

Privacy Losses as Wrongful Gains

Bernard Chao*

ABSTRACT: Perhaps nowhere has the pace of technology placed more pressure on the law than in the area of data privacy. Huge data breaches fill our headlines. Companies often violate their own privacy policies by selling customer data, or by using the information in ways that fall outside their policy. Yet, even when there is indisputable misconduct, the law generally does not hold these companies accountable. That is because traditional legal claims are poorly suited for handling privacy losses.

Contract claims fail when privacy policies are not considered contractual obligations. Misrepresentation claims cannot succeed when customers never read and rely on those policies. The economic loss rule thwarts many negligence claims. But undoubtedly the thorniest obstacle is that privacy harms are often not considered cognizable injuries under many common legal theories. Tort, contract, and constitutional standing doctrine all demand some form of concrete injury, but privacy injuries are often too intangible or risk-based to qualify. Thus, no matter how blatantly a company violates its privacy obligations or how porous a company's data security is, the victims' lawsuit is often perfunctorily dismissed.

While many commentators have persuasively argued that we should modify these doctrines to better accommodate privacy harms, this Article takes a different tack and revives an old, neglected common law approach to address these modern ills. Privacy victims should use the oft-misunderstood law of restitution and unjust enrichment to disgorge the wrongful gains companies earn when they break their privacy policies. This theory also will allow victims to recover any wrongful savings companies retain when they fail to take reasonable data security precautions and instead use deficient cybersecurity. Because unjust enrichment focuses on the defendant's wrongful gain and not the plaintiff's injury, this theory can avoid many of the pitfalls associated with the more conventional causes of action privacy plaintiffs typically raise.

* Bernard Chao is a Professor at the University of Denver Sturm College of Law. I would like to thank Derek Bambauer, Alan Chen, John Golden, Andrew Kull, Margaret Kwoka, Brian Love, Viva Moffat, Caprice Roberts, and Lauren Scholz for their comments on drafts of this Article. I also want to thank my research assistants, Nick Moore and Veronica Torok, for their help.

I.	INTRODUCTION.....	556
II.	PRIVACY LOSSES AND LEGAL OBSTACLES	558
	A. <i>CONTRACT LAW</i>	559
	B. <i>TORT LAW</i>	564
	C. <i>CONSTITUTIONAL STANDING</i>	567
III.	RESTITUTION AND UNJUST ENRICHMENT	571
	A. <i>THE DISGORGEMENT REMEDY</i>	574
	1. Privacy Promises “Unrelated to Profit”	582
	2. Data Security Promises as “Skipped Services”	584
	B. <i>MISUNDERSTANDING CONTRACTUAL PREEMPTION</i>	587
	C. <i>THE UNJUST ENRICHMENT CAUSE OF ACTION</i>	591
	D. <i>STANDING ON DEFENDANT’S GAIN</i>	595
IV.	COMPLICATIONS	600
	A. <i>OTHER BASES FOR UNJUST ENRICHMENT</i>	600
	B. <i>CONTRACTING AROUND UNJUST ENRICHMENT</i>	602
	C. <i>CALCULATING UNJUST ENRICHMENT</i>	603
V.	CONCLUSION	605

I. INTRODUCTION

Perhaps nowhere has the pace of technology placed more pressure on the law than in the area of data privacy. Huge data breaches fill our headlines. Companies often violate their own privacy policies by selling customer data or by using the information in ways that fall outside their policy. Yet even when there is indisputable misconduct, the law generally does not hold these companies accountable. That is because traditional legal claims are poorly suited for handling privacy losses.

Contract claims fail when privacy policies are not considered contractual obligations. Misrepresentation claims cannot succeed when customers never read and rely on those policies. The economic loss rule (which disallows recovery for purely economic injuries) thwarts many negligence claims. But undoubtedly the thorniest obstacle is that privacy harms are often not considered cognizable injuries under conventional legal theories. Tort, contract, and constitutional standing doctrine all demand some form of concrete injury, but privacy injuries are often too intangible or risk-based to qualify. Thus, no matter how blatantly a company violates its privacy obligations or how porous a company’s data security, the victims’ lawsuit is often perfunctorily dismissed.

Many commentators have persuasively argued that we should modify these doctrines to better accommodate privacy harms.¹ Others hope that legislation can solve some of these problems.² Both approaches are entirely sensible. But this Article advocates a less fashionable approach that has the potential for more immediate relief. That is because it does not rely on changing current law or enacting new laws. Rather the approach seeks to revive a legal theory that is well rooted in the common law. Specifically, this Article suggests that privacy victims should use the often-misunderstood law of restitution and unjust enrichment to disgorge wrongful gains companies earn when they break their privacy policies. This theory supplies both the basis for a more viable cause of action for data privacy plaintiffs and a workable remedy. Employing this theory will also allow victims to recover any wrongful savings companies retain when they fail to take reasonable data security precautions and instead use deficient cybersecurity. Because unjust enrichment focuses on the defendant's wrongful gain and not the plaintiff's injury, this theory can avoid many of the pitfalls associated with the more common causes of action privacy plaintiffs typically raise.

Part II of this Article describes the legal obstacles current privacy victims face in contract law, tort law, and constitutional standing doctrine. These obstacles include failing to recognize privacy policies as contractual obligations; the fact that victims rarely read and rely on privacy policies; and the economic loss rule. However, by far the thorniest obstacle is the nature of privacy victims' harms. Contract law, tort law, and constitutional standing doctrine all demand concrete injuries. But privacy harms are often too intangible and probabilistic in nature (i.e., it is probable but not certain that the loss of sensitive personal information will lead to identity theft or credit card fraud). Moreover, when a more concrete harm does manifest, it is hard to show that any particular wrongful act "caused" the injury. As a result, many otherwise meritorious privacy claims are dismissed at the pleading stage.

Part III of this Article then explains how the law of restitution and unjust enrichment can address the concerns described in Part II. Section III.A starts by explaining how disgorgement should be used as remedy in breach of contract claims. Disgorgement gives the plaintiff a monetary remedy based on the defendant's wrongful gains as opposed to the plaintiff's injury. Disgorgement is often used when expectation damages are inadequate or

1. See M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1132-35 (2011); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 744-46 (2018).

2. See Eric Goldman, *What We've Learned from California's Consumer Privacy Act so Far*, HILL (Jan. 11, 2020, 2:00 PM), <https://thehill.com/opinion/cybersecurity/477821-what-weve-learned-from-the-california-consumer-privacy-act-so-far> [<https://perma.cc/6VDB-B47K>] (arguing that Congress needs to enact uniform privacy laws); Peter M. Lefkowitz, *Why America Needs a Thoughtful Federal Privacy Law*, N.Y. TIMES (June 25, 2019), <https://www.nytimes.com/2019/06/25/opinion/congress-privacy-law.html> [<https://perma.cc/8TQ3-Z7LJ>].

simply difficult to assess. Because privacy injuries confound other traditional doctrines, disgorgement is particularly well suited to address these problems. Section III.B then explains that unjust enrichment is not just a remedy but also an independent source of liability. Thus, applying disgorgement to privacy harms does not rely on a privacy policy being a contractual obligation.

Part III also describes how courts have misunderstood the doctrine of unjust enrichment. Some courts incorrectly assert that unjust enrichment cannot exist when the parties have a contract.³ Other courts have said that unjust enrichment is not an independent cause of action but instead only exists as a remedy (e.g., for breach of contract).⁴ Paradoxically, some courts have actually taken both these views, although not within the same case.⁵ Depending on which decision one reads, an unjust enrichment claim fails because parties have a contract, or conversely, it fails because parties lack a contract. Both understandings are wrong. But unfortunately, these mistaken understandings have frustrated the ability of privacy victims to bring unjust enrichment claims. This Article seeks to clarify this area of the law so courts do not perpetuate these mistakes.

Because the law of restitution and unjust enrichment is flexible and far reaching, it is quite possible that it might expand to involve other “wrongs.” Section IV.A identifies some additional potential “wrongs” that might serve as the basis for an unjust enrichment claim. These include both statutory privacy violations and violations of fiduciary duties. Both theories are natural extensions for the application of unjust enrichment in privacy law.

Section IV.B then discusses an important limitation on the theory of unjust enrichment, the ability to bargain around the remedy. However, the ability to contract out of unjust enrichment is not unbounded. Clauses that seek to avoid liability for gross negligence or seek to avoid statutory obligations are typically invalid. If the defendant’s privacy wrong can be fairly characterized as either gross negligence or as a statutory violation, the ability to contract out of unjust enrichment will likely fail. Thus, while the first step toward widespread adaptation of unjust enrichment in privacy law may lie in contract, the doctrine’s future viability may depend on victims’ ability to find other “wrongs” that cannot be contracted around. Finally, Section IV.C identifies complexities in calculating the proper amount of disgorgement.

II. PRIVACY LOSSES AND LEGAL OBSTACLES

Both contract and tort law present a series of obstacles to privacy victims who seek relief in court. Unfortunately, these obstacles have little to do with the underlying merits of the victims’ grievances. Even when a company has unmistakably broken a privacy promise or engaged in shoddy cybersecurity

3. See *infra* Section III.B for examples.

4. See *infra* Section III.C for examples.

5. See *infra* Section III.C.

that has led to the loss of sensitive personal information, the company can often avoid liability. This is because traditional common law theories are not well suited to address the way privacy losses occur and the kinds of injuries their victims suffer. Breach of contract claimants have difficulty showing that a given promise is part of the contract. Misrepresentation claims fail because no one reads and relies on the broken promises. Causation is a problem for any harm that allegedly resulted from a data breach. But the most significant obstacle is the nature of the privacy victims' injuries. Regardless of whether the claim is based in contract, tort, or even state statutory law (e.g., unfair competition laws), a necessary element is damages. Courts often consider privacy harms to be too intangible or amorphous to recognize.

Recent developments in standing doctrine have only made these problems worse.⁶ Under the Constitution, courts only have jurisdiction over lawsuits when the plaintiff has standing.⁷ The Supreme Court has held that standing requires that a plaintiff be able to show the defendant caused the plaintiff to suffer a tangible and concrete injury.⁸ Unfortunately, the amorphous nature of privacy injuries often means that victims have no standing.⁹ The following two Sections explain why privacy plaintiffs have trouble satisfying the requirements of contract law and tort law. The third Section then explains why standing doctrine also presents unique challenges to privacy victims.

A. CONTRACT LAW

Companies commonly make two kinds of privacy promises. These promises are often found in their privacy policies.¹⁰ First, companies promise to limit how they use or disclose their customers' data (privacy promises). Second, companies often promise to take reasonable measures to secure customer data (cybersecurity promises). Unfortunately, companies have

6. Venkat Balasubramani, *9th Circuit Affirms Rejection of Data Breach Claims Against Gap*—Ruiz v. Gap, TECH. & MKTG. L. BLOG (June 4, 2010), https://blog.ericgoldman.org/archives/2010/06/9th_circuit_aff.htm [<https://perma.cc/BJ87-AH4T>] (noting that a few cases that found cognizable injury went on to be dismissed for lack of Article III standing).

7. U.S. CONST. art. III, § 2.

8. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548–49 (2016).

9. Thomas D. Haley, *Data Protection in Disarray*, 95 WASH. L. REV. 1193, 1195 (2020) (“Even where defendants have clearly acted illegally, federal courts routinely dismiss data-protection lawsuits for lack of standing.”).

10. Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587, 593 (2007) (“By 2001, virtually all of the most popular commercial websites had privacy notices . . .”). The California Online Privacy Protection Act (“CalOPPA”) requires companies that operate websites that collect personal information from California consumers to post their privacy policy. CAL. BUS. & PROF. CODE § 22575 (West 2014). Other federal statutes regulate privacy policies for certain types of industries (e.g., HIPAA for health care and Gramm–Leach–Bliley Act for banking).

frequently violated both their privacy promises and their cybersecurity promises.

A prominent example of a privacy promise involves the four major wireless carriers. Verizon, AT&T, T-Mobile, and Sprint have all promised to stop selling location data to third parties.¹¹ Ring, a maker of doorbells that contain digital cameras, has promised it will only use customer video recordings for research and development unless customers first make the recordings public or otherwise give consent.¹²

One might think that only fly-by-night companies would violate their own policies on how they use or share customer data. But Facebook, Walmart, Google, and even the American Association of Retired Persons (“AARP”) have all been accused of sharing customer data with third parties in violation of their own policies.¹³ Part of the problem may stem from the complexity of modern technology services. For some online services, it may be unclear when they are sending user ID’s or browsing histories. Part of the problem may be bureaucratic. Employees designing customer services may be unaware of their employer’s privacy commitments. But regardless of the underlying cause, broken promises should have consequences. For example, when customers store family photos online only to learn that their host company started using the photos to train facial recognition technology for law enforcement and the military, the company should face liability.¹⁴ The law should hold responsible companies that disclose personal information to third parties against the customer’s wishes.¹⁵ Customers find these behaviors objectionable yet can rarely hold companies accountable.

In addition to privacy promises, companies also regularly make cybersecurity promises. For example, General Motors’ privacy policy states:

11. See Jon Brodtkin, *After Broken Promise, AT&T Says It’ll Stop Selling Phone Location Data*, ARS TECHNICA (Jan. 11, 2019, 11:20 AM), <https://arstechnica.com/tech-policy/2019/01/after-broken-promise-att-says-itll-stop-selling-phone-location-data> [<https://perma.cc/5VKC-CRM6>].

12. See *Privacy*, RING, <https://shop.ring.com/pages/privacy> (last visited Nov. 16, 2020).

13. See, e.g., *Cappello v. Walmart Inc.*, 394 F. Supp. 3d 1015, 1022 (N.D. Cal. 2019) (accusing Walmart of sharing customer information with Facebook in violation of its own policy which required customers to “opt in” to the sharing of personal information); *Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2015 WL 1503429, at *1 (N.D. Cal. Apr. 1, 2015) (accusing Google of sharing private customer information with App vendors in violation of Google Wallet’s privacy policy); *Austin-Spearman v. AARP*, 119 F. Supp. 3d 1, 3 (D.D.C. 2015) (accusing AARP of sharing personally identifiable information with Facebook and Adobe in violation of AARP’s privacy policy).

14. Ever, a company that stored customer’s photos, began using the photos to train facial recognition technology. The company changed its privacy policy after NBC reached out to the company to inquire about the practice. Olivia Solon & Cyrus Farivar, *Millions of People Uploaded Photos to the Ever App. Then the Company Used Them to Develop Facial Recognition Tools.*, NBC NEWS (May 9, 2019, 3:10 AM), <https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371> [<https://perma.cc/RP3H-5QUK>].

15. See, e.g., *Carlsen v. GameStop, Inc.*, 833 F.3d 903, 906–08 (8th Cir. 2016) (alleging defendant violated its own privacy policy by disclosing personally identifiable information with Facebook).

“We maintain reasonable and adequate technical, administrative, and physical security and confidentiality measures designed to help protect your information from unauthorized access or acquisition.”¹⁶ Perhaps, it is less surprising to hear that companies regularly break their cybersecurity promises. The headlines are full of stories of well-known companies that have lost customer data due to inexcusable cybersecurity. Equifax lost the personal data of 143 million people because it did not update its system with a data patch that was available for more than two months prior to the breach.¹⁷ In 2018, Marriott disclosed sensitive personal information, including 5.25 million unencrypted passport numbers, on approximately 383 million customers.¹⁸ Apparently the attackers had been in the Starwood network since 2014 and should have been detected years earlier.¹⁹ A report by the Internet Society’s Online Trust Alliance found that 95 percent of breaches in 2018 were preventable,²⁰ but the list of offenders that could have easily avoided data breaches keeps growing.²¹

Despite these broken promises, victims typically have trouble bringing successful breach of contract claims. The problem is that the traditional breach of contract claim is not a good fit for privacy policy violations. There are three significant obstacles. First, privacy promises are not always part of the customer’s contract with the company. Courts often require the promises to be somehow incorporated in the customer contract to be enforceable.²² If

16. *Privacy Statement*, GEN. MOTORS (Jan. 2020), <https://www.gm.com/privacy-statement.html>.

17. Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017, 1:27 PM), <https://www.wired.com/story/equifax-breach-no-excuse> [<https://perma.cc/44F8-YVER>].

18. Ben Popken, *Marriott Reveals 5 Million Unencrypted Passport Numbers Were Leaked in 2018 Data Breach*, NBC NEWS (Jan. 4, 2019, 11:24 AM), <https://www.nbcnews.com/tech/tech-news/marriott-reveals-5-million-unencrypted-passport-numbers-were-leaked-2018-n954791> [<https://perma.cc/74KF-3VZ7>].

19. See Robert McMillan, *Marriott’s Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, WALL ST. J. (Dec. 2, 2018, 5:11 PM), <https://www.wsj.com/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659> [<https://perma.cc/R7WK-KJGY>]; Zack Whittaker, *Marriott Now Says 5 Million Unencrypted Passport Numbers Were Stolen in Starwood Hotel Data Breach*, TECHCRUNCH (Jan. 4, 2019, 11:11 AM), <https://techcrunch.com/2019/01/04/marriott-five-million-passport-numbers-stolen-starwood> [<https://perma.cc/AG6R-WD86>].

20. ONLINE TR. ALL., 2018 CYBER INCIDENT & BREACH TRENDS REPORT 3 (2019), https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf [<https://perma.cc/X6PV-XY4Y>].

21. See István Molnár, *How 2019’s Worst Corporate Hacks Could Have Been Prevented*, INFOSECURITY (Jan. 13, 2020), <https://www.infosecurity-magazine.com/blogs/worst-corporate-hacks-prevented> [<https://perma.cc/N7EB-BJZF>].

22. See, e.g., *In re Facebook Internet Tracking Litig.*, 290 F. Supp. 3d 916, 920 (N.D. Cal. 2017) (finding promise not to track logged-out users was not part of plaintiffs’ contract with Facebook), *aff’d in part, rev’d in part sub nom. In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020); *Austin-Spearman v. AARP*, 119 F. Supp. 3d 1, 12 (D.D.C. 2015) (“[T]he promises made in AARP’s Privacy Policy were not a part of Austin-Spearman’s binding AARP membership contract.”); *In re Nw. Airlines Priv. Litig.*, No. Civ.04-126(PAM/JSM), 2004 WL

they are not, the company has not breached any contractual obligation.²³ Thus, companies can make empty promises that make their business practices appear responsible. But they are not penalized for failing to honor these promises. Second, victims of data breaches may have trouble proving causation. If the alleged injury is identity theft or credit card fraud, it is often difficult to trace that injury to the defendant's specific breach.²⁴ Ironically, the fact that so many companies suffer from data breaches helps shield individual companies from liability. To date, when causation has come up in the context of pretrial motions, privacy victims have often been able to satisfy the laxer pleading standards.²⁵ However, it is unclear what level of proof will be necessary at trial.²⁶ Each of the first two obstacles is significant and can cause a court to dismiss an otherwise meritorious privacy claim. But by far the largest problem is that courts have found that the type of injuries that privacy victims suffer are not cognizable contract law injuries.

In an effort to overcome this problem, privacy victims have tried to characterize their injuries in several distinct ways regardless of which cause of action they are using.²⁷ This Article addresses privacy injuries first with respect to contracts, but privacy victims identify the same kinds of injuries in support

1278459, at *6 (D. Minn. June 6, 2004) ("The privacy statement on Northwest's website did not constitute a unilateral contract.").

23. There is a vigorous debate about whether courts actually treat privacy policies as contractual obligations. Compare Oren Bar-Gill, Omri Ben-Shahar & Florencia Marotta-Wurgler, *Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts*, 84 U. CHI. L. REV. 7, 25–30 (2017) (explaining the methodology and results of a study conducted by the Reporters for the new Restatement of Consumer Contracts, which found that courts recognize privacy policies as contracts), with Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 YALE J. ON REGUL. 45, 49 (2019) (reanalyzing the data from the Reporters' study and concluding that the data does not support their conclusions). Klass' findings appear more consistent with the observations of privacy scholars. See *infra* notes 33–38 and accompanying text (discussing how contract law has not played much role in privacy law).

24. See *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. 2012) ("[T]o prove that a data breach caused identity theft, the pleadings must include allegations of a nexus between the two instances beyond allegations of time and sequence."); *Stollenwerk v. Tri-West Health Care All.*, 254 F. App'x 664, 668 (9th Cir. 2007) (requiring plaintiff to show a causal relationship between the burglary of computers and the plaintiff's identity theft).

25. See *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 987 (N.D. Cal. 2016) ("[A]llegations . . . that each [p]laintiff had his or her [personal information] stolen, and that specific aspects . . . were used for illicit financial gain after the breach . . . establish the requisite logical and temporal connection necessary to demonstrate causation."); *Resnick*, 693 F.3d at 1327–28 ("Because their contention that the data breach caused the identity theft is plausible under the facts pled, [p]laintiffs meet the pleading standard . . .").

26. *Collins v. Athens Orthopedic Clinic, P.A.*, 837 S.E.2d 310, 316 n.6 (Ga. 2019) ("Proving that the plaintiff's injuries were proximately caused by the breach may also be more difficult.").

27. *Solove & Citron*, *supra* note 1, at 749 ("Although plaintiffs advance a number of theories of harm, at bottom, their claims are based on three overarching theories . . .").

of their tort and statutory claims too.²⁸ The categories roughly break down as follows: (1) risk of future injury; (2) the economic value of their personal data; (3) emotional distress of having their personal data stolen; and (4) the economic cost of taking precautions to avoid misuse of their information.²⁹

Although there are certainly exceptions, courts generally say that victims cannot recover any damages for these injuries.³⁰ First, courts largely do not recognize increased risk of identity theft because it is too speculative.³¹ Second, courts have said that unaggregated personal information has no value.³² After all, individuals typically cannot sell their own data. Third, except in rare circumstances, contract law only recognizes economic damages.³³ Therefore, emotional distress is not usually recoverable when companies break their privacy promises.³⁴ Fourth, courts generally do not compensate individuals for taking preventative measures to protect against future

28. *Id.* at 770 (discussing mental distress and “harms of broken trust, betrayal, and disrupted expectations of secrecy” (quoting Nancy Levit, *Ethereal Torts*, 61 GEO. WASH. L. REV. 136, 147–48 (1992))).

29. *Id.* at 749–50 (noting the risk of future injury, cost of preventative measures, and distress); *see, e.g.*, *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 912–13 (7th Cir. 2017) (discussing the concept of the economic value of personal data).

30. *See* Aaron Wynhausen, Note, *The Eighth Circuit Further Complicates Plaintiff Standing in Data Breach Cases*, 84 MO. L. REV. 297, 304 (2019) (“Yet, to date, most data breach class action cases have been dismissed either due to a plaintiff’s inability to show an injury in fact for purposes of standing or failure to state a claim for which relief can be granted.”); Balasubramani, *supra* note 6 (“The overwhelming majority of courts have rebuffed data breach claims brought by affected persons (particularly those that have been offered monitoring) on the basis that those individuals have not suffered any appreciable injury.”).

