share information and to use personal information of others in a responsible manner. Finally, this standard would boost innovation, because jurisdiction around reasonableness would incentivize the industry to offer productive self-measures for privacy and curtail the creation of bad precautions that are so common today.

While this Article is not the first to ponder the connection between information privacy law and intellectual property regimes,[31] it is the first to offer a normative and doctrinal analysis of information privacy and trade secret law in light of each other. It is also the first to propose a new conceptual framework for privacy law

28. *See* Scholz, *supra* note 26, at 657 n.21 ("The problem with many categorization articles is that they do not make clear how precisely these categorizations will help lead to better-protected privacy rights, beyond the general observation that it will provide policymakers with more information and 'clarity.'").

29. *See infra* text accompanying note 99.

30. *See infra* section I.C.2.

31. Two articles to date touched on this connection. *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1151–58 (2000) (analyzing whether privacy should be perceived as intellectual property); Sharon K. Sandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667, 669–70 (comparing the development of trade secrets and privacy law); *see also* Gianclaudio Malgieri, *Trade Secrets v Personal Data: A Possible Solution for Balancing Rights*, 6 INT'L DATA PRIVACY L. 102, 102 (2016) (discussing a particular conflict related to database protection under European law).

that can help the law overcome some of its most pressing contemporary problems.

This Article unfolds as follows. The first Part describes the law of trade secrecy and the law of privacy, and highlights the doctrinal similarities and differences between them. The second Part analyzes the theoretical underpinnings of the differences between the trade secrecy and privacy regimes, and inquires to what extent they are justified. Based on this analysis, I consider harmonization of some of the doctrines of trade secrecy and privacy law. A short conclusion ensues.

I. THE LAWS OF TRADE SECRECY AND OF PRIVACY

This Part examines the main doctrines of trade secret law and privacy law in the United States.[32] As I show below, trade secrecy is a robust intellectual property right that is well-defined and well-enforced by the courts. In contrast, privacy law is an incoherent landscape, riddled with specific regulations and enforced mainly by the administrative branch.

A. *Overview of Trade Secret Law*

Trade secret protection concerns valuable information that is not generally known to the public, when the owner of such information undertakes reasonable precautions to preserve secrecy.[33] Trade secret protection originated in state common law and unfair-competition principles.[34] But what started among individual states' common law has since become a powerful intellectual property right across the nation.[35] Almost all states adopted a version

32. For a historical assessment of the development of both trade secret law and privacy law, from common law to their expression in the *Restatement (Second) of Torts*, see generally Sandeen, *supra* note 31.

33. For early statements of these conditions, see, e.g., Nat'l Tube Co. v. E. Tube Co., 3 Ohio C.C. (n.s.) 459, 462 (1902), *aff'd*, 70 N.E. 1127 (Ohio 1903); Pressed Steel Car Co. v. Standard Steel Car Co., 60 A. 4, 9–10 (Pa. 1904); Eastman Co. v. Reichenbach, 20 N.Y.S. 110, 111, 116 (N.Y. Sup. Ct. 1892), *aff'd sub nom*. Eastman Kodak Co. v. Reighenbach, 29 N.Y.S. 1143 (N.Y. Gen. Term 1894).

34. *See* James Pooley, *The Myth of the Trade Secret Troll: Why the Defend Trade Secrets Act Improves the Protection of Commercial Information*, 23 GEO. MASON L. REV. 1045, 1048 (2016). For a detailed history of the evolution of trade secret law, see Sharon K. Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 493, 498, 500–01 (2010).

35. *See* Joseph P. Fishman & Deepa Varadarajan, *Similar Secrets*, 167 U. PA. L. REV.

of the 1979 United Trade Secrets Act ("UTSA"),[36] and in 2016, Congress passed the Defend Trade Secrets Act ("DTSA"), introducing federal trade secret protection that largely mirrors the UTSA.[37] In the words of Peter Menell, trade secrets have become "the most pervasive form of intellectual property in the modern economy."[38]

The scope of trade secrets is defined expansively.[39] Trade secrets can apply to information of any sort, such as technology, operations, strategy, financials, staff, and customers.[40] To qualify for protection as a trade secret, the information must meet three criteria. First, it must have "independent economic value, actual or potential."[41] Second, it must not be "generally known" or "readily ascertainable."[42] Third, the owner must take reasonable efforts to maintain its secrecy.[43] A trade secret has no fixed term—protection lasts as long as the secret is kept as such.[44]

Once a trade secret is established, its owner can enforce the trade secret against misappropriators. Misappropriation of trade

1051, 1055 (2019) ("Trade secrecy was once a decentralized product of individual states' common law. It's now a major IP scheme.").

36. *See* UNIF. TRADE SECRETS ACT (UNIF. LAW COMM'N 1985); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39–45 (AM. LAW INST. 1995) (outlining the principles of trade secret law). States have not always passed the UTSA verbatim. *See, e.g.*, CAL. CIV. CODE § 3426. New York, North Carolina, and Massachusetts have not adopted the UTSA. North Carolina has a similar statute, whereas New York and Massachusetts protect trade secrets under common law. *See* Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 CALIF. L. REV. 1, 3 n.7, 16 n.76 (2017); *see also* Pooley, *supra* note 34, at 1051 (discussing the implementation of the UTSA in courts).

37. *See* Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376; *see also* Fishman & Varadarajan, *supra* note 35, at 1055 (noting that trade secrecy is considered "a major IP scheme").

38. *See, e.g.*, Menell, *supra* note 36, at 3; *see also* JOHN E. JANKOWSKI, NAT'L SCI. FOUND., BUSINESS USE OF INTELLECTUAL PROPERTY PROTECTION DOCUMENTED IN NSF SURVEY 4 (2012), https://wayback.archive-it.org/5902/20150628145722/http://www.nsf.gov/statistics/infbrief/nsf12307/nsf12307.pdf [https://perma.cc/EL52-5NMJ] (reporting survey results that show that firms find trade secrets more important to their business than other IP).

39. *See, e.g.*, PETER S. MENELL, MARK A. LEMLEY & ROBERT P. MERGES, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE: 2019, at 36 (2019).

40. *See* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW INST. 1939); *see also* Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 780 (2007).

41. *See* UNIF. TRADE SECRETS ACT § 1(4)(i) (UNIF. LAW COMM'N 1985).

42. *See id.*

43. *See id.* § 1(4)(ii).

44. *See* Fishman & Varadarajan, *supra* note 35, at 1063 (noting that trade secrecy does not expire if the secret remains undisclosed); *see also* David S. Levine & Christopher B. Seaman, *The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act*, 53 WAKE FOREST L. REV. 105, 146 (2018).

secrets can occur either by acquisition of the information via "improper means,"[45] or by disclosing or using it in violation of a confidentiality duty.[46] Most cases of misappropriation fall into the second category; namely, they involve defendants who acquired the secret legitimately, but are using or disclosing it in breach of a confidentiality duty, such as through former employees or business associates.[47] Each of these acts—acquisition, disclosure, and use of a trade secret—forms an independent basis for trade secret liability.[48]

Trade secret law enforces the entitlement through both property and liability rules.[49] Thus, when a trade secret case is successful, an injunction is the most likely remedy.[50] Courts can enjoin either

45. *See* UNIF. TRADE SECRETS ACT § 1(1) (UNIF. LAW COMM'N 1985) ("[I]mproper means includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."); *see also* Telex Corp. v. Int'l Bus. Machs. Corp., 510 F.2d 894, 897–98 (10th Cir. 1975) (interpreting the prerequisite); Univ. Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 528 (5th Cir. 1974).

46. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 41 (AM. LAW INST. 1995) (defining breach of confidence as violations of express or implied duties of confidence); *see also* Union Carbide Corp. v. Exxon Corp., 77 F.3d 677, 678–79 (2d Cir. 1996); Tracer Research Corp. v. Nat'l Envtl. Servs. Co., 42 F.3d 1292, 1293 (9th Cir. 1994); Comprehensive Techs. Int'l, Inc. v. Software Artisans, Inc., 3 F.3d 730, 732 (4th Cir. 1993); Smith v. Snap-On Tools Corp., 833 F.2d 578, 579 (5th Cir. 1987); Metallurgical Indus., Inc. v. Fourtek, Inc., 790 F.2d 1195, 1197–98 (5th Cir. 1986); SI Handling Sys., Inc. v. Heisley, 753 F.2d 1244, 1251 (3d Cir. 1985); Roberts v. Sears, Roebuck & Co., 573 F.2d 976, 978 (7th Cir. 1978); Data Gen. Corp. v. Grumman Sys. Support Corp., 834 F. Supp. 477, 481 (D. Mass. 1992).

47. *See* Fishman & Varadarajan, *supra* note 35, at 1063–64 (quoting statistics that show that "[t]he vast majority of trade secret cases . . . involve departing employees accused of breaching express confidentiality duties," and that in the first year of the DTSA, "two-thirds of all cases . . . involv[ed] a current or former employee, a quarter involving a current or former business partner, and only a tenth involving parties without any prior relationship.").

48. *See, e.g.*, GlobeSpan, Inc. v. O'Neill, 151 F. Supp. 2d 1229, 1235 (C.D. Cal. 2001).

49. *See, e.g.*, Menell, *supra* note 36, at 46–47 ("[T]rade secret law allocates the entitlement to the trade secret information to the company and enforces that entitlement through both property and liability rules.").

50. *See* UNIF. TRADE SECRETS ACT § 2(a) (UNIF. LAW COMM'N 1985); Fishman & Varadarajan, *supra* note 35, at 1112 (encouraging the trend of some courts to limit the injunction's duration to the estimated length of time it would have taken the competitor to develop the secret independently); *see also* Halliburton Energy Servs., Inc. v. Axis Techs., LLC, 444 S.W.3d 251, 257 (Tex. App. 2014) ("[T]he 'usual equitable order' in a trade secret misappropriation case is a perpetual injunction against the wrongdoer."). *See generally* E.I. DuPont de Nemours & Co. v. Kolon Indus., Inc., 894 F. Supp. 2d 691, 706 (E.D. Va. 2012); Microstrategy, Inc. v. Bus. Objects, S.A., 661 F. Supp. 2d 548, 553 (E.D. Va. 2009) (granting injunction); Flotec, Inc. v. S. Research, Inc., 16 F. Supp. 2d 992 (S.D. Ind. 1998) (enjoining former employee from disclosure of trade secrets to new employer); Cybertek Computer Prods., Inc. v. Whitfield, 203 U.S.P.Q. (BNA) 1020 (Cal. App. Dep't Super. Ct. 1977) (enjoining former employee).

actual or threatened misappropriation, and require misappropriators (or potential misappropriators) to refrain from using or disclosing the secret.[51] An injunction is often granted alongside compensation, including actual damages and unjust enrichment.[52] Courts may also award exemplary damages of up to double the compensatory amount and attorneys' fees in cases of willful and malicious misappropriation.[53]

B. *Overview of Privacy Law*

Unlike trade secrecy's robust protection in state and federal law, privacy law is weak and fragmented. It is a patchwork of constitutional protections, federal and state statutes, tort law, regulatory rules, treaties, self-regulation, and administrative regulation.[54] Some of these norms apply broadly, but most of them apply only in certain economic sectors or industries.[55]

51. *See* UNIF. TRADE SECRETS ACT § 2(a) (UNIF. LAW COMM'N 1985).

52. *See* Elizabeth A. Rowe, *Unpacking Trade Secret Damages*, 55 HOUS. L. REV. 155, 162, 195–96 (2017) (citing empirical scholarship demonstrating that "a trade secret owner who prevails on damages is likely to also receive a permanent injunction"); *see also* RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 1 (AM. LAW INST. 2011).

53. *See* UNIF. TRADE SECRETS ACT §§ 2, 3(b), 4(iii) (UNIF. LAW COMM'N 1985).

54. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1211 (2004) ("Suspicion of the state has always stood at the foundation of American privacy thinking, and American scholarly writing and court doctrine continue to take it for granted that the state is the prime enemy of our privacy."); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1430 (2001) ("Privacy law consists of a mosaic of various types of law: tort law, constitutional law, federal and state statutory law, evidentiary privileges, property law, and contract law."); Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 61–62 (2000) (comparing the "European scheme of empowering national supervisory authorities" to the alleged "decentralized U.S. approach"); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1632 (1999) (criticizing the patchwork of privacy law).