31. *See* Solove & Citron, *supra* note 1, at 750–52 (describing various cases rejecting risk of future harm); *see also In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, No. 14-MD-2586 ADM/TNL, 2016 WL 81792, at *4, *8 (D. Minn. Jan. 7, 2016) (noting “the vast majority of courts have held that the risk of future identity theft or fraud is too speculative to constitute an injury in fact for purposes of Article III standing” and dismissing claims for negligence, breach of contract, and various statutory claims), *aff’d in part, rev’d in part*, 870 F.3d 763 (8th Cir. 2017). On appeal the Eighth Circuit said that the risk of identity theft and credit card theft were too “unlikely” to support a cause of action. *SuperValu*, 870 F.3d at 771.

32. *See, e.g.*, *Gubala*, 846 F.3d at 913 (characterizing plaintiff’s argument that defendant’s unlawful retention of personal information deprived plaintiff of economic value “gibberish”); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1040 (N.D. Cal. 2019) (“As to the loss of value of the personal information, plaintiff Adkins has provided no market for the personal information or the impairment of the ability to participate in that market. This lack of specificity is fatal.”); *In re JetBlue Airways Corp. Priv. Litig.*, 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005) (“There is likewise no support for the proposition that an individual passenger’s personal information has or had any compensable value in the economy at large.”).

33. RESTATEMENT (SECOND) OF CONTS. § 353 (AM. L. INST. 1981) (“Recovery for emotional disturbance will be excluded unless the breach also caused bodily harm or the contract or the breach is of such a kind that serious emotional disturbance was a particularly likely result.”).

34. Solove & Citron, *supra* note 1, at 753 (noting that courts reject claims of anxiety “nearly every time”); *see, e.g.*, *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 718 (8th Cir. 2017) (“Massive class action litigation should be based on more than allegations of worry and inconvenience.”).

injuries.³⁵ Again, that is because such measures protect against speculative, not past, harm.

Professors Solove and Citron have explored all these problems in detail and explained that “[t]he difficulty largely stems from the fact that data-breach harms are intangible, risk-oriented, and diffuse.”³⁶ Narrow definitions of harm persist even though consumers view data privacy harms more broadly: For example, many report they would pay to opt out of biometric data collection programs because of concerns about future harm.³⁷ Nonetheless, these enduring limitations make it difficult to raise a breach of contract claim and demonstrate why contract law has proven to be “largely irrelevant to information privacy law in the United States.”³⁸

B. TORT LAW

Tort law is also not a good fit for the problems privacy victims have. The classic privacy torts—(1) intrusion upon seclusion; (2) appropriation of name or likeness; (3) publicity given to private life; and (4) false light—are not well-suited for addressing the kind of broken promises that companies make in today’s data driven society.³⁹ These torts require a variety of elements that routinely do not apply to the loss or misuse of customer data. That may be because these torts require that the information at issue be “highly offensive” (cases 1 and 3), that the information be disclosed publicly (cases 3 and 4), or that the customer’s name or likeness be taken (case 2). In one way or another, these torts simply do not apply to most modern-day corporate privacy wrongs.

Thus, plaintiffs typically raise two primary kinds of more general tort claims: misrepresentation (i.e., fraud or negligent misrepresentation) and negligence. Since reliance is an element of all misrepresentation-based torts, these privacy claims require that plaintiffs have read and relied on the misrepresentation.⁴⁰ But most consumers have understandably not read

35. Solove & Citron, *supra* note 1, at 753; *see, e.g.*, *Reilly v. Ceridian Corp.*, 664 F.3d 38, 46 (3d Cir. 2011) (“[T]hey prophylactically spent money to ease fears of future third-party criminality. Such misuse is only speculative—not imminent. The claim that they incurred expenses in anticipation of future harm, therefore, is not sufficient to confer standing.”); *SuperValu*, 870 F.3d at 771 (“Because plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury.”).

36. Solove & Citron, *supra* note 1, at 737.

37. Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107, 142–43 (2019).

38. Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 151 (2017); *see also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 596 (2014) (“[C]ontract law . . . plays hardly any role in the protection of information privacy, at least vis-à-vis websites with privacy policies.”).

39. *See* RESTATEMENT (SECOND) OF TORTS §§ 652B–652E (AM. L. INST. 1977) (providing the elements of each of these torts).

40. *See id.* §§ 525, 552 (providing the elements of fraudulent and negligent misrepresentation).

privacy policies, let alone relied upon them.⁴¹ As a result, courts routinely dismiss claims for fraud and negligent misrepresentation.⁴² Commentators have also proposed promissory estoppel claims as a potential solution for privacy victims.⁴³ While promissory estoppel is generally considered part of contract law, the doctrine actually shares much in common with misrepresentation torts. Most relevantly, promissory estoppel requires reliance, and for that reason it does not help privacy plaintiffs either.⁴⁴

Thus, privacy victims typically resort to general negligence claims. As discussed in Section II.A, companies' deficient cybersecurity has allowed hackers to access billions of individuals' private information. Moreover, in many cases, it is not hard to characterize companies' behavior as unreasonable or falling below industry standards. Nevertheless, the nature of the victims' harm can thwart negligence claims. Here, privacy victims must contend with the economic loss rule. Although there is some variation on how the rule operates, at its core, the rule bars a plaintiff from recovering purely economic losses for negligence claims.⁴⁵ Since there is rarely physical injury in privacy cases, when the economic loss rule applies, it can defeat a privacy victim's negligence claim.

The rationale underlying the economic loss rule depends on whether it is being applied to strangers or to contracting parties. In some cases, privacy victims do not have a contractual relationship with the company that lost their data. These cases often fit in the so-called "stranger" category of economic loss cases. For example, Equifax collects credit information about consumers, but most people affected by the Equifax data breach probably did not have a contract with Equifax.⁴⁶ However, in the majority of data breach cases, it's the

41. Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261, 304 (2014) (explaining that it is rational for consumers not to read privacy policies); Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts"*, 78 U. CHI. L. REV. 165, 168 (2011) (estimating that "the overall average rate of readership of [end user license agreements] is on the order of 0.1 percent to 1 percent").

42. See, e.g., *Carlsen v. GameStop, Inc.*, 112 F. Supp. 3d 855, 865 n.4 (D. Minn. 2015) (dismissing misrepresentation claims because plaintiff failed to plead that they read and relied on privacy policy), *aff'd on other grounds*, 833 F.3d 903 (8th Cir. 2016); *In re iPhone Application Litig.*, 6 F. Supp. 3d 1004, 1020 (N.D. Cal. 2013) (granting summary judgment on misrepresentation claims because plaintiffs failed to show that they read and relied on Apple's privacy policies).

43. Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181, 208 (2016); Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. 653, 670 (2019).

44. Norton, *supra* note 43, at 194-95; see also *Smith v. Trusted Universal Standards in Elec. Transactions, Inc.*, No. 09-4567 (RBK/KMW), 2011 WL 900096, at *10 n.10 (D.N.J. Mar. 15, 2011) (holding lack of evidence of reliance precludes promissory estoppel).

45. Dan B. Dobbs, *An Introduction to Non-Statutory Economic Loss Claims*, 48 ARIZ. L. REV. 713, 713 (2006) ("Negligently inflicted economic loss that results from some other kind of injury may be recoverable, but recovery for stand-alone economic loss is frequently rejected.").

46. See *supra* text accompanying note 17 (discussing Equifax data breach).

company's customers who lose their data. For the stranger paradigm, the rule operates to prevent unlimited liability.⁴⁷ For contracting parties, the idea is to prod the parties to allocate risks through contract as opposed to imposing them by law.⁴⁸ Both of these justifications can potentially affect how the economic loss rule applies to data breach cases.⁴⁹ Consequently, there is much "confusion . . . as to whether and how the economic loss rule should apply" to these cases.⁵⁰

Numerous defendants have successfully raised the economic loss rule to reject negligence causes of action for data breach claims.⁵¹ Depending on the jurisdiction, the rule has important exceptions that privacy victims may be able to use. Some states have an independent duty exception which permits negligence claims when the defendant has a duty that does not arise from a contract.⁵² Other states have a "special relationship" exception which permits negligence claims for economic loss when there is a special relationship that would warrant imposing on the defendant a duty to act with reasonable care towards the plaintiff.⁵³ The result is that the viability of negligence claims is jurisdiction dependent.⁵⁴

But even if privacy plaintiffs can overcome these threshold issues, they still have to show a cognizable injury. Here, the obstacles look very much like the ones presented by contract law. The injuries privacy victims suffer are simply not recognized by the law of negligence.⁵⁵ As they do for contract claims, privacy victims that are pursuing tort claims characterize their injuries

47. Catherine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DEPAUL L. REV. 339, 344 (2017) (describing justifications for the economic loss rule).

48. *Id.* at 344-45.

49. *Id.* at 345 (noting that the credit card data security cases "often straddle the stranger/contracting parties paradigms" because of the "complex web of contracts" involved in the credit card transactions).

50. *Id.* at 344.

51. *See, e.g., In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1176 (D. Minn. 2014) (dismissing data breach negligence claims for five state-law claims based on the economic loss doctrine but allowing those same claims in the other six states to proceed).

52. *See, e.g., In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1321 (N.D. Ga. 2019) (applying Georgia law and finding that independent duty exception applied because companies "that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information[.]" (alteration in original) (quoting *Brush v. Mia. Beach Healthcare Grp. Ltd.*, 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017))).

53. *See, e.g., J'Aire Corp. v. Gregory*, 598 P.2d 60, 63 (Cal. 1979) (discussing six factors that determine whether the defendant owes the plaintiff a duty based on a special relationship).

54. Sharkey, *supra* note 47, at 342 ("[T]he extent to which the economic loss rule serves as a formidable barrier to credit card data security breach cases depends upon the underlying state law . . .").

55. Solove & Citron, *supra* note 1, at 754 ("Even in the face of wrongful conduct by defendants, courts are denying plaintiffs redress . . . because courts view the harm in overly narrow ways.").

in various ways.⁵⁶ And like contract law, tort law does not recognize these harms. When the alleged injuries are the risk of future harm or the expense of taking precautions, courts say these injuries are too remote or speculative.⁵⁷ Similarly, lost personal information has no value under tort law. Most privacy lawsuits are only viable when the victims' information has actually been misused.⁵⁸ The typical examples are identity theft and credit card fraud.⁵⁹ This is a very narrow set of claims, too inflexible to accommodate new types of injuries that technological advances inflict. In sum, traditional common law claims are not well suited for holding companies accountable for breaking their privacy promises or having shoddy cybersecurity.

C. CONSTITUTIONAL STANDING

For victims of privacy losses, constitutional standing poses yet another significant challenge. A 2020 study revealed that courts found standing in only 55 percent of cases that were based on data privacy or data breach claims.⁶⁰ When the case was related to a claim for data breach, standing was found in only 47 percent of the cases.⁶¹ Standing has proved to be an obstacle for all sorts of data protection claims including privacy torts, non-privacy torts, other common law claims, and even statutory claims.⁶² Cases denying standing included federal causes of action as well as state statutory violations, which were the study's largest categorical subset of data protection claims submitted for federal court review.⁶³

Standing is rooted in the Constitution's case or controversy requirement.⁶⁴ The doctrine limits the types of plaintiffs who can seek relief from the courts. Standing doctrine has evolved to have three primary requirements: (1) "the plaintiff must have suffered an 'injury in fact'"; (2) "there must be a causal connection between the injury and the [alleged

56. See *supra* text accompanying notes 27–29.

57. Solove & Citron, *supra* note 1, at 741 n.20, 753 nn.93–94 (listing cases in which future harm and precautionary expenses were deemed insufficiently injurious).