55. *See* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 877, 887–88 (2003) (arguing that "privacy is protected only through an amalgam of narrowly targeted rules. . . . leav[ing] many significant gaps and fewer clear remedies"); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014) ("There is a law for video records and a different law for cable records. The Health Insurance Portability and Accountability Act (HIPAA) protects the privacy of health data, but a different regime governs the privacy of financial data. In fact, there are several laws that regulate financial data depending upon the industry, and health data is not even uniformly protected: Not all health data is covered by HIPAA, and various constitutional and state laws can protect health data more stringently than HIPAA. Although state data security breach notification laws apply broadly across different industries, most state privacy laws are sectoral as well." (citations omitted)); Christian Nisttáhuz, Comment, *Fifty States of Gray: A Comparative Analysis of "Revenge-Porn" Legislation*

Famously, in 1960, Prosser identified four torts that confer information privacy: intrusion upon seclusion, publication of private facts, false-light publicity, and misappropriation of name or likeness.[56] The four torts offer a basis for liability for privacy harms in suitable cases, together with other torts that concern wrongful business practices, such as fraud, theft, tortious interference with contract, and breach of fiduciary duty.[57] In the context of information privacy, however, the relevance of these torts has eroded with time, as they struggle to apply to contemporary challenges of information privacy.[58]

Alongside tort law, contract law can, at least in theory, protect privacy law in circumstances of broken promises for confidentiality.[59] Contract theories of liability could in principle apply to agreements between users and online platforms—in particular, privacy policies.[60] However, in practice, contract theories are rarely attempted, and courts have been reluctant to interpret privacy policies as binding contracts.[61] Promissory estoppel—the equitable

Throughout the United States and Texas's Relationship Privacy Act, 50 TEX. TECH L. REV. 333, 357–60 (2018) (surveying states' legislation on revenge pornography).

56. *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977) (addressing intrusion upon seclusion tort); *id.* § 652C (addressing appropriation tort); *id.* § 652D (addressing public disclosure of private facts tort); *id.* § 652E (addressing false light tort); *see also* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 2, 6, 8 (2008); Sandeen, *supra* note 31, at 687–92. *See generally* WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS § 107 (1st ed. 1941).

57. *See* Scholz, *supra* note 26, at 670 (arguing that "contract law and related interests may be the primary source of consumer privacy rights is the status quo"). *See generally* GABRIEL ABEND, THE MORAL BACKGROUND: AN INQUIRY INTO THE HISTORY OF BUSINESS ETHICS (2014); NATHAN B. OMAN, THE DIGNITY OF COMMERCE: MARKETS AND THE MORAL FOUNDATIONS OF CONTRACT LAW (2016).

58. *See* Solove & Hartzog, *supra* note 55, at 587 (explaining why the four torts did not apply to many new challenges).

59. *See* KIM LANE SCHEPPELE, LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW 222–26 (1988); Scholz, *supra* note 26, at 669 (asserting that even implied warranties or fiduciary duties may suffice to establish liability, given the infeasibility of negotiated agreements).

60. *See* Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 91–92 (1999) (explaining ways in which website privacy policies resemble contracts); *see also* Scholz, *supra* note 26, at 669 (stating that firms routinely represent more privacy than they deliver).

61. *See, e.g.*, Smith v. Trusted Universal Standards in Elec. Transactions, Inc., No. 09-4567 (RBK/KMW), 2010 U.S. Dist. LEXIS 43360, at *28–30 (D.N.J. May 4, 2010) ("Some courts have held that general statements like 'privacy policies' do not suffice to form a contract because they are not sufficiently definite."); *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 316–18 (E.D.N.Y. 2005) (not finding JetBlue's privacy policy to form contractual obligation); Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) ("[B]road statements of company policy do not generally give rise to contract claims."); *In re* Nw. Airlines Privacy Litig., No. 04-126 (PAM/JSM), 2004 U.S. Dist. LEXIS 10580, at

doctrine that protects those who detrimentally rely upon promises—could also form a basis for privacy liability.[62] But courts have declined to enforce it in the privacy context, mainly due to a lack of detrimental reliance.[63] As a result, despite the theoretical applicability of contract law and the support of some scholars of this cause of action,[64] cases involving contract theories are marginal.[65] As Daniel Solove and Woodrow Hartzog stated, "Today, contract law—formal contract and promissory estoppel—plays hardly any role in the protection of information privacy, at least vis-à-vis websites with privacy policies."[66]

Throughout the years, federal and state laws have added specific privacy protections that apply to certain industries, economic sectors, or particular conduct.[67] California has taken a leading role in this trend, with some spillover effects on other states.[68] Yet, as dig-

*15–17 (D. Minn. June 6, 2004) (rejecting claim that Northwest Airlines' privacy statement constitutes unilateral contract); Daniels v. JP Morgan Chase Bank, N.A., No. 22575/09, 2011 WL 4443599, at *7–8 (N.Y. Sup. Ct. Sept. 22, 2011) (dismissing contract claim against bank's disclosure of secret materials during subpoena). *But see* Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 864–65 (N.D. Cal. 2011) (declining to dismiss a contractual claim based on privacy policy); Omri Ben-Shahar & Lior Jacob Strahilevitz, *Contracting over Privacy: Introduction*, 45 J. LEGAL STUD. S1, S7, S10 (2016) (showing that courts sometimes view privacy policies as binding).

62. *See* RESTATEMENT (SECOND) OF CONTRACTS § 90 (AM. LAW INST. 1981); *see also* Scholz, *supra* note 26, at 670 ("Even where representation by a company is not binding in contract, a showing of reliance on a promise provides grounds for an individual to seek relief in promissory estoppel.").

63. *See, e.g.*, Smith v. Trusted Universal Standards in Elec. Transactions, Inc., No. 09-4567 (RBK/KMW), 2011 U.S. Dist. LEXIS 26757, at *32 n.10 (D.N.J. Mar. 15, 2011) ("[T]here is no evidence . . . that Plaintiff relied on a promise . . . . Therefore, no reasonable jury could conclude that a contract existed between the parties based upon a doctrine of promissory estoppel.").

64. *See* Scholz, *supra* note 26, at 668–70.

65. *See* Solove & Hartzog, *supra* note 55, at 596. Courts sometimes dismiss contract-based privacy cases based on lack of finding of harm. *See infra* note 134.

66. *See* Solove & Hartzog, *supra* note 55, at 596–97.

67. *See, e.g.*, Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a); Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946 (codified as amended at 44 U.S.C. §§ 3541–3549). Other areas where privacy standards are predefined include, for example, limitations on the collection of personal data by government agencies, and limits on the interception of electronic data transmissions in the context of employment. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); *see also supra* note 55.

68. California law focuses mainly on limitations on data trading (rather than data collection). Parts of the Californian law have become the de facto national standard, for example the California Online Privacy Protection Act, CAL. BUS. & PROF. CODE §§ 22575–22579 (imposing requirements on privacy policies regarding California resident consumers). Driven by the continued rise in consumer data breaches, California passed the California

ital technologies reduced the costs of collecting and analyzing individual-level data, vulnerability to privacy violation expanded faster than these laws.[69] Some of the most troubling practices of increasingly dominant industries—such as data collection and analytics by data brokers, merchants, social networks, and other digital services—fall outside of the regulated scope.[70]

Self-regulation largely fills the void.[71] Individual firms, and in some contexts, industry groups, largely design their own privacy policies.[72] The Federal Trade Commission ("FTC") oversees this self-regulation regime, relying upon its broad powers under Section 5 of the FTC Act "to prevent . . . unfair or deceptive acts or practices in commerce."[73] Gradually, as privacy concerns that are

Consumer Privacy Act ("CCPA") in 2018. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100. "While the CCPA is likely to undergo substantial changes, it clearly sets to strengthen privacy protection in California, with likely spillover" to other states. *See* Helman, *supra* note 27, at 529 n.29.

69. *See* James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 58 (2003) (discussing "holes in this patchwork of sector-specific privacy laws"); Avi Goldfarb & Catherine Tucker, *Privacy and Innovation,* 12 INNOVATION POL'Y & ECONOMY 65 (2012) (arguing that contemporary practices are often unregulated).

70. Goldfarb & Tucker, *supra* note 69.

71. *See* Dennys Marcelo Antonialli, Note, *Watch Your Virtual Steps: An Empirical Study of the Use of Online Tracking Technologies in Different Regulatory Regimes*, 8 STAN. J. C.R. & C.L. 323, 333 (2012) ("In the United States, the debate revolves around improving the self-regulatory regime, rather than adopting a more normative framework."); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 251 (2011) ("Congress has declined to follow the European model of a dedicated privacy administrator."); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 2 (2001) (describing the debate between self-regulation and market solutions, and privacy rights and regulation).

72. *See* Helman, *supra* note 27, at 527–28 (showing that "in most cases in the United States, individual firms, and in some contexts, industry groups, determine their own level of privacy protection"). Examples of industry group regulation include, inter alia, the "Digital Advertising Alliance's Self-Regulatory Program" for online behavioral advertising, which enables users to opt out of some targeted advertising, and "www.aboutads.info," a partnership of public and private parties which provides information about online advertising. *YourAdChoices Gives You Control*, YOURADCHOICES, https://youradchoices.com/ [https://perma.cc/NNN7-GFJR].

73. Federal Trade Commission Act, ch. 49, § 5(a), 52 Stat. 111, 111–12 (1938) (codified as amended at 15 U.S.C. § 45) (often referred to as Section 5 jurisdiction); *see* Marcia Hofmann, *Federal Trade Commission Enforcement of Privacy*, *in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE § 4:1.2 (Kristen J. Mathews ed., 2012) (discussing the FTC's authority under Section 5). The FTC also enforces several privacy statutes and the Safe Harbor Agreement between the United States and the European Union. *See A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMMISSION (Oct. 2019), http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/TR85-MPGP] ("[T]he Commission enforces a variety of other consumer protection statutes . . . prohibit[ing] specifically defined [trade] practices [and] . . . generally specify[ing] that violations . . . be treated as if they were 'unfair or deceptive' acts or practices under Section 5(a)," including

not covered by other laws began occupying a larger share of the privacy landscape, the FTC became a primary source of privacy regulation—more than nearly any privacy statute or common law tort.[74] The fact that virtually none of the FTC's rulings have been challenged in court has fortified the powerful position of the agency,[75] and some commentators now view it as the most influential regulating force in the United States.[76]

Considering the complex mosaic of privacy law, it is difficult to ascertain coherent doctrines of privacy recognition, violation, and remedies, as were easily portrayed for trade secret law.[77] One doctrine that emerges as relatively constant across the different norms concerns the "expectations of privacy" standard. Except for the particular sectoral norms, which have their own conditions, virtually all sources of privacy law determine that an actual or subjective expectation of privacy is paramount to establish a privacy

the Truth-in-Lending Act, Fair Credit Reporting Act, and Children's Online Privacy Protection Act).

74. *See* Solove & Hartzog, *supra* note 55, at 586–88 ("The statutory law regulating privacy is diffuse and discordant, and common law torts fail to regulate the majority of activities concerning privacy."); Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 811–12 (2011) (tracing the development of the FTC's role in consumer protection enforcement). *See generally* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016).

75. *See* Solove & Hartzog, *supra* note 55, at 610–13 (discussing why companies do not challenge FTC rulings in court).

76. *Id.* at 586–87 (noting that, in practice, "FTC privacy jurisprudence is the broadest and most influential regulating force on information privacy in the United States").