58. Wynhausen, *supra* note 30, at 317–18 (noting that, to bring a data breach action in the Eighth Circuit, "plaintiffs [should] have a credible allegation of identity theft that is somehow traceable to the data breach" and further concluding that "mere risk of identity theft is not enough").

59. Solove & Citron, *supra* note 1, at 750–51; see, e.g., *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 366 (M.D. Pa. 2015) (citing *Reilly v. Ceridian Corp.* and finding no impending injury because there were no allegations of impersonation and no changes to plaintiffs' credit information or bank accounts).

60. See Haley, *supra* note 9, at 1224; see also Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 439 (2017) ("Article III standing has emerged as a major barrier to federal court litigation for plaintiffs who assert a violation of their privacy rights.").

61. Haley, *supra* note 9, at 1225.

62. *Id.* at 1225–29.

63. *Id.* at 1226–27 (reporting that state statutory violations were the most prevalent type of data-protection claim in the 209 federal court cases analyzed, appearing in 65 percent of cases).

64. U.S. CONST. art. III, § 2.

wrongful] conduct,” and; (3) the injury must be likely to be redressed by a favorable judicial decision.⁶⁵

Privacy’s standing problem can be traced to the Supreme Court’s decision in *Clapper v. Amnesty International*.⁶⁶ In *Clapper*, the plaintiffs sued to halt the U.S. government’s expansive foreign surveillance program.⁶⁷ The Supreme Court held that the plaintiffs lacked standing to challenge the government’s actions because they could not show that their specific communications were being intercepted.⁶⁸ The *Clapper* plaintiffs’ injuries were not “certainly impending.”⁶⁹ Rather, the alleged harms relied on what the Court called a “speculative chain of possibilities.”⁷⁰ Moreover, to the extent that the plaintiffs undertook costly and burdensome precautions to protect their international communications, the Supreme Court said the plaintiffs could not “manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm.”⁷¹ The result was that individuals could not sue unless they learned the government was intercepting their specific communications. Given that the surveillance program was secret, this was a daunting obstacle. It was only when Edward Snowden leaked information about the program that a subsequent group of plaintiffs had standing to sue the government.⁷²

Clapper has had a powerful influence on standing in data privacy law. While some courts have recognized standing based on financial outlay and the increased risk of various concrete privacy harms like identity theft,⁷³ many decisions continue to rely heavily on *Clapper* and find that data protection plaintiffs lack standing.⁷⁴ In these cases, the reasoning is strikingly similar to

65. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992).

66. *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 410–18 (2013).

67. *Id.* at 401–07.

68. *Id.* at 410.

69. *Id.*

70. *Id.* at 410, 414.

71. *Id.* at 416.

72. The ensuing case was *ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *aff’d in part, vacated in part*, 785 F.3d 787 (2d Cir. 2015). See Seth F. Kreimer, “Spooky Action at a Distance”: *Intangible Injury in Fact in the Information Age*, 18 U. PA. J. CONST. L. 745, 762–63 (2016) (discussing Snowden’s role in the standing issue).

73. See Solove & Citron, *supra* note 1, at 742 (discussing various cases that “pushed back against the trend” and found standing); see also *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App’x 384, 389–90 (6th Cir. 2016) (finding standing where data breach victims suffered an “identifiable taking” of personal data and a concrete injury in reasonably incurred mitigation costs (quoting *Reilly v. Ceridian Corp.*, 664 F.3d 38, 44 (3d Cir. 2011))); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) (finding standing because of “an ‘objectively reasonable likelihood’” that hackers would use data breach victims’ stolen credit card information (quoting *Clapper*, 568 U.S. at 410)).

74. See Haley, *supra* note 9, at 1220–21 (finding that 49.3 percent of post-*Clapper* privacy cases cited *Clapper*, while 64 percent of plaintiffs in these 103 cases were denied standing).

that found in *Clapper*.⁷⁵ As a threshold matter, courts have found that the mere loss of data in a cyberattack without evidence that it has been misused is insufficiently concrete to confer standing.⁷⁶ To the extent that the plaintiffs attempt to rely on the substantially increased risks of credit card misuse or identity theft, courts say that the alleged harms are too remote and rely on a speculative chain of possibilities. Finally, when the victims point out they paid for credit monitoring services and took other burdensome preventative measures, courts have said that plaintiffs “cannot manufacture standing” by taking precautions to avoid an uncertain injury.⁷⁷

Standing is not just an obstacle for victims of cyberattacks. It can also present a problem for those seeking to compel companies to comply with statutory privacy obligations. In *Spokeo, Inc. v. Robins*, the website Spokeo published inaccurate information about the plaintiffs.⁷⁸ The plaintiffs then brought suit under the Fair Credit Reporting Act (“FCRA”), which “seeks to ensure ‘fair and accurate credit reporting.’”⁷⁹ The question presented to the Supreme Court was whether the plaintiffs’ injuries were sufficiently concrete to provide them with standing.⁸⁰ The Supreme Court noted that standing is not “automatic[.]” just because there is a law that “grants a person a statutory right and purports to authorize that person to sue to vindicate that right.”⁸¹ By enacting legislation, “Congress may ‘elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.’”⁸² But there still must be a concrete harm, and “bare procedural violation[s]” will not be enough for standing.⁸³ This result can undermine privacy statutes. For example, Congress has enacted several statutes that place restrictions on the storage of personal data and give victims a private cause of

75. See *id.* at 1220–23; Solove & Citron, *supra* note 1, at 741 (“In decision after decision, courts have relied on *Clapper* to dismiss data-breach cases.”).

76. E.g., *Reilly*, 664 F.3d at 42 (finding that victims whose data was exposed in a cyberattack had no standing because they “have not suffered any injury; there has been no misuse of the information, and thus, no harm”); *In re Sci. Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 19 (D.D.C. 2014) (“[M]ost [courts] have agreed that the mere loss of data—without evidence that it has been either viewed or misused—does not constitute an injury sufficient to confer standing.”).

77. *In re Sci. Applications Int’l Corp.*, 45 F. Supp. 3d at 24 (quoting *Clapper*, 568 U.S. at 416); see *id.* at 26; see also *Clapper*, 568 U.S. at 416 (holding that plaintiffs concerned about unlawful government surveillance do not have standing based on “certain costs as a reasonable reaction to a risk of harm” that “is not certainly impending”).

78. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1544 (2016).

79. *Id.* at 1545 (quoting 15 U.S.C. § 1681(a)(1) (2018)).

80. See *id.*

81. *Id.* at 1549.

82. *Id.* (alteration in original) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 578 (1992)).

83. *Id.* at 1549–50.

action.⁸⁴ But for some statutes, courts have denied standing to plaintiffs, effectively neutering them.⁸⁵

Commentators have criticized privacy law's standing doctrine on both theoretical and doctrinal grounds. Solove and Citron have explained how other areas of the law recognize injuries similar to those suffered by privacy victims and argue that privacy harms should receive the same treatment.⁸⁶ Felix Wu says that standing doctrine has changed in unjustifiable ways.⁸⁷ While the doctrine's original focus was to channel policy questions to the political branches, the standing doctrine's current incarnation causes courts to overreach. Under the modern interpretation, courts are effectively deciding individuals' substantive privacy rights.⁸⁸ This is true even though Congress has determined that certain privacy breaches deserve a remedy. These decisions actually flip one of the rationales behind standing on its head. Instead of keeping the federal courts from meddling in policy, these decisions overrule the political branches' policy decisions. Wu calls this "a usurpation of legislative power."⁸⁹

Critics have also argued that when it comes to privacy, the lower courts are simply misinterpreting *Clapper*. Seth Kreimer argues that *Clapper* should be understood to mean that the "illicit acquisition of personal information is a cognizable 'injury in fact' in and of itself."⁹⁰ Finally, because the Supreme Court itself has suggested that standing is different for private parties

84. Stored Communications Act, 18 U.S.C. §§ 2701–2713 (2018); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2018); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (2018); Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–2725 (2018); Fair Credit Reporting Act, 15 U.S.C. § 1681 (2018); Video Privacy Protection Act, 18 U.S.C. § 2710 (2018).

85. See *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 912–13 (7th Cir. 2017) (concluding there was no standing for wrongful retention of data in violation of the Cable Communications Policy Act when there were no allegations that defendant had disclosed data); *Braitberg v. Charter Commc'ns, Inc.*, 836 F.3d 925, 930 (8th Cir. 2016) (same); *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 514 (D.C. Cir. 2016) (reasoning that collecting zip codes in violation of two D.C. statutes did not give rise to a sufficiently concrete injury for standing); see also *Frank v. Gaos*, 139 S. Ct. 1041, 1046 (2019) (remanding a case in which Google attempted to settle a case alleging that it violated the Stored Communications Act to determine whether the plaintiff had a sufficiently concrete injury to justify standing).

86. Solove & Citron, *supra* note 1, at 761–64 (describing how the law recognizes "probabilistic injuries" in several contexts); see also Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change*, 66 DEPAUL L. REV. 535, 542–43 (2017) (pointing out that courts assess the value of information and data in intellectual property contexts). See generally Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361 (2014) (arguing that harms in privacy law are not exceptional).

87. See Wu, *supra* note 60, at 460–61.

88. *Id.* at 457–58. For example, apparently Congress can no longer enact legislation that uses a private cause of action to enforce restrictions on the storage of personal data unless the victims suffer tangible injury as defined by the Supreme Court. See, e.g., *supra* notes 84–85 and accompanying text.

89. Wu, *supra* note 60, at 458.

90. Kreimer, *supra* note 72, at 765.

vindicating private rights (as opposed to public rights), several commentators have argued that courts should not apply *Clapper* to cases where victims are asserting that their data was wrongfully lost.⁹¹ Indeed, this is the minority position for which Justice Thomas advocated.⁹²

But despite a large body of criticism, standing still remains a serious hurdle for privacy victims trying to vindicate their rights. Thomas Haley has summed up the problem by saying that “[j]udicial reticence to recognize harm in data-protection litigation contributes to rampant, judicially approved, consequence-free lawbreaking by businesses, which continue to improperly collect, store, trade, and lose valuable private information.”⁹³ But it is not just standing that stymies meritorious privacy claims. As discussed in the preceding Sections, the law’s conception of privacy injuries generally also hinders victims’ ability to bring privacy claims. As Solove and Citron put it: “No matter how derelict defendants might be with regard to security, no matter how much warning defendants have about prior hacks and breaches, if plaintiffs cannot show harm, they cannot succeed in their lawsuits.”⁹⁴

When one also considers whether privacy policies are contracts, whether victims have read and relied on the broken promises, and the economic loss rule, it becomes clear that plaintiffs must walk through a veritable gauntlet of legal obstacles to hold companies accountable for even the most egregious privacy violations. But this does not mean the law has no answer for privacy claims. In Part III, this Article explains why the law of restitution and unjust enrichment can overcome many of the legal hurdles privacy victims’ claims commonly face.

III. RESTITUTION AND UNJUST ENRICHMENT

Tort, contract, and standing doctrine all have trouble addressing privacy harms because they are too amorphous. In response, scholars argue that courts should push at the edges of these doctrines to recognize privacy harms.⁹⁵ Such thinking is both logical and desirable.

But this Article offers an alternative front; a different way that others have generally ignored. The current doctrinal limitations exist because they focus on the *harm plaintiffs suffer*. But that is not how the law of restitution and unjust enrichment operates. This often-misunderstood area of the law focuses on the

91. See Haley, *supra* note 9, at 1224; Wu, *supra* note 60, at 446–51, 461.

92. See *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1552 (2016) (Thomas, J., concurring) (“[T]he concrete-harm requirement does not apply as rigorously when a private plaintiff seeks to vindicate his own private rights.”); *Frank v. Gaos*, 139 S. Ct. 1041, 1046–47 (2019) (Thomas, J., dissenting) (“As I have previously explained, a plaintiff seeking to vindicate a private right need only allege an invasion of that right to establish standing.”).

93. Haley, *supra* note 9, at 1197.

94. Solove & Citron, *supra* note 1, at 739.

95. *Id.* at 785 (arguing that courts should take the opportunity “to push doctrines in a progressive direction when it comes to data-beach harms”).

*defendant's wrongful gain.*⁹⁶ Moreover, it does not require that the broken privacy promise result in any particular harm like identity theft. Consequently, restitution can provide victims of privacy breaches a way forward.

To date, most privacy scholars have overlooked restitution. Consider Solove and Citron's important article on data breach harms. The authors are two of the leading experts on privacy law.⁹⁷ But their article never uses the term "restitution" and it only mentions "unjust enrichment" as one of the "tools that can be used to address harm."⁹⁸ Even then, the reference is only found in a single sentence in the article's conclusion, and there is no citation to a source or discussion of the claim.⁹⁹

This is not to say that unjust enrichment and restitution have been totally overlooked in privacy law. Attorneys raise unjust enrichment in privacy lawsuits but often as an afterthought following a long list of other causes of action.¹⁰⁰ As a result, court decisions on unjust enrichment often address the issue perfunctorily.¹⁰¹ Some academics have also said that unjust enrichment and restitution have a place in privacy law. In an amicus brief filed in *Spokeo, Inc. v. Robins*, a leading group of remedies scholars argued that unjust enrichment and restitution can provide standing when privacy injuries are otherwise insufficient.¹⁰² Lauren Scholz has built on this work and concluded that the doctrine can also solve privacy's "harm problem."¹⁰³ While Scholz focuses on privacy ills caused by companies that do not have a relationship with the injured party, this Article primarily focuses on holding companies

96. See, e.g., *Wright v. Genesee County*, 934 N.W.2d 805, 811 (Mich. 2019) ("Unjust enrichment has evolved from a category of restitutionary claims with components in law and equity into a unified independent doctrine that serves a unique legal purpose: it corrects for a benefit received by the defendant rather than compensating for the defendant's wrongful behavior.").

97. Professor Solove is the co-author of several privacy casebooks and a privacy treatise, founder of the blog TeachPrivacy, and author of numerous privacy articles. *Daniel Justin Solove*, GEO. WASH. L., <https://www.law.gwu.edu/daniel-justin-solove> [<https://perma.cc/8PDX-TBLR>]. In addition to writing a book, *Hate Crimes in Cyberspace*, and numerous articles on privacy, Professor Citron received a MacArthur "Genius Grant" in 2019. *Danielle K. Citron*, B.U. SCH. L., <https://www.bu.edu/law/profile/danielle-citron> [<https://perma.cc/2RAY-V2VK>].

98. Solove & Citron, *supra* note 1, at 785. Other terms one might expect in a discussion of restitution and unjust enrichment like "disgorgement," "equity," "quasi-contract," and "quantum meruit" are absent as well.

99. See *id.*

100. See, e.g., *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1031 (N.D. Cal. 2012) (explaining that plaintiffs alleged unjust enrichment as their seventh cause of action, and because they did not even address the claim in their opposition to defendant's motion to dismiss, "[c]ourt deem[ed] this claim abandoned").

101. See, e.g., *In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *15 (N.D. Cal. Sept. 20, 2011) (concluding in the last two paragraphs of the decision that there is no cause of action, with plaintiffs apparently conceding that it is only an equitable remedy).

102. See *infra* Section III.D.

103. Scholz, *supra* note 43, at 688.

accountable when they do have such a relationship.¹⁰⁴ But these ideas have not received much traction.

It should come as no surprise that the law has not thought seriously about applying restitution and unjust enrichment to privacy harms. “[R]estitutionary causes of action dropped out of the curriculum of American law schools in the third quarter of the twentieth century”¹⁰⁵ The result is that practicing attorneys do not have a good grasp of restitution and unjust enrichment, and contemporary courts often misapply the doctrine.¹⁰⁶ Moreover, because restitution is deeply intertwined with equity, its scholars tend to be historians looking at how earlier courts addressed issues of that time.¹⁰⁷ In contrast, scholars who study data privacy and cybersecurity tend to be futurists looking at how the law should accommodate emerging technology. While both perspectives are undoubtedly important, it is not surprising that they rarely converge.

Because restitution is largely unfamiliar to modern American lawyers, jurists, and scholars, this Section now introduces some terminology. Unfortunately, even experts disagree about the meaning of some of restitution’s basic terms.¹⁰⁸ Even worse, courts and attorneys regularly confuse the terminology. According to the *Restatement*, “[t]he law of restitution is predominantly the law of unjust enrichment.”¹⁰⁹ The term “restitution” is used to designate both liabilities and remedies in unjust enrichment.¹¹⁰ “The substantive part of . . . restitution is concerned with identifying . . . [what is]

104. See *id.* at 663–81 (discussing restitution and unjust enrichment as applied to third party “data trafficking”).

105. Douglas Laycock, *Restoring Restitution to the Canon*, 110 MICH. L. REV. 929, 930 (2012) [hereinafter Laycock, *Restoring Restitution*].

106. Andrew Kull, *Rationalizing Restitution*, 83 CALIF. L. REV. 1191, 1195 (1995) [hereinafter Kull, *Rationalizing Restitution*] (“To put it bluntly, American lawyers today (judges and law professors included) do not know what restitution is.”); Laycock, *Restoring Restitution*, *supra* note 105, at 930 (“When a lawyer or judge encounters a restitution problem today, there is a substantial risk that she will view it as an isolated problem, only dimly aware that there is a large body of law on restitution and unjust enrichment and that arguments about her particular problem can be tested and refined in light of larger principles.”).

107. That does not mean all of restitution is equitable. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 4 cmt. b (AM. L. INST. 2011) (“The law of restitution is not easily characterized as legal or equitable, because it acquired its modern contours as the result of an explicit amalgamation of rights and remedies drawn from both systems.”).

108. Kull, *Rationalizing Restitution*, *supra* note 106, at 1191–92 (discussing “[t]he linguistic confusion that bedevils the law of restitution”).

109. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 1 cmt. b (AM. L. INST. 2011). But see Douglas Laycock, *The Scope and Significance of Restitution*, 67 TEX. L. REV. 1277, 1279 (1989) [hereinafter Laycock, *Scope and Significance*] (suggesting that law of restitution encompasses both unjust enrichment and specific restitution—the latter referring to remedies that restore something to the plaintiff).

110. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 1 cmt. e (AM. L. INST. 2011).

‘unjust’ for purposes of imposing liability.”¹¹¹ Even though no express or implied-in-fact contract exists, some jurisdictions use the terms “implied contract” or “quasi-contract” to refer to a cause of action based on unjust enrichment.¹¹²

Restitution has a remedial side too. The entire body of restitution encompasses multiple types of remedies including ejectment, replevin, rescission, and reformation.¹¹³ This Article is focused on just one of restitution’s remedies: disgorgement. Some cases refer to this remedy as an “accounting” or “account for profits,” but this Article simply uses the term “disgorgement.”¹¹⁴ A related remedy is a constructive trust, but unlike a constructive trust, disgorgement need not identify a particular asset or fund.¹¹⁵ Disgorgement focuses on taking the wrongdoer’s unjust profits or savings and awarding them to the victim. Although this remedy results in a monetary award, disgorgement is generally not considered a form of damages. That is because “damages” refers to a monetary award that compensates the victim for the harm (i.e., damage) suffered. In short, disgorgement is based on the defendant’s enrichment while damages focus on the plaintiff’s injury.¹¹⁶

The following Sections discuss how the law of restitution and unjust enrichment can be applied to privacy losses while avoiding the many doctrinal pitfalls found in tort, contract, and constitutional standing law.

A. THE DISGORGEMENT REMEDY

The most straightforward application for unjust enrichment for data loss victims occurs when a company makes money it would not have made but for the improper use of the victims’ data. This can occur when a company breaks a promise to keep information private and then sells it or otherwise uses that information for profit.

The legal analysis differs depending on whether the promise is part of the company’s contract with their customers or the promise is made outside of a contract.¹¹⁷ In the former case, unjust enrichment provides a remedy for a breach of contract. In the latter case, unjust enrichment allows for a distinct

111. *Id.* § 1 cmt. b.

112. More specifically, “implied-in-law” meaning “invented.” This conception does not create a valid contract; it leads only to restitution remedies. This is in contrast to implied-in-fact contracts for which the court finds conduct through which it can imply assent, thus finding a valid contract and reaching contract remedies. *See* DAN B. DOBBS & CAPRICE L. ROBERTS, *LAW OF REMEDIES: DAMAGES, EQUITY, RESTITUTION* § 4.2, at 390–92 (3d ed. 2018).

113. *Id.* § 4.2(1), at 389, § 4.3(1), at 398.

114. *RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT* § 51 cmt. a (AM. L. INST. 2011).

115. DOBBS & ROBERTS, *supra* note 112, § 4.3(1), at 398, § 4.3(2), at 399.

116. *See* Laycock, *Restoring Restitution*, *supra* note 105, at 938.

117. This analysis tracks two of three ways that Laycock says modern restitution matters: “when unjust enrichment is the only source of liability,” and “when [the] plaintiff prefers to measure recovery by defendant’s gain.” Laycock, *Scope and Significance*, *supra* note 109, at 1284.

cause of action that is not grounded in contract, tort, or even property law. Section III.A first explains how victims of data losses can sue companies for breaking contractual privacy promises and then use unjust enrichment to obtain a monetary recovery that is based on the company's unjust enrichment as opposed to the plaintiff's own injury. But because not all promises are found in the contract, Section III.B describes how unjust enrichment can also serve as an independent cause of action.¹¹⁸

For data breaches covered under a contractual relationship, a restitution-based disgorgement remedy exists as an alternative to contract law's traditional remedies. The primary remedy for breach of contract is expectation damages.¹¹⁹ In other words, contract law tries to place the successful plaintiff in the position she would have occupied had the promise been fulfilled (i.e., in the absence of a breach). But as discussed earlier, even when a company violates an express provision in their customer contract, contract law often fails data loss victims because the doctrine does not recognize the victims' injuries.

Because unjust enrichment does not focus on the plaintiff's injury but on the defendant's gain, unjust enrichment can step in and provide data loss victims a viable remedy.¹²⁰ Chapter 4 of the *Restatement* is entitled "Restitution and Contract" and sections 37–39 deal explicitly with alternative remedies for breach of contract.¹²¹ Importantly, section 39 entitled "Profit from Opportunistic Breach" allows the plaintiff to recover money based on the defendant's wrongful profits. Section 39(1) provides:

If a deliberate breach of contract results in profit to the defaulting promisor and the available damage remedy affords inadequate protection to the promisee's contractual entitlement, the promisee has a claim to restitution of the profit realized by the promisor as a result of the breach. Restitution by the rule of this section is an alternative to a remedy in damages.¹²²

118. Unjust enrichment can also serve as a remedy for other common law doctrines, and even for statutory violations, making it a suitable remedy for privacy violations that do not just involve broken promises. DOBBS & ROBERTS, *supra* note 112, § 4.1(1), at 370 ("Restitution remedies may flow from a freestanding cause of action based on unjust enrichment or may piggyback on other causes of action such as contracts, torts, fiduciary duties, and intellectual property.")