77. *See supra* section I.A.

claim.[78] "Expectations of privacy" is a vague standard.[79] Courts' analyses focus on whether the plaintiff can expect that the information at issue remains private, considering how the information became available to the defendant in the first place.[80] In particular,

78. The "expectations of privacy" standard has originated in the context of privacy infringements by the state. Early jurisprudence fostered a broader view, following the seminal 1890 paper by Warren and Brandeis. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195, 201 (1890) (rejecting the view that expectations of privacy are required to establish a privacy claim); *see, e.g.*, Leverton v. Curtis Publ'g Co., 192 F.2d 974, 976–78 (3d Cir. 1951); Strickler v. Nat'l Broad. Co., Inc., 167 F. Supp. 68, 71 (S.D. Cal. 1958); Banks v. King Features Syndicate, Inc., 30 F. Supp. 352 (S.D.N.Y. 1939); Reed v. Real Detective Publ'g Co., 162 P.2d 133, 138–39 (Ariz. 1945); Gill v. Curtis Publ'g Co., 239 P.2d 630, 634–35 (Cal. 1952); Roberts v. McKee, 29 Ga. 161, 164–65 (1859); Eick v. Perk Dog Food Co., 106 N.E.2d 742, 745–47 (Ill. App. Ct. 1952); Douglas v. Stokes, 149 S.W. 849, 850 (Ky. Ct. App. 1912); Denis v. Leclerc, 1 Mart. (o.s.) 297, 212–13 (La. 1811); Baker v. Libbie, 97 N.E. 109, 111 (Mass. 1912); Bennett v. Gusdorf, 53 P.2d 91 (Mont. 1935); Edison v. Edison Polyform & Mfg. Co., 67 A. 392, 394–95 (N.J. Ch. 1907); Gautier v. Pro-Football, Inc., 107 N.E.2d 485, 488 (N.Y. 1952); Binns v. Vitagraph Co. of America, 103 N.E. 1108, 1109–11 (N.Y. 1913); Holmes v. Underwood & Underwood, Inc., 233 N.Y.S. 153, 155 (N.Y. App. Div. 1929); Myers v. U.S. Camera Publ'g Corp., 167 N.Y.S.2d 771, 774 (N.Y. City Ct. 1957); Lawrence v. Ylla, 55 N.Y.S.2d 343, 346 (N.Y. Sup. Ct. 1945); Mackenzie v. Soden Mineral Springs Co., 18 N.Y.S. 240 (N.Y. Sup. Ct. 1891); Bartholomew v. Workman, 169 P.2d 1012, 1013–14 (Okla. 1946); Donahue v. Warner Bros. Pictures Distrib. Corp., 272 P.2d 177 (Utah 1954); Pollard v. Photographic Co., [1888] 40 Ch. 345 (Eng.). The turning point was the case of *United States v. Katz*, 389 U.S. 347 (1967), where the Supreme Court stated that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351–52 (citation omitted). The *Katz* decision intended to *expand* the right to privacy by shifting the question away from the location where private information was accessed. But it had the opposite effect. *See* Sandeen, *supra* note 31, at 695 ("Ironically, although the expectation of privacy doctrine was used in *Katz* to expand the defendant's zone of privacy, it is often applied to limit the types of information protected under the Fourth and Fifth Amendments."); *see also* Doe v. Mills, 536 N.W.2d 824, 831 (Mich. Ct. App. 1995) (stating that importing a Fourth Amendment ruling into all privacy cases may be a misapplication of *Katz*).

79. *See, e.g.*, Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 920–21 (2005) (noting the lack of a "coherent [and] consistent methodology for determining whether an individual has a reasonable expectation of privacy in a particular fact that has been shared with one or more persons"); *see also* Kay Connelly, Ashraf Khalil & Yong Liu, Do I Do What I Say?: Observed Versus Stated Privacy Preferences 622–23 (2007) (unpublished manuscript), https://link.springer.com/content/pdf/10.1007/978-3-540-74796-3_61.pdf [https://perma.cc/BP74-P4L3] (noting that people express different privacy expectations in their words and in their actions).

80. *E.g.*, Pearce v. Whitenack, 440 S.W.3d 392, 401 (Ky. Ct. App. 2014) ("'Nor is there liability for observing him or even taking his photograph while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye.' . . . By analogy, Pearce's Facebook posting was a walk on the Internet, the information super-highway." (citation and emphasis omitted) (quoting RESTATEMENT (SECOND) OF TORTS § 652B cmt. c)); People v. Stipo, 124 Cal. Rptr. 3d 688, 691 (Ct. App. 2011) ("A subscriber has no expectation of privacy in the subscriber information he supplies to his Internet provider. Therefore, his challenge to a warrant requiring his Internet provider to identify him through his Internet Protocol (IP) address has no merit."); *see also* Sandeen, *supra* note 31, at 696, 702 ("[C]ourts tend to focus so much on whether the information was disclosed that they ignore the context and purpose of disclosure."); Solove, *supra* note 54, at

courts inspect whether the plaintiff herself originally revealed the information.[81] While clearly not any disclosure by the plaintiff would negate a finding of "expectations of privacy,"[82] a standard that turns on initial consent to sharing weakens the plaintiff's position—especially today, where users do not always have much of a choice but to share information.[83]

As in trade secrecy, violators of privacy may or may not have a prior relationship with the subject.[84] Individuals can suffer privacy harms that result from actions by, say, their social network,[85] but they can also suffer from actions by data brokers with whom they have no prior relationship, and who collected their data without their knowledge.[86] In both cases, it is often difficult for the plaintiff to show that the violator infringed their *expectations of privacy*,

1431 ("Privacy law was developed largely to address privacy problems of disclosure and surveillance, and consequently was aimed at protecting secrets and concealed information.").

81. Sandeen, *supra* note 31, at 702.

82. *See, e.g.*, Taus v. Loftus, 151 P.3d 1185, 1218 (Cal. 2007) (finding that information can be private despite limited disclosure by the plaintiff); M.G. v. Time Warner, Inc., 107 Cal. Rptr. 2d 504, 511–12 (Ct. App. 2001) (holding that a photo is protected despite circulation within community); Times-Mirror Co. v. Superior Court, 244 Cal. Rptr. 556, 561 (Ct. App. 1988) (finding that a person's identity is private despite disclosure to friends, neighbors, family, and police); Vassiliades v. Garfinckel's, 492 A.2d 580, 587 (D.C. 1985) (holding that limited disclosure of plastic surgery to family and friends does not negate privacy finding); Multimedia WMAZ, Inc. v. Kubach, 443 S.E.2d 491, 494 n.1 (Ga. Ct. App. 1994); Y.G. v. Jewish Hosp. of St. Louis, 795 S.W.2d 488, 500–02 (Mo. Ct. App. 1990) (holding that medial information can be private despite disclosure to, inter alia, to medical personnel); *see also* Lior Jacob Strahilevitz, *Consent, Aesthetics, and the Boundaries of Sexual Privacy After* Lawrence v. Texas, 54 DEPAUL L. REV. 671, 683 (2005) ("[I]n a plurality of states, disclosing information to a network of friends, relatives, and even some strangers, does not necessarily waive a plaintiff's reasonable expectation of privacy for the purposes of tort law."). *But see infra* text accompanying note 86.

83. *See, e.g.*, JOSEPH TUROW, MICHAEL HENNESSY & NORA DRAPER, THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION 3 (2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf [https://perma.cc/N2QB-Q7TC] (explaining users' putting up with privacy-invasive practices not by a theory of willful choice, but by a theory of resignation, namely a belief that an "undesirable outcome is inevitable" and a feeling of helplessness to change it); Helman, *supra* note 27, at 537–38 (discussing the limited choice users have in the context of using social media); Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95, 164–65 (discussing the "take it or leave it" nature of online privacy deals); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1152 (2002) ("Life in the modern Information Age often involves exchanging information with third parties, such as phone companies, Internet service providers, cable companies, merchants, and so on. Thus, clinging to the notion of privacy as total secrecy would mean the practical extinction of privacy in today's world.").

84. *See supra* note 47 and accompanying text.

85. *See generally* Helman, *supra* note 27.

86. *See infra* notes 128–30 and accompanying text.

considering that in many cases today the plaintiff initially surrendered the information willingly.[87]

The "expectations of privacy" standard is the backbone of FTC rulemaking as well.[88] But the FTC takes a broader, probably more realistic approach to "expectations of privacy," which does not turn on the initial disclosure of the information.[89] Rather, the FTC considers the entire relationship between the user and the alleged privacy violator and takes an expansive view of "expectations of privacy" as a moving target that changes with time, technology, and market trends.[90]

As the above discussion demonstrates, the protection of information under trade secret law is strikingly superior to the protection provided to private information under privacy law. The next section delves into the doctrines that give rise to the differences in protection.

C. *Doctrinal Comparison*

As discussed above, trade secret law provides greater protection than does privacy law. Below, I uncover the main doctrinal differences that lead to this reality.

1. What Can Be a Secret?

In principle, neither firms' secrets nor private secrets need to be confined to specific types of information. Different firms and individuals may need protection for different types of information.

87. *See supra* note 83 and accompanying text.

88. *See* Solove & Hartzog, *supra* note 55, at 667 ("Although the FTC began enforcing broken *promises* of privacy, its focus seems to have shifted to broken *expectations* of consumer privacy.").

89. *See id.* ("[A]ctions for deception have been based on expectations created by marketing materials, user manuals, pop-up windows, emails, privacy settings, icons, and various other aspects of a website's or software program's design." (citations omitted)).

90. *Id.*; *see also* Fred H. Cate & Robert Litan, *Constitutional Issues in Information Privacy*, 9 MICH. TELECOMM. & TECH. L. REV. 35, 61 (2002) ("The public's expectations of privacy are changing, as are the many influences that shape those expectations, such as technology, law, and experience."); Adam Thierer, *A Framework for Benefit-Cost Analysis in Digital Privacy Debates*, 20 GEO. MASON L. REV. 1055, 1101–02 (2013) (describing a resistance, adaptation, assimilation cycle towards privacy-related technologies). *See generally* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET (2000) (examining the changing conceptions of privacy throughout American history).

Some firms, for example, can deem chemical formulas confidential,[91] while others may require protection of their financials.[92] Likewise, some individuals may find their health status sensitive, while others may wish to conceal their social or romantic relationships.[93] The law, however, gives effect to this reality only in the case of trade secrets. Under trade secret law, protection turns on the firm's views and behaviors regarding its information.[94] If a firm maintains the secrecy of valuable secret information, protection will attach to the information.[95]

This is not the case in privacy law. Privacy law has taken an objective, categorical view of what constitutes sensitive information. As discussed, federal and state laws have singled out certain categories of information for greater protection, such as medical or financial information, and, in some states, revenge pornography.[96] The ultra-protection zone applies to all people, with no diversity or variability for individuals' preferences. Granted, this legal reality was created bit by bit rather than by any thoughtful, comprehensive legal development; nonetheless, this is the legal landscape.[97]

Outside of the enhanced protection zones, the standard of privacy protection has turned on "expectations of privacy." As discussed below, this standard offers inferior protection to the trade

91. The formula for Coca-Cola is probably the most famous example. *See* Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co., 107 F.R.D. 288, 294 (D. Del. 1985).

92. *See supra* note 40 and accompanying text.

93. The scholarship that discussed heterogeneous privacy preferences typically focused on the fact that some individuals generally value privacy more than others, and not on the diverse types of information that individuals may require protection of. *See, e.g.*, Ryan Calo, *Code, Nudge, or Notice?*, 99 IOWA L. REV. 773, 788 (2014) ("Consumer preferences are also deeply heterogeneous. Some consumers wish for more privacy while others could not care less."); Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2026 (2013) ("American attitudes toward privacy are highly heterogeneous"); Daniel J. Gilman & James C. Cooper, *There Is a Time to Keep Silent and a Time to Speak, the Hard Part Is Knowing Which Is Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. & TECH. L. REV. 279, 318 (2010) (discussing the heterogeneity of privacy preferences in the context of health-related data); Samuelson, *supra* note 31, at 1134–35 ("Although some individuals may value privacy so highly that they will choose not to engage in market transactions about their personal data, others may be quite willing to sell their personal data to firms *A*, *B*, and *C* (even if not to *X*, *Y*, or *Z*).").

94. *See supra* notes 41–43 and accompanying text.

95. *See supra* notes 41–43 and accompanying text.

96. *See supra* notes 55, 67.

97. *See supra* section I.B.

secrecy standard of "efforts that are reasonable under the circumstances to maintain secrecy."[98]

2. "Expectations of Privacy" Versus "Efforts That Are Reasonable Under the Circumstances to Maintain Secrecy"

Trade secret protection attaches to valuable secret information if the owner of the information is taking "efforts that are reasonable under the circumstances to maintain secrecy."[99] There is no bright-line rule for what reasonable measures a secret holder must take to meet this prerequisite. Clearly, *some* measures must be taken,[100] and these measures need to show that the holder indeed viewed the information as secret in real time.[101] The reasonableness of the precautions is also circumstantial, and would be relaxed, for example, in cases of close relationships with the person who received the information.[102]

The privacy standard for protection is different. Except for the categories that are covered by targeted federal and state laws, the

98. *See* UNIF. TRADE SECRETS ACT § 1(4)(ii) (UNIF. LAW COMM'N 1985) (defining a trade secret as information that, inter alia, is the subject of "efforts that are reasonable under the circumstances to maintain its secrecy").

99. *Id.*

100. *See, e.g.*, Solid Wood Cabinet Co. v. Partners Home Supply, No. 13-3598, 2015 U.S. Dist. LEXIS 31655 (E.D. Pa. Mar. 13, 2015) (granting summary judgement to defendants after finding no evidence of protective steps); Int'l Mezzo Techs., Inc. v. Frontline Aerospace, Inc., No. 3:10-cv-00397-SCR, at *18 (M.D. La. Sept. 25, 2014) ("Although [the report at issue] was marked as proprietary and confidential, the plaintiff did not introduce evidence to demonstrate its affirmative efforts to maintain the secrecy of the information contained in the report."); SortiumUSA LLC v. Hunger, No. 3:11-cv-1656-M, 2013 U.S. Dist. LEXIS 191498, at *37 (N.D. Tex. Mar. 31, 2013) (granting a motion to dismiss based on plaintiff's failure to mark information as confidential, require the defendant to execute a confidentiality agreement, and "plead any other steps to protect the secrecy").

101. *See, e.g.*, Dryco, LLC v. ABM Indus., Inc., No. 07-CV-0069, 2009 U.S. Dist. LEXIS 97610 (N.D. Ill. Oct. 16, 2009) (finding that plaintiffs' measures did not amount to reasonable attempts to keep the information confidential); Opus Fund Servs. (USA) LLC v. Theorem Fund Servs., LLC, No. 17-C-923, 2018 U.S. Dist. LEXIS 35569, at *9 (N.D. Ill. Mar. 5, 2018) (finding no proof that the plaintiff treated the secret as "any more confidential than all of [plaintiff's] internal information"); OTR Wheel Eng'g, Inc. v. W. Worldwide Servs., Inc., No. CV-14-085-LRS, 2015 U.S. Dist. LEXIS 179509 (E.D. Wash. Nov. 30, 2015) (denying protection because there was no "Confidential" designation on the single document produced by plaintiff regarding the alleged trade secret).

102. *See* JAMES POOLEY, TRADE SECRETS § 4.04[2][b] (2020) ("If evidence of a confidential relationship and secrecy is strong, courts may relax the requirement to show reasonable precautions."); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. g (AM. LAW INST. 1995) ("When other evidence establishes secrecy and the existence of a confidential relationship, courts are properly reluctant to deny protection on the basis of alleged inadequacies in the plaintiff's security precautions.").

standard of privacy protection turns on "expectations of privacy."[103] This standard means that information will be protected only to the extent that the appropriator's actions with it were against the subject's expectations of privacy.

The "expectations of privacy" standard is not only different than the trade secrecy "reasonable precautions" standard;[104] it is strikingly narrower. First, as discussed, in court, the "expectations of privacy" standard often turns on a plaintiff's initial consent to disclosure, namely the binary question of whether the individual originally consented to the disclosure (or even made the disclosure herself).[105] The problem is not only that, as discussed above, voluntary sharing is involved in virtually all social and commercial interactions, especially online.[106] Under this line of thinking, voluntary sharing of information can be understood as consent to virtually everything in the current digital landscape. Indeed, how can internet users prove reasonable "expectations of privacy" in light of the common knowledge regarding the widespread practices of collecting, analyzing, storing, and scraping information?[107] As Sharon Sandeen puts it, "plaintiffs in privacy cases understandably assert a bright line test: if personal information has been shared with others it cannot be the subject of a privacy claim."[108] While this interpretation might be somewhat exaggerated,[109] it is true that the focus on how the information was originally made available to the violator weakens the plaintiff's position.[110]

103. *See supra* notes 77–85 and accompanying text.

104. *See* UNIF. TRADE SECRETS ACT § 1(4)(ii).

105. *See supra* note 80.

106. *See supra* note 83 and accompanying text.

107. *See* TUROW ET AL., *supra* note 83 (showing that individuals are aware of digital practices and feel helpless towards them); Alessandro Acquisti, *The Economics and Behavioral Economics of Privacy*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 76, 87 (Julia Lane et al. eds., Cambridge Univ. Press 2014) ("[A]fter an individual has released control of her personal information, she is in a position of information asymmetry with respect to the party with whom she is transacting. In particular, the subject might not know if, when, or how often the information she has provided will be used.").

108. *See* Sandeen, *supra* note 31, at 696; *see also* Shulman v. Group W Prods., Inc., 955 P.2d 469, 491 (Cal. 1998) (finding no expectation of privacy with respect to events that occurred in public view); Katherine J. Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L. REV. 1235, 1298 (2005) ("Traditionally, there is an assumption of a single 'public' and thus rather minimal disclosures destroy any 'expectation of privacy.'"); Karl D. Belgum, *Who Leads at Half-Time?: Three Conflicting Visions of Internet Privacy Policy*, 6 RICH. J.L. & TECH. 1, ¶ 21 (1999) ("Plaintiffs repeatedly lose such cases upon a showing that the fact in question was already in the public domain . . . .").

109. *See supra* note 82.

110. *See supra* note 80 and accompanying text.

Second, the "expectations of privacy" standard is not under the immediate control of the secret owner. In the trade secrecy context, employers routinely require employees and business associates to sign nondisclosure agreements ("NDAs") and return confidential information upon their departure, in order to effectuate trade secrecy protection.[111] But the law does not grant such constitutive effect to self-help precautions that individuals can take in the privacy context. Users can read privacy policies,[112] inspect when a service uses cookies to track them on other websites,[113] use anonymous or fake identities,[114] turn off location services, or use technologies that examine the data protection methods firms use.[115] These methods might be effective in the sense of interfering with data collection, but they have no legal effect: if the measures do not work (the equivalent of an NDA that was not followed), none of these (or other) methods would guarantee privacy protection nor create an obligation for the appropriator to avoid using their data.

Finally, the "expectations of privacy" standard has an adverse dynamic effect. The harder it becomes to satisfy the standard, the more users learn to expect less privacy.[116] These lower expectations

111. NDAs seem to be necessary to receive protection, but they do not always suffice. *See, e.g.*, Opus Fund Servs. (USA) LLC v. Theorem Fund Servs., LLC, No. 17-C-923, 2018 U.S. Dist. LEXIS 35569, at *8 (N.D. Ill. Mar. 5, 2018) ("While 'an agreement restricting the use of information may be considered a reasonable step to maintain secrecy of a trade secret,' such an agreement, without more, is not enough." (quoting Fire 'Em Up, Inc. v. Technocarb Equip. (2004) Ltd., 799 F. Supp. 2d 846, 851 (N.D. Ill. 2011))); Bison Advisors LLC v. Kessler, No. 14-3121(DSD/SER), 2016 U.S. Dist. LEXIS 107244, at *10 (D. Minn. Aug. 12, 2016) ("The law is clear that the mere existence of a confidentiality agreement is insufficient to establish that the covered information is a trade secret."). Companies also use NDAs because various privacy regimes require safeguarding of certain records. *See, e.g.*, Menell, *supra* note 36, at 3, 17.

112. *But see* Helman, *supra* note 27, at 532 (discussing "[t]he uninformative nature of privacy policies"); Solove & Hartzog, *supra* note 55, at 667 (citing surveys showing that users do not read privacy policies).

113. *See, e.g.*, COOKIE CHECKER, http://www.cookie-checker.com/ [https://perma.cc/KH6U-N8JR].

114. But note that social networks' Terms of Service typically forbid anonymous use. *See, e.g.*, *Terms of Use*, FACEBOOK, https://www.facebook.com/terms.php [https://perma.cc/K9V7-K723] (requiring users to "[u]se the same name that [they] use in everyday life" and "[p]rovide accurate information about [themselves]"); *User Agreement*, LINKEDIN, https://www.linkedin.com/legal/user-agreement#obligations [https://perma.cc/6ST2-JBY6] ("[Y]ou will . . . [p]rovide accurate information . . . [and] [u]se your real name on your profile"). Even when users can have anonymous profiles, such as on Tumblr, the firm itself can and does track users' activity. *See, e.g.*, *Privacy Policy*, TUMBLR, https://www.tumblr.com/privacy/en [https://perma.cc/QQH5-UBUU].

115. *See, e.g.*, *Security Data*, SECURITY SCORECARD, https://securityscorecard.com/product/security-data [https://perma.cc/PE8Y-PQ6G].

116. *See also* Helman, *supra* note 27, at 560 ("[T]he more users would learn to expect

feed back to the legal standard of "expectations of privacy" and have the effect of further eroding these expectations.[117]

3. Third-Party Liability

Trade secrets and privacy protection can both last forever, but they are terminated upon publication of the underlying information. Indeed, protection of trade secrets expires once the secrets become known or if the owner stops protecting them.[118] Similarly, private information loses protection once the subject loses privacy expectations, which typically follows publication of the information.[119] Granted, the original misappropriator may well bear liability for a breach, and in a trade secret case will typically be enjoined from future usage.[120] But monetary damages would often be inadequate or unavailable to stem the loss of the secret being lost for most practical purposes.[121] This is particularly troubling in the privacy context, where courts require proof of harm that is unrealistic for most victims, which means that damages from the original misappropriator would often not be available at all.[122]

Trade secrecy is mindful of this effect and includes a notable limitation. Under trade secret law, liability *does* extend to third parties who use or disclose information that they "knew or had reason to know" was obtained through improper means or in violation of a confidentiality duty.[123] This is a crucial rule. Holders of misappropriated secrets typically wish to use them via a third party—either a competitor of the secret owner or a new entity of their own. Yet, any third party who attempts to hire a holder of a competitor's secret in hopes of putting its hands on the secret is likely to be enjoined.[124]

---

better privacy terms from online companies the more privacy they would be entitled to.").

117. *Id.*

118. *See* Menell, *supra* note 36, at 47 ("Unfortunately, once a secret is divulged to the public, it is not possible to obtain an injunction against those who have learned of the trade secret legitimately. . . .").

119. *See supra* notes 78–81 and accompanying text.

120. *See supra* note 50 and accompanying text.

121. *See* Elizabeth A. Rowe, *Trade Secret Litigation and Free Speech: Is It Time to Restrain the Plaintiffs?*, 50 B.C. L. REV. 1425, 1451–52 (2009); Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet Through Sequential Preservation*, 42 WAKE FOREST L. REV. 1, 45–46 (2007).

122. *See infra* note 134 and accompanying text.

123. *See* UNIF. TRADE SECRETS ACT § 1(2) (UNIF. LAW COMM'N 1985).

124. *Id.*

The prohibition on knowingly using a misappropriated secret is in fact quite broad. In the extant jurisprudence, any derivative use of the trade secret is impermissible—no matter how remote and dissimilar the downstream use is to the original function of the secret.[125] As Joseph Fishman and Deepa Varadarajan explain,

> The case law seldom investigates whether the copied information was a significant part of the plaintiff's entitlement or whether the defendant's use poses any threat of market harm. Instead, the test quickly collapses into a binary question of whether exposure to the secret educated the defendant at all, regardless of what the defendant's final product or process ends up looking like.[126]

Banning any downstream use of a misappropriated secret is a broad—perhaps too broad—feature of trade secrecy.[127] And it stands in sharp contrast to privacy law. Privacy law includes no prohibition on the use of data that was obtained illegally, let alone data that was obtained through violation of the data subject's expectations of privacy. Information in the data-trafficking industry is often hacked and resold, and laundered so many times that its sources become indistinguishable at some point.[128] Data brokers routinely purchase data from entities that acquire the information from blatantly illegal sources.[129] And to alleviate a concern of any claim of willful blindness or plausible deniability, data brokers rarely "affirmatively evaluate the legitimacy, stability, and quality of their sources before accepting data from them."[130] The collection,

125. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (AM. LAW INST. 1995) ("Even if the defendant's final product or process differs significantly from that of the plaintiff, substantial use of the trade secret in the course of the defendant's research can be sufficient to constitute an appropriation.").