119. See RESTATEMENT (SECOND) OF CONTS. § 347 cmt. e (AM. L. INST. 1981).

120. See Laycock, *Scope and Significance*, *supra* note 109, at 1285–86 (explaining how restitution can serve as a remedy for substantive causes of action like torts and breaches of contract).

121. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT §§ 37–39 (AM. L. INST. 2011).

122. *Id.* § 39(1).

This type of remedy is disgorgement.¹²³ The comments to section 39 explain the underlying purpose for the recovery of profits “is the reinforcement of an entitlement that would be inadequately protected if liability for interference were limited to provable damages.”¹²⁴ Privacy loss victims are ideal candidates for using section 39. The *Restatement* uses the term “inadequate” to suggest that damages are smaller than they should be to effectuate the purpose of the contract. That certainly applies to privacy loss victims. Their remedies are not merely inadequate; they are nonexistent. Without a stronger alternative remedy, businesses would have no incentive to abide by the privacy promises they make in their customer contracts.¹²⁵

While it is fair to call section 39 a “new rule,” there is precedent supporting the rule.¹²⁶ A number of courts had previously awarded a disgorgement remedy for intentional breach when typical contract damages would leave the plaintiff inadequately protected.¹²⁷ For example, in *May v. Muroff*, the seller of land improperly sold fill from the land before the transaction closed.¹²⁸ The trial court awarded \$122,067 in expectation damages, the difference between the value of the land as promised and as delivered.¹²⁹ But the Florida District Court of Appeal revised the award and ordered disgorgement of the proceeds of sale of the fill, \$240,000.¹³⁰ The court first noted that the breach was “deliberate” and justified the remedy by explaining that the seller “should not be permitted to profit by his own wrong

123. Melvin A. Eisenberg, *The Disgorgement Interest in Contract Law*, 105 MICH. L. REV. 559, 560–61 (2006) [hereinafter Eisenberg, *The Disgorgement Interest*] (explaining that “the disgorgement interest . . . is the promisee’s interest in requiring the promisor to disgorge a gain that was made possible by her breach, but did not consist of a benefit conferred on her by the promisee”); Caprice L. Roberts, *Restitutory Disgorgement for Opportunistic Breach of Contract and Mitigation of Damages*, 42 LOY. L.A. L. REV. 131, 134 (2008) [hereinafter Roberts, *Opportunistic Breach*] (describing disgorgement as “strip[ping] the defendant’s gain”).

124. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 39 cmt. b (AM. L. INST. 2011).

125. Punitive damages would offer an even stronger disincentive. See William S. Dodge, *The Case for Punitive Damages in Contracts*, 48 DUKE L.J. 629, 633 (1999) (arguing for punitive damages in cases of willful and opportunistic breach).

126. Roberts, *Opportunistic Breach*, *supra* note 123, at 140 (saying that section 39 “is an ‘essentially new’ rule, although not without precedent” (quoting RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT, reporter’s introductory memorandum, at xv (AM. L. INST., Tentative Draft No. 4, 2005))). But see Roy Ryden Anderson, *The Compensatory Disgorgement Alternative to Restatement Third’s New Remedy for Breach of Contract*, 68 SMU L. REV. 953, 962 (2015) (pointing out that disgorgement as remedy for breach of contract is not found in the *Restatement (Second) of Contracts*).

127. Marco J. Jimenez, *Retribution in Contract Law*, 52 U.C. DAVIS L. REV. 637, 718–22 (2018) (discussing cases prior to the *Restatement* that provided a disgorgement remedy for opportunistic breach); see also DOBBS & ROBERTS, *supra* note 112, § 4.4(2), at 449 & n.392 (describing more recent cases that allow for disgorgement upon intentional breach of contract).

128. *May v. Muroff*, 483 So. 2d 772, 772 (Fla. Dist. Ct. App. 1986).

129. *Id.*

130. *Id.*

and enjoy a windfall profit.”¹³¹ Thus, the disgorgement remedy allowed the plaintiff to recover more than his expectation damages. This outcome is necessary in disgorgement cases to effectuate the intent of the parties. It is particularly appropriate where the plaintiff would have been able to seek and receive equitable relief such as an injunction or specific performance *if only* the plaintiff had possessed advance notice of the breach.

Admittedly, the idea of awarding a monetary recovery that exceeds the value of the plaintiff’s injury seems antithetical to conventional contract law.¹³² One of the core principles of contract remedies is that it is not punitive except when the breach is also a tort.¹³³ Any damages are simply intended to place the party in the position it expected to be in had there been performance. But the point of providing a disgorgement remedy for intentional breach is entirely consistent with the more fundamental contract law goal of effectuating the parties’ intent. If the conventional contract remedy (i.e., expectation damages) fails to provide an adequate incentive for a party to comply with its promises, restitution needs to step in and provide an alternative remedy that will incentivize the party to comply with its promises. Further, disgorgement is not punitive or at least not disproportionately so.¹³⁴ It only strips that portion of the gain that is wrongful in order to undo the unjust enrichment and deter further opportunism.

Importantly, the term “deliberate” in section 39 has been interpreted to apply to conduct beyond purely intentional breaches.¹³⁵ In *Kansas v. Nebraska*, the U.S. Supreme Court held that deliberate breach also occurs when a party

131. *Id.* (citing *Laurin v. DeCarolis Constr. Co.*, 363 N.E.2d 675 (Mass. 1977)). In *Laurin*, the seller sold loam, gravel, trees, and shrubs from the property prior to closing. *Laurin*, 363 N.E.2d at 676. Like the court in *May*, the Massachusetts Supreme Court awarded the plaintiff the value of the sold items, saying, “where the defendant’s breach is deliberate and wilful, we think damages limited to diminution in value of the premises may sometimes be seriously inadequate.” *Id.* at 678; *see also* *Watson v. Cal-Three, LLC*, 254 P.3d 1189, 1195–97 (Colo. App. 2011) (“If the breaching party’s wrongdoing is intentional or substantial, or there are no other means of measuring the wrongdoer’s enrichment, recovery of the breaching party’s profits may be granted.”).

132. *See* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 39 cmt. a (AM. L. INST. 2011) (“Judged by the usual presumptions of contract law, a recovery for breach that exceeds the plaintiff’s provable damages is anomalous on its face.”).

133. RESTATEMENT (SECOND) OF CONTS. § 355 (AM. L. INST. 1981); E. ALLAN FARNSWORTH, CONTRACTS § 12.8, at 760 (4th ed. 2004) (“No matter how reprehensible the breach, damages are generally limited to those required to compensate the injured party for lost expectation . . .”). *But see* *Jimenez*, *supra* note 127, at 662–714 (arguing that courts already take into account “retributive considerations” as they apply a variety of different contract doctrines).

134. *See* Mark P. Gergen, *Causation in Disgorgement*, 92 B.U. L. REV. 827, 830 (2012) (arguing that courts often “fudge” the causal analysis in disgorgement to arrive at amounts that serve to deter wrongdoing).

135. *See* *Anderson*, *supra* note 126, at 979–80 (criticizing the use of the term “deliberate” in section 39 as confusing, and suggesting that the term was meant “to describe a breach designed to further the self-interest of the breaching party at the other party’s expense”).

exposes the other side to a known risk of breach.¹³⁶ In the underlying dispute, Kansas had filed suit in the U.S. Supreme Court alleging Nebraska had violated a prior settlement agreement, and taken more than its proper share of water from the Republican River.¹³⁷ The Supreme Court appointed a special master who found Nebraska in breach and “award[ed] Kansas \$3.7 million for its loss, and another \$1.8 million in partial disgorgement of Nebraska’s still greater gains.”¹³⁸

Because the special master’s ruling found that Nebraska officials did not “deliberately set out to violate the [settlement],”¹³⁹ Nebraska argued disgorgement was not warranted under section 39(1) of the *Restatement*.¹⁴⁰ In an opinion by Justice Kagan, the Supreme Court took an expansive view of the meaning of “deliberate” saying that in some contexts, “the distinction between purposefully invading and recklessly disregarding another’s rights makes no difference.”¹⁴¹ Since the special master found Nebraska “‘knowingly exposed Kansas to a substantial risk’ of breach, and blithely proceeded,” disgorgement was called for in this case.¹⁴² The Court justified its decision by saying that it “may order disgorgement of gains, if needed to stabilize a compact and deter future breaches, when a State has demonstrated reckless disregard of another, more vulnerable State’s rights under that instrument.”¹⁴³

Kansas v. Nebraska only says what the federal common law is. While there is no general federal common law, federal common law controls certain specialized disputes such as those between co-equal states where neither state’s law can govern.¹⁴⁴ In applying common law contract principles and the disgorgement remedy in *Kansas v. Nebraska*, the Supreme Court created federal common law that is informative but not binding for state courts. Consequently, the various state courts will have to decide whether they are also willing to consider reckless breach to justify disgorgement. Justice Thomas concurring in part and dissenting in part (joined by Justices Scalia and Alito) provides the counterpoint.¹⁴⁵ The dissent first challenged the very

136. *Kansas v. Nebraska*, 135 S. Ct. 1042, 1055–56 (2015).

137. *Id.* at 1048–49. U.S. CONST. art. III, § 2 gives the United States original jurisdiction over suits between states.

138. *Kansas*, 135 S. Ct. at 1051.

139. *Id.* at 1056 (quoting Brief for Nebraska at 16, *Kansas*, 135 S. Ct. 1042 (No. 126)).

140. *Id.*

141. *Id.*; see also *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 756, 767–70 (2011) (finding that willful blindness can satisfy the knowledge requirement in a civil lawsuit for patent infringement by an 8–1 margin).

142. *Kansas*, 135 S. Ct. at 1046 (quoting Report of Special Master at 130, *Kansas*, 135 S. Ct. 1042 (No. 126)).

143. *Id.* at 1057.

144. See *Tex. Indus., Inc. v. Radcliff Materials, Inc.*, 451 U.S. 630, 641 (1981).

145. *Kansas*, 135 S. Ct. at 1064–74 (Thomas, J., concurring in part and dissenting in part). Chief Justice Roberts joined as to Part III of Justice Thomas’ opinion which was concurring in

idea of disgorgement, saying that the Supreme Court “has never before relied on [section] 39 nor adopted its proposed theory of disgorgement. . . . The sheer novelty of this proposed remedy counsels against applying it here.”¹⁴⁶ But even accepting section 39, the dissent pointed out that disgorgement was only available “in cases of *deliberate* breach.”¹⁴⁷ Moreover, Justice Thomas resisted “fashioning a new remedy of disgorgement for reckless breach” saying that “[d]isgorgement is strong medicine,” and should be used “only sparingly.”¹⁴⁸ Both the majority and minority’s views of disgorgement in *Kansas v. Nebraska* will undoubtedly be influential as states decide whether section 39 is consistent with their views on unjust enrichment.

This Article sides with the majority view, in part because it is the only way to provide an entire category of deserving plaintiffs with a remedy. While *Kansas v. Nebraska* appears to break new ground, applying disgorgement to reckless breach is entirely consistent with the purposes underlying the *Restatement*. Section 39 is titled “Profit from Opportunistic Breach,” and that term is intended to capture the situation where the breaching party can ignore her contractual obligation because the conventional remedy is inadequate.¹⁴⁹ In so doing, the breaching party can obtain more than what she bargained for. That rationale makes equal sense for intentional breaches or reckless breaches. If conventional contract remedies are deemed inadequate to protect against intentional breaches, those same remedies are also inadequate to deter companies from recklessly ignoring their contractual obligations.