126. *See* Fishman & Varadarajan, *supra* note 35, at 1054 (criticizing this caselaw).

127. *See id.* Note that this broad provision applies not only with regard to third parties but with regard to any downstream use of a trade secret. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (AM. LAW INST. 1995).

128. *See* Scholz, *supra* note 26, at 666 ("By the time the most legitimate data traffickers, such as the ones interviewed by the FTC, choose to purchase access to the data, the sources of the data have become unclear.").

129. *Id.* at 665–66 (arguing also that the ability to sell hacked data provides an incentive for hackers to steal data—because they can launder it through data trafficking companies). Illegal methods include, for example, hacking into private databases in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, or exceeding the limitation of use of the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721–2725, or that of state laws restricting the use of voter registration information. *Id.* at 665–66 n.61; *see Voter List Information*, U.S. ELECTIONS PROJECT, http://voterlist.electproject.org [https://perma.cc/V8SL-NB5X] (last updated Aug. 22, 2015); *see also* David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907, 926–42 (2013) (showing that these actions can be illegal).

130. *See* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND

use, or disclosure of this information by data brokers is not inhibited a bit by the fact that this data was originally obtained while infringing on privacy rights.

4. Remedies

As discussed previously, a successful trade secret case is likely to yield permanent injunctions, alongside compensation—actual damages or unjust enrichment, and in suitable cases, exemplary damages and attorneys' fees.[131] Misappropriation of trade secrets is also a criminal offense.[132]

In contrast, privacy law features incoherent remedies. Beyond specific federal or state laws, injunctions are fairly rare, although some courts are sometimes open to this remedy.[133] Damages are also difficult to obtain. Under both tort and contract theories of liability, courts require plaintiffs to show concrete harm.[134] Ryan

ACCOUNTABILITY, at iv, 16 (2014) [hereinafter DATA BROKERS], https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/G9CE-E8X6].

131. *See* UNIF. TRADE SECRETS ACT §§ 2–4 (UNIF. LAW COMM'N 1985).

132. *See* Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376; *see also* United States v. O'Rourke, 417 F. Supp. 3d 996 (N.D. Ill. 2019) (enforcing criminally attempted misappropriation despite lack of secrets); Orly Lobel, *The DTSA and the New Secrecy Ecology*, 1 BUS. ENTREPRENEURSHIP & TAX L. REV. 369, 372–73 (2017) (noting a serious increase of criminal enforcement measures pertaining to trade secrecy under the Economic Espionage Act).

133. *See, e.g.*, Doe 1 v. AOL, LLC, 719 F. Supp. 2d 1102 (N.D. Cal. 2010) (holding that plaintiffs were eligible for compensatory damages, restitution, injunctive relief, or punitive damages for privacy violations).

134. *See, e.g.*, Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (stating that a plaintiff must show a concrete, discernible injury rather than a "conjectural or hypothetical" one for standing in federal court (quoting Los Angeles v. Lyons, 461 U.S. 95, 102 (1983))); *In re* LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013) (finding no "resulting damages of [the] alleged breach" of contract); Rudgayzer v. Yahoo! Inc., No. 5:12-CV-01399 EJD, 2012 U.S. Dist. LEXIS 161302, at *18–19 (N.D. Cal. Nov. 9, 2012) (finding no actual harm to support a privacy claim of breach of contract); Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1028 (N.D. Cal. 2012) (rejecting embarrassment and property-based theories of harm as insufficient in contract-based privacy claim); *In re* Facebook Privacy Litig., No. C 10-02389 JW, 2011 U.S. Dist. LEXIS 147345, at *15 (N.D. Cal. Nov. 22, 2011) (rejecting plaintiffs' claim that they suffered "appreciable and actual damage" in contract-based suit); Smith v. Trusted Universal Standards in Elec. Transactions, Inc., No. 09-4567 (RBK/KMW), 2010 U.S. Dist. LEXIS 43360, at *30–31 (D.N.J. May 4, 2010) (dismissing contract-based claim because plaintiff failed to show loss flowing from the alleged breach); Cherny v. Emigrant Bank, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) (holding that the release of an email address does not constitute sufficient injury); *see also* Lawrence Friedman, *Establishing Information Privacy Violations: The New York Experience*, 31 HOFSTRA L. REV. 651, 653–55, 659–61 (2003) (discussing two New York cases in which the court required plaintiffs to show actual harm to property or monetary loss).

Calo has observed that courts have tended to use a particularly strict harm standard for privacy cases.[135] The heightened standard may stem from the concern that privacy injuries are inherently subjective, and relaxing the harm standard may yield unpredictable, excessive damages.[136] Yet showing concrete privacy harms is nearly impossible.[137] Many privacy cases fail because of this prerequisite.[138]

Courts have recently begun exploring the territory of restitution in privacy cases.[139] Restitution, in brief, is liability for benefits received. Restitution lies when a person receives a benefit from another, in circumstances where, as between the two persons, it is unjust for them to retain it.[140] The theory suggests that using and profiting from a person's information without that person's consent

135. *See* Ryan Calo, *Privacy Harm Exceptionalism*, 12 J. ON TELECOMM. & HIGH TECH. L. 361, 361 (2014) ("[C]ourts and some scholars require a showing of harm in privacy out of proportion with other areas of law."). For scholarship that proposed more achievable ways to measure privacy harms, see, e.g., Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907 (2013); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007).

136. *See* Scholz, *supra* note 26, at 656 ("Courts worry that recognizing the privacy right in the absence of a clearly defined concrete harm may lead to unpredictable, excessive damages based on plaintiffs' subjective perceptions.").

137. *Id.* at 655 (discussing the "'harm problem' . . . the difficulty in defining a measurable economic harm issuing from privacy infringements"). *See generally* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018).

138. *See, e.g.*, cases cited *supra* note 134.

139. *See, e.g.*, WIS. STAT. § 995.50 ("The right of privacy is recognized in this state. One whose privacy is unreasonably invaded is entitled to the following relief: . . . [c]ompensatory damages based either on plaintiff's loss or defendant's unjust enrichment; and [a] reasonable amount for attorney fees."); Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012) (recognizing a claim for unjust enrichment); Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735 (W.D.N.Y. 2017) (discussing plaintiffs' restitution claim); Enslin v. Coca-Cola Co., 136 F. Supp. 3d 654 (E.D. Pa. 2015) (discussing plaintiffs' restitution claim); Fraley v. Facebook, Inc., 830 F. Supp. 2d 785 (N.D. Cal. 2011) (denying motion to dismiss on unjust enrichment claims); State v. Moua, 874 N.W.2d 812 (Minn. Ct. App. 2016) (finding victims of identity theft entitled to restitution). Some states explicitly confer restitution upon privacy cases. *See* Scholz, *supra* note 26, at 659 (endorsing restitution as a remedy and as a cause of action).

140. *See* RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 1 (AM. LAW INST. 2011) ("A person who is unjustly enriched at the expense of another is subject to liability in restitution."); Scholz, *supra* note 26, at 680 ("Harm or unjust enrichment arises from data processing or data dissemination when: (1) there is a relationship of trust between the two parties that makes it reasonable for the plaintiff to expect her data would not be handled in that way; and/or (2) society deems it morally wrong or outrageous for data to be processed or disseminated in such a way; and/or (3) the information is being processed or disseminated by the defendant in a way that [either] subjected [the] plaintiff to harm [or risk of harm or unjustly enriched the defendant].").

is unjust. Restitution as a cause of action couples with restitution as a form of relief (and the latter can be available without the former).[141] While not free of problems of its own,[142] in suitable cases, this path obviates the requirement of harm, which often precludes relief from privacy victims.[143] Despite this new path for recovery, for now, lawsuits against privacy intrusions are often unsuccessful.[144]

To a large extent, together with privacy regulation more generally, privacy enforcement has become the domain of the FTC. But as an administrative enforcement agency—and as will be expanded upon below—the FTC is confined to enforcement measures that are not easily translated to relief for the injured parties.

5. Institutions

The inferiority of privacy law in terms of remedies, as discussed above,[145] is also a product of the different institutions that trade secret owners and privacy victims have de facto access to. As discussed, courts form an effective venue for trade secret holders to combat the misappropriation of their rights. In court, plaintiffs can request compensation, restitution, and injunctive relief.[146] By contrast, courts are playing an increasingly marginal role in privacy lawmaking, leaving the arena for administrative rulemaking by the FTC.[147] As Daniel Solove and Woodrow Hartzog put it, if there is any common law on privacy today, it is within the FTC.[148]

141. *See generally* Scholz, *supra* note 26. The FTC is also authorized to apply restitutionary remedies. *See* 15 U.S.C. § 45.

142. *See, e.g.*, Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. REV. 1327, 1328 (2012) (stating that individuals have difficulty in determining the value of the data they are trading).

143. *See supra* notes 134–38 and accompanying text; *see also* Sandeen, *supra* note 31, at 706 (noting that nothing requires us to limit available causes of action to ones that are designed to compensate for economic loss); Colleen P. Murphy, *Misclassifying Monetary Restitution*, 55 SMU L. REV. 1577, 1591 (2002) (noting that there are two principle types of monetary remedies available: (1) damages, where relief is measured by loss to plaintiff; and (2) restitution, where relief is measured by gain of defendant.).

144. *See* Anita Bernstein, *Real Remedies for Virtual Injuries*, 90 N.C. L. REV. 1457, 1475 (2012); *see also* Scholz, *supra* note 26, at 653.

145. *See supra* section I.B.

146. *See supra* section I.A.

147. *See supra* section I.B; *see also* Bernstein, *supra* note 144, at 1475 (noting that privacy cases typically fail in court).

148. *See* Solove & Hartzog, *supra* note 55, at 619 (discussing "[t]he Privacy 'Common Law' of the FTC").

Absent broad jurisdiction and general authority to issue civil penalties,[149] the FTC is restricted to investigating companies for alleged privacy violations and reaching settlements with them through consent orders.[150] The FTC's authority to design consent orders is broad.[151] Consent orders can include, for example, financial sanctions, prohibitions on future activities, and reporting, audit, and compliance requirements for up to twenty years.[152]

While these enforcement measures may sound extensive, they barely pose a real threat to companies. To begin with, the nature of a consent order is that it involves the privacy violator in designing the settlement.[153] Second, the sanctions themselves are not particularly severe. Financial sanctions (including penalties and monetary corrective measures such as disgorgement of revenues) are relatively modest, partially because they must reflect, inter alia, consumer loss—a major obstacle in the privacy context.[154] The ban on future activities is essentially a ban on activities that are forbidden anyway. For example, companies accused of misrepresenting information to users were prohibited from making future misrepresentations.[155] Indeed, as part of settlements, companies often agree to delete or refrain from using information that was gained through the investigated privacy violations;[156] but again, this information was barred from use in the first place. FTC cases may also bring bad press,[157] but their actual reputational damage

149. *See id.* at 605 (noting that "the FTC lacks the general authority to issue civil penalties"); Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L.J. 1183, 1205 (2003) ("The FTC[] . . . does not have jurisdiction over many private sector, non-profit, and governmental record keepers.").

150. The FTC can fine companies for violating consent orders, but such violations are rare. *See* Solove & Hartzog, *supra* note 55, at 605.

151. *Id.* at 613 (noting that the FTC has unrestrained power to design consent orders).

152. *See id.* at 613–14.

153. *See supra* note 150 and accompanying text.

154. *See, e.g.*, United States v. Danube Carpet Mills, Inc., 737 F.2d 988, 993 (11th Cir. 1984) (indicating "injury to the public" as a factor in determining penalty amount); *see also supra* notes 135–38 and accompanying text.

155. Solove & Hartzog, *supra* note 55, at 155–56; *see also* Stipulated Final Order for Permanent Injunction at 5, FTC v. Frostwire LLC, No. 1:11-cv-23643-DLG (S.D. Fla. Oct. 12, 2011) (restraining defendants from misrepresenting that consumers' computers are not publicly sharing downloaded files).

156. *See* Solove & Hartzog, *supra* note 55, at 616.

157. *See id.* at 606 ("Beyond fines, cases bring bad press.").

is dubious, especially considering the rampant privacy intrusions that the public has learned to expect.[158]

In fairness, the FTC has been able to compel companies to agree to measures that can improve future privacy practices. For example, companies have agreed to "comprehensive privacy program[s],"[159] and to subject such programs to third-party supervision.[160] Yet overall, what looks like solid FTC enforcement may only appear so in comparison to the ineffectiveness of other privacy regulators.[161] In reality, the agency's enforcement mechanisms depend on companies' voluntary cooperation. This cooperation may be stemming from fear of a long and tedious auditing process or of a scenario where the agency would push for privacy legislation that would jeopardize the self-regulation regime.[162]

Beyond remedies, the fact that privacy becomes the domain of the FTC has other disadvantages for privacy protection. Administrative agencies are prone to capture and public choice problems, which may partially explain their soft hand towards companies that they regulate.[163] Some commentators have also criticized the FTC for acting arbitrarily and providing little guidance to companies, although this may be changing slightly.[164]

158. *See* Jake Nevrla, *Voluntary Surveillance: Privacy, Identity and the Rise of Social Panopticism in the Twenty-First Century*, 6 COMM-ENTARY 5, 5–6 (2010) ("Societal norms have inevitably adapted to this new medium of communication and the level of surveillance that has come with it."); TUROW ET AL., *supra* note 83, at 3–4.

159. *E.g.*, Decision and Order at 4, *In re* Google, Inc., FTC File No. 102-3136, Docket No. C-4336 (Oct. 13, 2011) (consent order).

160. *See id.* at 5; *see also* Agreement Containing Consent Order at 6, *In re* Facebook, Inc., FTC File No. 092-3184, Docket No. C-4365 (Nov. 29, 2011).

161. *See supra* section I.A.

162. Ryan Moshell, . . . *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 383 (2005) (discussing "FTC's inadequacy and toothlessness in ensuring privacy protection").

163. *See* Richard Pierce, *Institutional Aspects of Tort Reform*, 73 CALIF. L. REV. 917, 935 n.104 (1985) ("'Capture' refers to the tendency of some agencies to favor the industry they are required to regulate by protecting the industry from outside competition and stifling innovation that threatens the status quo in the industry." (citing Roger G. Noll, *The Behavior of Regulatory Agencies*, 29 REV. SOC. ECON. 15 (1971))); Thomas W. Merrill, *Capture Theory and the Courts: 1967–1983*, 72 CHI.-KENT L. REV. 1039, 1050 (1997) ("[A]gencies were likely to become 'captured' by the business organizations that they are charged with regulating.").

164. *See* Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 689–94 (2013) ("[The] inherent ambiguity [of unfairness authority] can be dangerous for regulated entities . . . ."); Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 165–71

Finally, the dominant rulemaking by the FTC compared to courts has a self-perpetuating effect. This reality adversely influences the incentives of privacy victims to bring lawsuits. In turn, the scarcity of lawsuits prevents development of tort and contract doctrines to the extant privacy challenges and self-perpetuates the reliance on the FTC.

* * *

In sum, even though both trade secrecy and privacy law are designed to protect information that the owner or subject of which deems secret, the inferiority of privacy protection is unmistakable. Individuals do not have the privilege that firms have, to decide for themselves which pieces of information about them deserve enhanced protection. None of the safeguards that firms can take to trigger protection of their secrecy are of any avail to individuals, because the law would not give effect to such measures. While trade secrecy includes protection of downstream conscious use of misappropriated secrets, privacy protection does not extend against third parties. Privacy remedies also pale in comparison to the remedies available to trade secret owners, reflecting the general disarray of privacy law. Finally, the stagnation in courts on privacy cases has created a critical institutional effect. Below, I consider whether this divergence is justified and whether some harmonization of the two regimes can provide a better way forward.

II. CONSIDERING HARMONIZATION

A. *The Case for (Some) Harmonization of Trade Secrecy and Privacy Law*

Why is it that trade secrecy is so much better protected than privacy law? One explanation has to do with legal history. Sharon Sandeen has studied the development of both trade secret law and privacy law, from common law to tort law to the extant state.[165]

(2008) ("No guidelines exist under which the Commission will act or refrain from acting if a data security breach occurs."). *But see* Solove & Hartzog, *supra* note 55, at 606–27, 648–66 (refuting these arguments).

165. *See* Sandeen, *supra* note 31.

She concluded that while many parallels exist between the development of these laws, at some point in time, trade secrecy jurisprudence grew while privacy common law ceased to evolve.[166]

Another (or complementary) explanation for the protection gap between the regimes may concern their normative approval: privacy law does not enjoy the wall-to-wall normative support that trade secret law enjoys. Trade secrets' justification is supposedly evident.[167] Neither scholars nor courts seriously dispute that companies have legitimate reasons for limiting the disclosure of their proprietary information.[168] In contrast, privacy skeptics abound,[169] and even among supporters, the underpinnings of privacy law are subject to fierce debates.[170] The undisputed normative basis of trade secrecy translates to an eloquent trade secret law, while the dubious privacy grounds are echoed in the heightened standards for privacy liability and in the reluctance to extend existing doctrines to contemporary privacy harms.[171]

Not only are privacy rights contested, but it is not even clear what kind of interests they form, unlike trade secret law. In theory, under the classic framework for the distinction between liability

166. *Id.* at 687, 692 (arguing that "unlike trade secret law, information privacy law has not fully developed", partially because "[i]nformation privacy concerns are more personal and are unlikely to garner the attention of attorneys until there is a gross invasion of privacy").

167. *See infra* notes 178–91 and accompanying text.

168. *See, e.g.*, Menell, *supra* note 36, at 8 (conceding that firms have a legitimate interest in maintaining secrecy even with regards to "the disclosure of proprietary information that allegedly reveals illegal activity"). *But cf.* Lobel, *supra* note 132 (arguing that the interest of secrecy needs to be balanced against the interest of openness in order to promote innovation); Robert G. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803, 1807–08 (2014) (expressing skepticism that "trade secret law generates incentive benefits that exceed its costs").

169. *See, e.g.*, Ann Bartow, *A Feeling of Unease About Privacy Law*, 155 U. PA. L. REV. PENNUMBRA 52, 52 (2006); Richard Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978); Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 414–17 (2013); *see also* Chi Ling Chan, *Privacy Is (Not) Dead*, STAN. DAILY (Oct. 7, 2014), https://www.stanforddaily.com/2014/10/07/privacy-is-not-dead/ [https://perma.cc/T4LW-YNWL]; Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy [https://perma.cc/4TXZ-X4FQ].

170. *See, e.g.*, LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 142–63 (1999) (advocating the use of property rights to enhance privacy protection); Friedman, *supra* note 134, at 652; Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1259–65 (1998); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 26–41 (1996); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2385 (1996); *see also supra* note 169 and accompanying text.

171. *See supra* section I.B.

and property as described by Guido Calabresi and A. Douglas Melamed, both trade secrets and privacy interests could be viewed as dualistic.[172] Both have some property features, but the right to exclude from access or use of the information that they entail is circumstantial and is not freestanding against the world.[173] Yet, the legal reality is that trade secrecy is comfortably branded as intellectual property,[174] while privacy remains wandering.[175] This misfit of privacy law has adverse implications. As Lauren Henry Scholz explains,

> Classifying and describing the type of interest—be it a personal interest, a property interest, or some other type of interest—allows courts to decide cases through comparison to other cases implicating the

172. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).

173. *See, e.g.*, E.I. DuPont de Nemours Powder Co. v. Masland, 244 U.S. 100, 102 (1917) ("The word property as applied to . . . trade secrets is an unanalyzed expression of certain secondary consequences of the primary fact that the law makes some rudimentary requirements of good faith. Whether the plaintiffs have any valuable secret or not the defendant knows the facts, whatever they are, through a special confidence that he accepted. The property may be denied but the confidence cannot be. Therefore the starting point for the present matter is not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs . . . ."); Peabody v. Norfolk, 98 Mass. 452, 458 (1868) (recognizing a property right in a trade secret, but also recognizing that "he has not indeed an exclusive right to it as against the public, or against those who in good faith acquire knowledge of it; but he has a property in it, which a court of chancery will protect against one who in violation of contract and breach of confidence undertakes to apply it to his own use, or to disclose it to third persons"); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1284–85 (2000) (outlining skeptical perspectives on privacy as property); Samuelson, *supra* note 31, at 1129; Lauren Henry Scholz, *Privacy as Quasi-Property*, 101 IOWA L. REV. 1113, 1116, 1131 (2016) (categorizing both privacy and trade secrecy as quasi-property).

174. *See* 1 ROGER M. MILGRIM & ERIC E. BENSON, MILGRIM ON TRADE SECRETS § 2.01 (2020) (listing cases describing trade secrets as property and intellectual property); *see, e.g.*, Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) ("Trade secrets have many of the characteristics of more tangible forms of property. A trade secret is assignable. A trade secret can form the res of a trust, and it passes to a trustee in bankruptcy." (citations omitted)); Tabor v. Hoffman, 23 N.E. 12, 12 (N.Y. 1889) (holding that "an inventor or author, has, by the common law, an exclusive property in his invention or composition"); *Peabody*, 98 Mass. at 458 (recognizing a property right in a trade secret, but also recognizing that "he has not indeed an exclusive right to it as against the public, or against those who in good faith acquire knowledge of it; but he has a property in it, which a court of chancery will protect against one who in violation of contract and breach of confidence undertakes to apply it to his own use, or to disclose it to third persons").

175. *See* Samuelson, *supra* note 31, at 1170–71 ("[A] serious impediment to a comprehensive approach [to privacy] in the U.S. is the lack of clarity in this country about the nature of the interest that individuals have in information about themselves: Is it a commodity interest, a consumer protection interest, a personal dignity interest, a civil right interest, all of the above, or no interest at all?").

> same type of interest. . . . Since privacy has not been consistently approached as either property or a personal interest, courts have hesitated to compare privacy cases to anything but other privacy cases.[176]

The result is a vibrant trade secrecy jurisprudence and a privacy law that gets a cold shoulder from courts.[177]

Historical or normative roots for the divergence of the laws obviously do not justify maintaining such deviation. The discussion below aims to demonstrate that such a deviation is not justified today, if indeed it has ever been. The first subsection below will analyze the core justifications of trade secrecy and argue that they are valid in the privacy context as well, even though they do not capture the theoretical and normative depth of privacy protection. In the second subsection, I discuss how collisions of trade secrecy and privacy law are increasingly common, and why maintaining the doctrinal gap between the regimes has an amplifying effect on the inferiority of privacy interests.

1. The Shared Objectives of Trade Secrecy and Privacy

a. Innovation Policy

First and foremost, trade secrecy is justified as innovation policy—it encourages companies to engage in innovation that requires sharing of information internally or with business partners.[178] In-

176. *See* Scholz, *supra* note 173, at 1114.

177. *Id.* at 1115–16 ("In an era where the development of technology inevitably outpaces the development of preexisting law, common law plays a significant role."); *see also* Bruce P. Keller, *Condemned to Repeat the Past: The Reemergence of Misappropriation and Other Common Law Theories of Protection for Intellectual Property*, 11 HARV. J.L. & TECH. 401, 428 (1998) ("It stands to reason that the faster a technology develops, the more rapidly it will surpass preexisting law, and the more prominent common law theories may become. It is not surprising, therefore, that as the Internet geometrically expands its speed, accessibility, and versatility—thereby vastly increasing the opportunities for economic free-riders to take, copy, and repackage information and information systems for profit—intellectual property owners again must consider the common law as a source of protection at the end of this century, much as it was at the beginning.").