Whether disgorgement can apply in cases of “reckless breach of contract” is particularly important in the data security context. When customers lose their data in cyberattacks, most companies will be able to say they did not intentionally breach promises to provide reasonable data security. But these victims will often be able to show that particular companies recklessly broke these promises. If the state courts follow *Kansas v. Nebraska*, these companies will have to take their data security promises more seriously.

Importantly, the concept of awarding damages that exceed the plaintiff’s injuries is generally inconsistent with the idea of “efficient breach.”¹⁵⁰ This

part and dissenting part, but not Part II which dealt with the disgorgement analysis. *Id.* at 1064 (Roberts, C.J., concurring in part and dissenting in part).

146. *Id.* at 1068–69 (Thomas, J., concurring in part and dissenting in part).

147. *Id.* at 1069.

148. *Id.* at 1069–70 (quoting *Missouri v. Jenkins*, 515 U.S. 70, 131 (1995) (Thomas, J., concurring)).

149. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 39 cmt. b (AM. L. INST. 2011) (“The common rationale of every instance in which restitution allows a recovery of profits from wrongdoing, in the contractual context or any other, is the reinforcement of an entitlement that would be inadequately protected if liability for interference were limited to provable damages.”).

150. Caprice L. Roberts, *Restitutory Disgorgement as a Moral Compass for Breach of Contract*, 77 U. CIN. L. REV. 991, 1009 (2009).

theory suggests breach may sometimes be desirable in cases where the promisor's gain from the breach exceeds the promisee's loss.¹⁵¹ However, if the promisor must disgorge her profits upon a breach, there would be no incentive to breach regardless of how efficient it might be. The *Restatement* recognized this tension and expressly rejected the idea of efficient breach.¹⁵²

The *Restatement's* justifications align with some of the prominent critiques of efficient breach. These critiques are grounded in both efficiency and the general concept of good faith. To start, efficient breach incorrectly assumes: (1) that a promisee is "indifferent between performance and damages," and (2) that "the promisor knows the value" of performance to the promisee.¹⁵³ These issues are particularly salient for victims of data losses. First, since these victims often cannot recover any damages, they are not indifferent between performance and damages. They undoubtedly prefer performance. Second, since the companies are unlikely to have to pay any compensatory damages for their breach, companies may view the value of performance to the promisee as zero. This would be true even in cases where customers care deeply about keeping their data private. Thus, efficient breach would suggest that companies should breach their privacy promises whenever they can derive any non-zero value from their customers' data. But the law should not allow companies to ignore their privacy promises in this way. This is precisely the kind of situation the law of unjust enrichment governs. By forcing companies to disgorge any resulting profits, section 39 provides real disincentives to breaking privacy promises.

But even if we assume that a particular breach could make the promisor better off without harming the promisee, the *Restatement* favors a negotiated release.¹⁵⁴ This approach is arguably more efficient, fair, and consistent with notions of good faith. It is more efficient because a negotiated release will take into account a "richer mix of information."¹⁵⁵ This is because any

151. RICHARD A. POSNER, *ECONOMIC ANALYSIS OF LAW* § 4.10, at 129 (9th ed. 2014). Although Posner is well known for advocating efficient breach, he does not apply that theory to opportunistic breach. There he says, "[w]e can deter A's opportunistic behavior by making it worthless to him, which can be done by making him hand over all his profits from the breach to the promisee. No lighter sanction would deter." *Id.*

152. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 39 cmt. h (AM. L. INST. 2011) ("The rationale of the disgorgement liability in restitution, in a contractual context or any other, is inherently at odds with the idea of efficient breach in its usual connotation.").

153. Melvin A. Eisenberg, *Actual and Virtual Specific Performance, the Theory of Efficient Breach, and the Indifference Principle in Contract Law*, 93 CALIF. L. REV. 975, 998 (2005) [hereinafter Eisenberg, *Actual and Virtual Specific Performance*]; *id.* at 999-1003; *see also* Andrew Kull, *Disgorgement for Breach, the "Restitution Interest," and the Restatement of Contracts*, 79 TEX. L. REV. 2021, 2051 (2001) [hereinafter Kull, *Disgorgement for Breach*] (pointing out that efficient breach ignores litigation costs).

154. *See* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 39 cmt. h (AM. L. INST. 2011) ("A voluntary transaction in the present context requires a negotiated release or modification of the existing obligation.").

155. Eisenberg, *Actual and Virtual Specific Performance*, *supra* note 153, at 1001.

negotiation is more likely to account for how both parties value performance. A negotiated release is also fairer because the parties could split any surplus. Finally, a negotiated release is more consistent with notions of good faith because it does not reward intentional breaches.¹⁵⁶ By allowing for disgorgement of a breaching party's profits, the *Restatement* is clearly siding against the idea of efficient breach.¹⁵⁷

The *Restatement's* view on negotiated release should be less controversial in privacy law than in other contexts. In privacy law, the FTC already views the failure to disclose changes to a privacy policy as an unfair trade practice.¹⁵⁸ It has brought enforcement actions against companies that have tried to retroactively change their privacy policies.¹⁵⁹ Thus, at least with respect to privacy law, the *Restatement* simply requires the same standards of conduct already imposed by the FTC and other state unfair trade practice statutes.

One potential advantage of the disgorgement remedy is that it may be more palatable to critics of class actions lawsuits. One common argument is that class action damage awards are disproportionate to the underlying wrongdoing.¹⁶⁰ However, by only taking the defendant's wrongful gains (or savings), the disgorgement remedy simply places the defendant in the same state it would have occupied had it not committed the offense. Companies also have the ability to seek offsets to disgorgement awards based upon gains that are not attributable to the wrong (in other words, independently earned by the companies' efforts without use of consumers' data).¹⁶¹ In contrast, punitive damages typically make the defendant worse off. The same is often true for statutory damages which are not based on either the defendant's gain

156. See Kull, *Disgorgement for Breach*, *supra* note 153, at 2051 (describing efficient breach as "a conscious decision to give the plaintiff less than what was promised").

157. *Id.* at 2050 ("The law of unjust enrichment condemns [efficient breach] and seeks to frustrate it by imposing a remedy—disgorgement of profits—that forecloses any possibility that the defendant could respond in damages to the plaintiff and still come out ahead.").

158. Solove & Hartzog, *supra* note 38, at 640 ("According to the FTC, it is unfair to change the terms that govern personal information that was collected under a previous, different agreement.").

159. *In re Gateway Learning Corp.*, 138 F.T.C. 443, 449 (2004) ("Respondent's retroactive application of its revised privacy policy . . . was, and is, an unfair act or practice."); Complaint at 9, *In re Facebook, Inc.*, No. C-4365, 2012 WL 3518628, at *6 (F.T.C. July 27, 2012) (alleging that the retroactive change of a material privacy promise constituted an unfair act or practice).

160. See *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 368 (M.D. Pa. 2015) ("[F]or a court to require companies to pay damages to thousands of customers, when there is yet to be a single case of identity theft proven, strikes us as overzealous and unduly burdensome to businesses."); Sheila B. Scheuerman, *Due Process Forgotten: The Problem of Statutory Damages and Class Actions*, 74 MO. L. REV. 103, 115 (2009) (discussing the problem of excessive statutory damages in class action suits).

161. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 51 (AM. L. INST. 2011).

or the plaintiff's actual loss.¹⁶² Of course, given that most privacy wrongs will likely go undetected, disgorgement may not serve as a complete deterrent.¹⁶³ Still, it will provide some measure of compensation to privacy victims. In short, disgorgement occupies a middle ground.¹⁶⁴ It provides a larger award and a more secure route than more commonly used claims, although it certainly provides less of a stick than punitive or statutory damages.

1. Privacy Promises "Unrelated to Profit"

Even though privacy loss victims appear to fit squarely within section 39, judges may be reluctant to allow a disgorgement remedy because of their unfamiliarity with both restitution law and privacy harms. Accordingly, the next two Sections illustrate how different kinds of privacy losses fit squarely within the classic disgorgement cases.

Melvin Eisenberg has cataloged the various types of cases in which disgorgement should be used.¹⁶⁵ He labels one of these categories, "Bargains Designed to Serve Interests Other Than Profit-making."¹⁶⁶ For privacy victims whose data have been sold or used in breach of a privacy promise, these cases can serve as a model for asking courts to disgorge a company's unjust profits.

For contracts that include promises made for reasons other than profit, expectation damages are often inadequate because the primary purpose of the promise is unrelated to money. Thus, expectation damages will not provide the promisee with what she actually contracted for. Moreover, for some situations, the law will not be able to place a value on the expectation interest. Thus, the "best and perhaps only way" to effectively police these promises is through disgorgement.¹⁶⁷

An important example of this kind of bargain is found in the well-known case of *Snepp v. United States*.¹⁶⁸ As an employee of the Central Intelligence Agency ("CIA"), Snepp had signed an employment agreement promising he would not publish any information or material relating to his employment

162. See *Parker v. Time Warner Ent. Co.*, 331 F.3d 13, 21–22 (2d Cir. 2003) (noting that statutory damages in class actions can cause the potential liability to be grossly disproportionate to the actual harm from the violation).

163. See William T. Allen, *Commentary on the Limits of Compensation and Deterrence in Legal Remedies*, 60 LAW & CONTEMP. PROBS., Autumn 1997, at 67, 72 (explaining why a compensation-based remedy will under-deter wrongs when there are undetected violations).

164. See DOUG RENDLEMAN & CAPRICE L. ROBERTS, *REMEDIES: CASES AND MATERIALS* 542 (9th ed. 2018); Daniel Friedmann, *Restitution of Benefits Obtained Through the Appropriation of Property or the Commission of a Wrong*, 80 COLUM. L. REV. 504, 552 (1980) (describing disgorgement as less harsh than punitive damages); see also *Snepp v. United States*, 444 U.S. 507, 515–16 (1980) (per curiam) (preferring the disgorgement remedy over exemplary damages because it deals fairly with both parties).

165. Eisenberg, *The Disgorgement Interest*, *supra* note 123, at 581–97.

166. *Id.* at 588.

167. *Id.* at 591.

168. *Snepp*, 444 U.S. at 507.

without specific prior approval.¹⁶⁹ He breached the agreement by publishing a book about the CIA's activities during the end of the Vietnam War without prior approval.¹⁷⁰ However, the book contained no classified information.¹⁷¹

The Supreme Court was asked to decide the appropriateness of the remedy.¹⁷² Clearly, the purpose of the clearance requirement was about national security, not profit.¹⁷³ The injury had nothing to do with how much money the government expected. The government had no financial interest in the book. Rather, the undisputed testimony was that the breach "seriously impaired the effectiveness of American intelligence operations."¹⁷⁴ The Supreme Court noted that "actual damages . . . are unquantifiable."¹⁷⁵ The only way to protect the CIA's interest was to punish Snepp or somehow take away incentives for future breaches. The Court rejected the first tactic, saying punitive damages were both "speculative and unusual."¹⁷⁶ Instead, the Supreme Court affirmed the district court's decision to impose a constructive trust on Snepp's profit.¹⁷⁷ The Court believed that this remedy dealt "fairly with both parties" saying that the remedy simply required Snepp "to disgorge the benefits of his faithlessness."¹⁷⁸ At the same time, the Court noted that the remedy avoided punitive damages that may be disproportionate to Snepp's gain.¹⁷⁹

Contracts that include promises to keep information private have clear parallels to the contract in *Snepp*. Like the U.S. government in *Snepp*, consumers do not expect that promises to keep their information private will benefit them financially. Rather, these individuals are simply asked to be left alone. Conventional contract remedies are inadequate to protect these privacy promises because courts refuse to recognize the loss of personal information as a compensable injury. Finally, specific performance is unhelpful because the contract has been breached and there is no way to put the proverbial cat back in the bag. Accordingly, the best and perhaps only way to incentivize companies to respect privacy promises is to insist that they

169. *Id.* at 507–08.