178. *See* Menell, *supra* note 36, at 36 ("[T]rade secret protection augments other intellectual property protections in promoting innovation. It encourages companies to invest in their workforce and facilitates a productive environment for technological progress."); David D. Friedman, William M. Landes & Richard A. Posner, *Some Economics of Trade Secret Law*, 5 J. ECON. PERSP. 61, 64 (1991) (contending that trade secrecy "supplements the patent system" and that it "provides a means of internalizing the benefits of innovation"); Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 329 (2008) (arguing that trade secrets share "two critical features . . . with other IP

deed, trade secret law, like other intellectual property law, is designed to confront the concern that in a free market, too little information sharing would occur.[179] As Arrow's disclosure paradox famously shows, without legal protection information would not be shared, because "in order to sell the information, [the seller] must disclose it to the potential buyer, but once she does, she has nothing left to sell."[180] Trade secrecy is thus designed to facilitate safe sharing of information. Clearly, uncareful sharing is also not desired. To drive efficient results for innovation, companies need to be mindful about sharing. Trade secret law achieves this balance by requiring companies to safeguard their information sharing, a standard that encourages careful and conscious sharing of information.

What current law is missing, though, is that information privacy law shares the same mission. It is mistakenly assumed that to encourage innovation in data-intensive sectors, a lax privacy standard is preferred.[181] Arguably, the fewer limitations imposed on collecting, analyzing, and using people's private information, the fewer constraints on developing and experimenting with big-data usage and business models.[182] The main flaw in this theory is ignoring the supply chain: users' provision of data. Indeed, the law does not value private disclosure nearly as much as commercial disclosure. In fact, privacy law treats disclosure like a fault. As discussed above, the "expectations of privacy" standard practically denies protection of much of the information that was originally

rights—they promote inventive activity and they promote disclosure of those inventions"). The Supreme Court has echoed that justification. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 485 (1974) ("Trade secret law will encourage invention in areas where patent law does not reach, and will prompt the independent innovator to proceed with the discovery and exploitation of his invention."); *id.* at 486 (observing that, absent trade secret protection, "[t]he holder of a trade secret would . . . hoard rather than disseminate knowledge" and "[i]nstead, then, of licensing others to use his invention and making the most efficient use of existing manufacturing and marketing structures within the industry, the trade secret holder would . . . limit his utilization of the invention, thereby depriving the public of the maximum benefit of its use"); *see also*, *e.g.*, Am. Can Co. v. Mansukhani, 742 F.2d 314, 329 (7th Cir. 1984) ("The primary purpose of trade secret law is to encourage innovation and development . . . .").

179. *See supra* note 178.

180. *See* Oren Bar-Gill & Gideon Parchomovsky, *Law and the Boundaries of Technology-Intensive Firms*, 157 U. PA. L. REV. 1649, 1654 (2009).

181. *See, e.g.*, Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L. 74 (2013) (explaining the tension between the virtues of big data industries on the one hand and consumer privacy on the other).

182. *Id.* at 76–77 (giving examples of how firms use consumer data).

shared voluntarily.[183] The more a person is responsible for the original disclosure of her private information, the less protection the information will be awarded.[184] The fact that privacy law frowns upon any disclosure in a social and business world that encourages disclosure leads to severe exposure to privacy risks.

This cannot be a sound policy in today's economy, which is fueled by personal data.[185] Unlike trade secret holders, who are motivated to share information and use safeguards, individuals are incentivized to do neither. On the one hand, sharing information voluntarily invites unforeseeable privacy risks. On the other hand, mindfully using safeguards while sharing information has no effect. It does not pay to read privacy policies, to show preferences to services with more transparency, or to invest in other safeguards.[186] For the data industry to develop in a welfare-maximizing manner,

183. *See supra* notes 78–83 and accompanying text.

184. *See supra* notes 78–83 and accompanying text.

185. *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1918–27 (2013) (arguing that lack of privacy may harm innovation); Goldfarb & Tucker, *supra* note 69, at 85 (drawing on empirical analysis to argue that "ultimately privacy policy is interlinked with innovation policy and consequently has potential consequences for innovation and economic growth," and summarizing evidence that "privacy regulations directly affect the usage and efficacy of emerging technologies"); Ohm, *supra* note 135, at 927 ("Many companies are actively reshaping their business models to try to profit from customer secrets."); DATA BROKERS, *supra* note 130, at 13; FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 8 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/S58Q-MY54] ("[Privacy protections] not only will help consumers but also will benefit businesses by building consumer trust in the marketplace."); *H.R. 5777, the "BEST PRACTICES Act," and H.R. __, a Discussion Draft to Require Notice to and Consent of an Individual Prior to the Collection and Disclosure of Certain Personal Information Relating to That Individual: Hearing Before the H. Subcomm. on Commerce Trade & Consumer Prot.*, 111th Cong. 125 (2010) (statement of Leslie Harris, President and Chief Executive Officer, Center for Democracy & Technology) ("Privacy is an essential building block of trust in the digital age."); John Rose, Christine Barton, Rob Souza & James Platt, *The Trust Advantage: How to Win with Big Data*, BOS. CONSULTING GROUP (Nov. 6, 2013), https://www.bcg.com/publications/2013/marketing-sales-trust-advantage-win-with-big-data [https://perma.cc/4BYU-WLLX] ("In order for global companies to have the greatest possible access to personal data, consumers need to trust that this information will be well stewarded."); Press Release, Carnegie Mellon Univ., Increasing Control over Release of Information Leads People to Divulge More Online, Carnegie Mellon Researchers Find (Nov. 28, 2012), https://www.cmu.edu/news/stories/archives/2012/november/nov28_informationcontrol.html [https://perma.cc/FEP3-FFS8]; *Data Privacy Is a Major Concern for Consumers*, TRUSTARC BLOG (Jan. 28. 2015), http://www.truste.com/blog/2015/01/28/data-privacy-concern-consumers/ [https://perma.cc/Y588-U7FJ] (citing surveys that show "[c]onsumers consider data privacy to be a hot button issue").

186. *See also supra* note 112.

the same logic that leads to trade secrecy law needs to apply here as well: privacy law needs to facilitate safe sharing of information.

b. Self-Help Measures

Trade secret law is also concerned that without protection, companies will invest in wasteful self-help measures for information protection and surveillance of employees and business partners. Indeed, trade secrecy provides an effective ex-post tool to remediate situations of disloyal partners, and thus obviates the need to rely on expensive ex-ante inspections of business associates.

Notably, the concern of inefficient self-help measures that may be taken to protect sensitive information is valid in the privacy context as well. Because self-help measures are not recognized under the law, users do not have an incentive to use measures that are desired from a societal standpoint. People increasingly react to the lack of ineffective privacy protection by employing a range of privacy-seeking strategies, from adoption of technical protections to using fake profiles to self-censorship and withdrawal of content.[187] The law creates no incentive to use privacy strategies that are desired from a societal point of view, and so more and more people use identity-obscuring techniques, turn on Virtual Private Networks ("VPNs") to mask their IP addresses, and engage in other methods that may be effective to safeguard their information from data-collectors, but may also be destructive from a societal standpoint.[188] Such methods not only constitute pure waste from a societal point of view, but they may have negative externalities,

187. *See, e.g.*, Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 576 (2017) ("Individuals and businesses are rapidly adopting technical protections."); Danah Boyd & Eszter Hargittai, *Facebook Privacy Settings: Who Cares?*, 15 FIRST MONDAY, no. 8, 2010, at 1 (finding an increase in youth's practices to modify privacy settings on Facebook between 2009–2010); Kevin Lewis, Jason Kaufman & Nicholas Christakis, *The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network*, 14 J. COMPUTER-MEDIATED COMM. 79 (2008).

188. *See* Helman, *supra* note 27, at 544–45 (demonstrating "privacy-seeking behaviors such as adopting of technical protections, arranging privacy settings within social media sites, using fake profiles, and practicing 'self-censorship and withdrawal of content'"); Samantha Murphy, *Facebook's Facial-Recognition Acquisition Raises Privacy Concern*s (June 25, 2012), http://mashable.com/2012/06/25/facebook-facial-recognition-privac/ [https://perma.cc/NPW3-QV59] ("[S]ome users might exercise more caution with how they upload pictures.").

such as interfering with law enforcement activities, slowing internet use, or generating other risks.[189]

c. Business Ethics

Even trade secrecy's business ethics rationale applies to the privacy realm in today's economy.[190] The same concern that companies have—that a misappropriator will acquire an advantage over them based on information that they develop and own—is now shared by individuals. Indeed, privacy violators can use information about individuals in order to enhance their bargaining power when dealing with them, such as by price discriminating against them or exploiting their vulnerabilities.[191]

Indeed, while the underpinning of privacy law remains an ongoing exploration, the main justifications of trade secret law may give grounds to adoption of some trade secrecy doctrines in the information privacy context.

2. Collisions of Trade Secrecy and Privacy Law

The importance of harmonization intensifies in view of the growing zone of collision between trade secrecy and privacy regimes. As

189. *See* Helman, *supra* note 27, at 544–45; Murphy, *supra* note 188.

190. *See, e.g.*, Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481 (1974) (noting "[t]he maintenance of standards of commercial ethics" as an additional "polic[y] behind trade secret law"); E.I. DuPont de Nemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970); Jet Spray Cooler, Inc. v. Crampton, 385 N.E.2d 1349, 1354–55 (Mass. 1979); RESTATEMENT (FIRST) OF TORTS § 757 cmt. f (AM. LAW INST. 1939) (defining wrongful acquisition as means "which fall below the generally accepted standards of commercial morality and reasonable conduct").

191. *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999 (2014) ("Firms will increasingly be able to trigger irrationality or vulnerability in consumers"); Joseph Farrell, *Can Privacy Be Just Another Good?*, 10 J. TELECOMM. & HIGH TECH. L. 251, 252 (2012) ("[L]oss of privacy could identify a consumer as having a high willingness to pay for something, which can lead to being charged higher prices if the competitive and other conditions for price discrimination are present."); *see, e.g.*, Authorization and Authentication Based on an Individual's Social Network, U.S. Patent No. 8,302,164 (filed July 22, 2004) ("In a fourth embodiment of the invention, the service provider is a lender. When an individual applies for a loan, the lender examines the credit ratings of members of the individual's social network who are connected to the individual through authorized nodes. If the average credit rating of these members is at least a minimum credit score, the lender continues to process the loan application. Otherwise, the loan application is rejected."). *See generally* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015) (discussing how powerful interests in the online business abuse users' secrets for profit).

data becomes increasingly central for almost every business,[192] more and more companies maintain vast customer databases.[193] These databases are an obvious source of conflict because the content that they hold (personal data of customers) is the domain of both trade secrecy and privacy law. Consumer databases can almost always be considered trade secrets of the firms that manage them.[194] Yet they are typically not perceived as "secrets" for privacy purposes. The first implication of this insight is that if a database is hacked and the information stolen, the trade secret owner can sue, but absent any particular law that grants such a right to consumers, the information subjects cannot.[195] This is absurd, considering that the leak exposes the subject to much greater harm than the database owner, who can still use the database.[196]

The second implication of the fact that databases comprise a trade secret but not a privacy right is that users can be barred from accessing, challenging, or correcting the information in such databases—unless a particular law specifically grants them such a right.[197] This not only leads to the fact that these databases are often full of incorrect and unverified data, which can be inefficient,[198] but it also makes it more difficult for individuals who do

192. Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1426 ("Providers have what some have called 'Google envy.' Google has demonstrated how to grow rapidly by monetizing user behavior, in their case by displaying advertisements matching a users' recent search queries.").

193. *See* Malgieri, *supra* note 31; DATA BROKERS, *supra* note 130, at 13.

194. *See infra* section II.B.1 (discussing the criteria for establishing trade secrets).

195. *See also* William J. Fenrich, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 956 (1996) ("The balance of power between the direct marketing industry and the consumers upon whose information it depends is currently tilted strongly in favor of the marketers."); Craig D. Tindall, *Argus Rules: The Commercialization of Personal Information*, 2003 U. ILL. J.L. TECH. & POL'Y 181. It may be possible for data subjects to file a lawsuit in data-leakage cases based on negligence or on contractual obligations, or to file a complaint with the FTC.

196. *See, e.g.*, Lee Rainie, Sara Kiesler, Ruogu Kang & Mary Madden, *Anonymity, Privacy, and Security Online*, PEW INTERNET PROJECT (Sept. 5, 2013), http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/ [https://perma.cc/3JE9-NLLH] (finding that "[eleven percent] of internet users have had important personal information stolen such as their Social Security Number, credit card, or bank account information").

197. Granted, one of the most prominent principles of the United States self-regulatory scheme is the individual's right to have notice about the data gathered about herself and the right to know how it will be used. But in practice this requirement is deemed satisfied by privacy policies. *See* Solove & Hartzog, *supra* note 55, at 593. *But see* Helman, *supra* note 27, at 532.

198. Clearly this "inefficiency" can also be desirable when these databases are not desired from a societal point of view to begin with.

not know what information firms hold about them to know that they are imperiled or to prove their cases in court.[199]

As we have seen, trade secrets and privacy law bear fundamental similarities. They also share a basic objective: to encourage mindful sharing of information to enable the flow of the economy and future innovation. Moreover, the fact that trade secrecy is so much stronger than privacy rights is not only a comparative factor that goes to show that private secrets are treated unfairly. The relative strength of trade secrecy means that despite the exponentially increasing stakes for users, trade secrecy hands-down trumps the privacy interests of users in learning or contesting what firms know about them.[200] A more balanced approach would give privacy interests a fair game when users' privacy rights are infringed. In the next section, I explore ways that the law can level the playing ground and enhance the protection of privacy law.[201] This discussion is intended to be suggestive and is certainly not comprehensive. The idea is to demonstrate a new way to conceptualize this matter, which can be expanded upon in subsequent scholarship.

B. *Harmonization in Practice*

To be sure, in highlighting the resemblance between trade secrecy and privacy law, I am mindful that there are differences between the regimes that are justified. For example, attaching property status to information in the privacy context would be highly problematic, as other scholars have demonstrated.[202] Some of the changes that I propose herein should have probably been proposed

199. Kenneth A. Bamberger & Deirdre K. Mulligan, *New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry*, 33 L. & POL'Y 477, 498–99 (2011) (citing an interview with an executive: "I hate to say 'what they don't know won't hurt them,' but that's really how I see it. If we buy personal information . . . or pull some from another database, there's never any way the customers will know about it . . . they won't ever be able to figure out . . . how can they complain?" (alterations in original)).

200. A superficial solution that would also grant users control over these databases, like the European model, would lead to "schizophrenic law" where both users and trade secret holders can control the same source. *See* Malgieri, *supra* note 31.

201. This Article also opens the path to discuss ways to decrease the strength of trade secret law to achieve the same effect. Some scholarship has indeed begun criticizing the broad doctrines of trade secret law in various contexts, though not in the context of the effect of these broad doctrines on privacy law. *See, e.g.*, Menell, *supra* note 36; Fishman & Varadarajan, *supra* note 35.

202. *See, e.g.*, Samuelson, *supra* note 31, at 1136–46.

anyway, regardless of their existence in trade secret law. Yet, as Joseph Fishman and Deepa Varadarajan have mentioned in a different context, "where a proposed rule seems justified on its theoretical merits, it's still helpful to know that another regime has actually employed a similar rule in practice."[203]

Below I consider doctrinal changes that would mirror the above discussion about the doctrinal differences in trade secrecy and privacy law.[204] Indeed, as discussed, privacy and trade secret laws are different in the legal power granted to self-help protective measures taken by the owner, in the standard that they apply to establish secrecy, in the doctrines for third-party liability, in the remedies that they award, and in the institutions that control enforcement.[205] My key proposal below tackles the two first doctrinal differences, by proposing to use the self-help precaution standard as a sufficient condition to trigger a privacy right. I also propose to enhance the liability for conscious third-party infringement of privacy and the remedial landscape of successful privacy lawsuits, which I view as an easier doctrinal leap, and in the case of third-party liability, a mere regulatory oversight. Applying these changes would also bring courts back to the front of the stage in cases of privacy violations and would thus tackle the institutional differences between the laws of privacy and of trade secrets and the remedial space.

1. Establishing a "Secret" Under Privacy Law

Imagine that a new privacy statute provides that a right to privacy would mirror the trade secrecy requirements. The right would then be established for valuable secret information if a person could show that they took reasonable measures to protect the secrecy of the information.[206] The first challenge an individual would have in such a scenario would be to establish that the information that they wish to keep private has value. In the business context of trade secrecy, the requirement is to show that the information

203. Fishman & Varadarajan, *supra* note 35, at 1079. Previous scholarship has identified three doctrines in trade secret law that may be relevant for privacy protection: "the relative secrecy doctrine, a balanced focus on relationships, and a broader view of actionable wrongdoing and actionable harm." *See* Sandeen, *supra* note 31, at 692; *see also* Samuelson, *supra* note 31, at 1152–58.

204. *See supra* section I.B.

205. *See supra* section I.B.

206. *See supra* section I.A.

has "economic value," the definition of which makes complete sense in the trade secrets context.[207] Indeed, trade secrets operate in the business world and their value is determined via economic measures. Yet in the privacy context, a focus on economic value would make little sense. Intuitively, a person should receive protection for information that has value other than that of the economic sort. But expanding the "value" requirement to *any* value would essentially mean foregoing the requirement altogether. Such an expanded value criteria would also raise justified concerns over highly subjective harms and manipulative cases.[208]

How about the second trade secrets prerequisite—that protection would apply to information that is neither "generally known" nor "readily ascertainable"? This requirement may subject privacy protection to the same problems that it faces now under the "expectations of privacy" standard as interpreted by courts.[209] Indeed, it would be unrealistic for users to show that their information is not "generally known" nor "easily ascertained" when virtually everyone's personal information is already all over the Web and subject to rigorous data analytics.[210]

But the idea that users could show that they took precautions in order to trigger protection of their information is in fact rather appealing. I do not propose that the trade secrecy standard of using reasonable precautions would replace the "expectations of privacy" standard. Rather, I propose that taking reasonable measures to protect one's information would satisfy the "expectations of privacy" standard.

Courts would decide ad hoc, on a case-by-case basis, whether the safeguards that a person takes satisfy the "expectations of privacy" standard. Courts already have experience in determining the reasonableness of information precautions from trade secret law.[211] They are thus well suited to make such determinations in privacy cases as well. Courts would also be able to develop jurisprudence around the "reasonableness" of precautions, which would take into

207. *See* UNIF. TRADE SECRETS ACT § 1(4)(i) (UNIF. LAW COMM'N 1985).

208. *See supra* note 136 and accompanying text.

209. *See supra* sections I.A., I.B.

210. *See* Helman, *supra* note 27, at 534 ("Data collection and data analytics technologies also progress at an overwhelming speed, enabling social networks to learn *more* sensitive information from *less* active information sharing by users . . . .").

211. *See supra* Introduction, section I.A.

account changes in technology and social norms,[212] as well as normative considerations such as the desirability of the precautions taken from a societal point of view. Courts' decisions on the matter could thus curtail the creation of precautions that interfere with internet use or generate other negative externalities.[213]

Applying the "reasonable precautions" standard in the privacy context would encourage internet users to share information in a thoughtful, responsible, and cautious manner, and would compel internet platforms and data collectors to mirror users' choices. This is a virtuous policy that would enhance the control of users over the level of privacy that they require and allow them to decide ex ante how each piece of data that they share should be treated. As a result, the "reasonable precautions" standard would generate a data economy that is based on responsible sharing and use of data. This proposal would also be technology-endorsing and induce innovation, because it would incentivize the industry to offer productive self-measures for users that the law would endorse.

I am mindful that this proposal would probably also have the effect of under-protection of uncareful sharing of information. This is particularly troubling in cases where users would not take precautions and would regret their sharing at a later time.[214] Yet under this proposal, the position of such users would not be worse than the current situation, where such users typically do not enjoy protection either.[215] Indeed, as described above, sharing of information today can easily be viewed as consent to almost any use of the information, even by third parties. This proposal would allow for attaching privacy protection to careful acts of information sharing. In any event, complementary rules may need to be created to

212. *See supra* note 90.

213. *See supra* note 188 and accompanying text.

214. *See* Strahilevitz, *supra* note 82, at 679 (discussing cases where people may regret earlier sharing); *see, e.g.*, Virgil v. Time, Inc., 527 F.2d 1122, 1124 (9th Cir. 1975) (discussing the possibility of regretting an agreement for sharing); Jacqueline Howard, *What's the Average Age When Kids Get a Social Media Account?*, CNN (June 22, 2018, 2:22 PM), https://edition.cnn.com/2018/06/22/health/social-media-for-kids-parent-curve/index.html [https://perma.cc/BKK4-UQKT] (noting that people share information on social media when they are younger and may come to regret it later in life); *'Wild' FSU Student Sues*, ORLANDO SENTINEL (Jan. 23, 2002), https://www.orlandosentinel.com/news/os-xpm-2002-01-23-0201230311-story.html [https://perma.cc/U95U-3A4L] (discussing a lawsuit filed by a college student who regretted her earlier exposure); *see also* CARL D. SCHNEIDER, SHAME EXPOSURE AND PRIVACY 42 (1977).

215. *See supra* Introduction, section I.B.

contend with such situations, perhaps in the spirit of the right to be forgotten.

2. Third-Party Liability

I also propose that, like in trade secret law, third parties would incur liability if they traded in information that they knew or should have known was achieved via illegal measures and through violations of privacy. Considering the way that privacy law has evolved, it is safe to assume that the lack of any rule that forbids data brokers from knowingly trafficking illegal content is not the product of deliberate legal decision-making.[216] Most likely, it is the result of oversight or lack of any conscious decision by lawmakers. I am mindful of the fact that requiring data brokers to verify the source of information may sometimes be a burden.[217] Some exceptions or safe harbors may need to be crafted after studying the matter more carefully. Yet overall, I believe that such a change would not only enhance privacy protection, but would also help weed out wrong or harmful information from databases and generate an incentive for the data-sharing industry to operate responsively.[218]

3. Remedies

In trade secrecy, injunctive relief is typically the most relevant remedy because it directly addresses companies' concerns of unfair competition by the misappropriating party. But privacy violations are more diverse. Not every infringement of privacy results in the same kind or the same level of harm. In many cases, it would be more effective to deter potential industry misappropriators via monetary damages than by a ban on using one item out of their vast databases.[219]

The landscape of remedies that courts de facto award in privacy law obviously must be expanded. Yet I believe that a considerable part of the solution would be available once courts adopt the "self-help" recognition that I proposed above. Indeed, once the hurdle of

216. *See supra* sections I.B, I.C.

217. *See supra* note 128 and accompanying text.

218. *See supra* note 129 (collecting sources arguing that the possibility of data laundering through data brokers encourages hacking in the first place).

219. *See also* Sandeen, *supra* note 31, at 705 (proposing to consider statutory damages).

establishing a right under privacy law is overcome, the path to matching remedies to that harm becomes much shorter.

CONCLUSION

Privacy law needs to be conceptualized within a framework that would encourage lawmakers in general, and courts in particular, to enforce it. Privacy law has gone a long time without such a framework. But it cannot maintain this gap for much longer. Increasing commodification of users' data and growing uses of private information cannot afford the lack of a national policy on information privacy.

Fortunately, there is a regime that can provide such a framework. Trade secrecy is an equivalent regime that has solid caselaw, robust policy justifications, and relevant experience in how to identify and protect secrets under the law. While there are differences between trade secrets and personal information, there are sufficient similarities between the goals of trade secrets and privacy law to justify similar rules. At their core, both laws are designed to promote beneficial sharing and to protect information that society values.

My proposal paves the road to thinking of trade secrets standards that can apply to the privacy realm. Most of all, my proposal can change the way the law conceptualizes privacy and can lay a much-needed foundation for this analysis. But it would do so using doctrinal tools that the law already has. Those tools can boost the confidence of both companies and individuals with regards to the use of private data in their businesses and in their lives.