170. *Id.*

171. *Id.* at 510.

172. *Id.* at 507.

173. *See id.* at 514–16.

174. *Id.* at 512.

175. *Id.* at 514.

176. *Id.* The general rule is that punitive damages cannot be awarded in contract cases. DOUGLAS LAYCOCK & RICHARD L. HASEN, MODERN AMERICAN REMEDIES: CASES AND MATERIALS 260 (5th ed. 2019).

177. *Snepp*, 444 U.S. at 515–16; *see also* Att'y Gen. v. Blake [2000] UKHL 45, [2001] 1 AC (HL) 268 (appeal taken from Eng.) (using similar analysis, the House of Lords in England also awarded disgorgement when their own former intelligence operative published a book without clearance).

178. *Snepp*, 444 U.S. at 515.

179. *Id.* at 515–16.

disgorge their profits if they impermissibly sell or otherwise profit from the data.

2. Data Security Promises as “Skimped Services”

For privacy victims who have lost their personal data because a company failed to take reasonable data security measures, another category of cases called “skimped services” can serve as a model for asking for a company’s unjust savings. In these cases, the unjust savings would be the money the company should have spent if it had actually delivered on its promise of adequate cybersecurity. Commentators generally agree that disgorgement is appropriate where the wrong is based on a skimmed service.¹⁸⁰ In these cases, the contract typically requires the promisor to provide a specific service or good. The promisor either fails to perform entirely or underperforms.

Andrew Kull, the Reporter for the *Restatement*, has cataloged the paradigmatic skimmed service cases.¹⁸¹ A shortened list includes: the mining company that failed to restore the land after extracting coal;¹⁸² the firefighting company that failed to keep the required number of firemen ready;¹⁸³ and Coca-Cola, which substituted high fructose corn syrup for cane sugar.¹⁸⁴ In each case, expectation damages would have resulted in either under compensation or no compensation. For the landowner, the diminution in value of the unrestored land after mining was minimal.¹⁸⁵ The City of New Orleans was undamaged because the smaller number of firefighters were able to adequately handle the fires during the term of the contract.¹⁸⁶ For the bottlers who sued Coca-Cola, the customers apparently did not care if cane sugar or corn syrup was used.¹⁸⁷ So there were no actual damages. However, the breach in each of these cases can be labelled as opportunistic, and the defendants were all unjustly enriched. Under section 39 of the *Restatement*, disgorgement would apply in all of these situations.

180. See Eisenberg, *The Disgorgement Interest*, *supra* note 123, at 592–93 (explaining why disgorgement is appropriate in “skimped-services cases”); Kull, *Disgorgement for Breach*, *supra* note 153, at 2047; E. Allan Farnsworth, *Your Loss or My Gain? The Dilemma of the Disgorgement Principle in Breach of Contract*, 94 YALE L.J. 1339, 1384–86 (1985) (describing why disgorgement is appropriate where there has been an “abuse of contract”).

181. Kull, *Disgorgement for Breach*, *supra* note 153, at 2047.

182. *Peevyhouse v. Garland Coal & Mining Co.*, 382 P.2d 109, 111 (Okla. 1962).

183. *City of New Orleans v. Firemen’s Charitable Ass’n*, 9 So. 486, 487 (La. 1891) (finding the contract required the defendant to employ 124 firefighters, but it retained no more than 70).

184. *Coca-Cola Bottling Co. of Elizabethtown, Inc. v. Coca-Cola Co.*, 988 F.2d 386, 409 (3d Cir. 1993).

185. Moreover, the plaintiffs were not permitted to recover the cost of performance because the Supreme Court of Oklahoma viewed that remedy as “grossly disproportionate” to the economic value of that work. *Peevyhouse*, 382 P.2d at 114.

186. *City of New Orleans*, 9 So. at 488.

187. *Coca-Cola*, 988 F.2d at 408.

The justification for applying disgorgement to skimmed service cases is that the rule would make it more likely parties would abide by their contractual promises. The problem in cases of skimmed services is that “[e]xpectation damages give the promisor insufficient incentives to perform.”¹⁸⁸ Providing a disgorgement remedy serves “to deter a form of conscious wrongdoing that encounters no adequate disincentive.”¹⁸⁹ Allan Farnsworth, a Reporter for the *Restatement (Second) of Contracts*, has one of the narrower views of disgorgement in contract cases, but even he suggests that disgorgement is appropriate when the plaintiff has no other adequate remedy.¹⁹⁰

Notably, the skimmed services cases illustrate how disgorgement is not limited to the recovery of profits earned, but also “savings made.” In these cases, disgorgement awards the difference between how much money the defendant actually spent and the amount it should have spent if it had not “skimmed” on its promise. That is the amount of money the fire department saved by providing fewer firefighters. This is fully consistent with how the *Restatement* views disgorgement. Section 39 states that “[p]rofits from breach include saved expenditure.”¹⁹¹ This type of recovery is important for victims who lost their data from third party cyberattacks. Unlike cases where victims’ data was taken by the company and impermissibly sold or used, here there are no profits to disgorge. Victims of data breaches will have to seek savings that represent the difference between the money the company actually spent on data security and the amount the company should have spent.

Of course, all the justifications for using disgorgement in skimmed services cases apply with equal force to companies that promise reasonable data security and then fail to deliver. In the typical data breach case, personal information from millions of customers has been taken. There is undoubtedly real injury. The courts simply refuse to place a dollar value on that injury. Disgorgement may make even more sense in data breach cases than in many other skimmed service cases that at least provide the aggrieved party with some damages. Absent disgorgement, victims of data loss often would continue to receive nothing.

For some courts and policymakers, applying disgorgement to inadequate cybersecurity may swing the balance of power too far in favor of customers. That is because disgorgement does not only apply when damages are hard to

188. Eisenberg, *The Disgorgement Interest*, *supra* note 123, at 593.

189. Kull, *Disgorgement for Breach*, *supra* note 153, at 2049.

190. Farnsworth would limit disgorgement in contract law to those situations to what he calls an “abuse of contract.” The following example illustrates the concept: “If I realize a gain as a result of my breach of contract, there has been an abuse of that contract if you, the injured party, are left with a defective performance and no opportunity to use your return performance to attempt to obtain a substitute.” Farnsworth, *supra* note 180, at 1384.

191. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 39(3) (AM. L. INST. 2011).

measure; it even applies in the absence of any injury.¹⁹² For data security cases, that means disgorgement can come into play even if there has not been a successful cyberattack. In other words, the predicate for the unjust enrichment claim is not losing customer data, it is unjustly skimping on data security services. While suits that do not involve successful cyberattacks are theoretically possible, in practice, they are unlikely to occur. That is because customers typically learn about company's poor data security practices only after a breach has occurred.

A critique of my argument is that the common law support for applying disgorgement to skimmed service cases is not nearly as settled as the theoretical support. For many of the paradigmatic cases, the defendants were not actually required to disgorge their gains.¹⁹³ That may be because neither the plaintiffs nor the court considered the remedy, as appears to be the case in *Peevyhouse*.¹⁹⁴ Or it might be because the plaintiffs abandoned the unjust enrichment theory after trial as happened in the dispute over the sweetener in *Coca-Cola*.¹⁹⁵ Moreover, in *New Orleans v. Firemen's Charitable Association*, the court rejected the city's attempt to get any damages because there was no actual injury.¹⁹⁶ But these critiques are directed to section 39 of the *Restatement* as a whole. If a jurisdiction accepts section 39, the idea of applying disgorgement to broken privacy promises should be uncontroversial.

One might also question whether courts are really equipped to determine whether companies have broken their cybersecurity promises and failed to provide "adequate" or "reasonable" data security. William McGeeveran has already done much of the work here. He describes "fourteen different 'frameworks' that impose data security obligations on private companies" and shows how they are "converging on a common set of standards."¹⁹⁷ In short, the United States has already developed a common understanding of which practices do or do not constitute reasonable data security. Courts should be

192. See *supra* text accompanying notes 186–87 (discussing how in both the cases of hiring fewer firefighters than contracted and substituting corn syrup for cane sugar, there were no allegations of actual injury).

193. Anderson, *supra* note 126, at 996 (pointing out that many of the skimmed service cases underlying various *Restatement* examples did not actually apply a disgorgement remedy, and arguing that contract law can provide an adequate remedy by taking approaches that are not based purely on expectancy damages).

194. The decision does not mention restitution, unjust enrichment, or disgorgement, but Farnsworth and Judith Maute separately explain how the court could have used disgorgement to prevent Garland Coal from being unjustly enriched by its breach. Farnsworth, *supra* note 180, at 1384–89; Judith L. Maute, *Peevyhouse v. Garland Coal & Mining Co. Revisited: The Ballad of Willie and Lucille*, 89 NW. U. L. REV. 1341, 1442–43 (1995).

195. *Coca-Cola Bottling Co. of Elizabethtown, Inc. v. Coca-Cola Co.*, 988 F.2d 386, 408–09 (3d Cir. 1993).

196. *City of New Orleans v. Firemen's Charitable Ass'n*, 9 So. 486, 488 (La. 1891) (denying New Orleans any recovery because there were no allegations of "any damage suffered by the city in consequence of any violation of the contract").

197. William McGeeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1139 (2019).

able to apply these standards to determine whether companies are violating them. After all, judges and juries are regularly asked to apply reasonableness standards in a variety of other contexts, most notably for negligence torts.¹⁹⁸ Those cases often involve complex technical issues like whether a particular safety precaution is reasonable. Yet, the law does not hesitate to ask our judicial system to make these decisions. The law should treat decisions on data security similarly.¹⁹⁹

Finally, I should note that a few courts have allowed privacy victims to proceed on a claim of unjust enrichment (as a cause of action).²⁰⁰ For example, in *Resnick v. AvMed, Inc.*, two laptops were stolen from the offices of AvMed, a health care service provider.²⁰¹ “The unencrypted laptops contained the sensitive information of approximately 1.2 million current and former AvMed members.”²⁰² The Eleventh Circuit denied the defendant’s motion to dismiss and allowed the plaintiffs to attempt to recover a portion of their monthly premiums on a theory of unjust enrichment.²⁰³ Beyond demonstrating that privacy claims do not have to base their demands on the victims’ injuries, *Resnick* also demonstrates how unjust enrichment does not suffer the causation problems that plague other causes of action. The Eleventh Circuit specifically noted that “[p]laintiffs’ unjust enrichment claim does not have a causation element.”²⁰⁴ Thus, plaintiffs would not have to show the thieves used the information on the laptops to harm the victims. To be clear, unjust enrichment does not receive much attention in any of these cases. The claims tend to be alleged as one of the later causes of action in the complaints, and judicial decisions do not spend much time on these claims. But because unjust enrichment does not suffer from many of the doctrinal problems of traditional claims, privacy victims may wish to privilege these claims.

B. MISUNDERSTANDING CONTRACTUAL PREEMPTION

Modern courts often do not understand the relationship between unjust enrichment and contract law. Unfortunately, this misunderstanding can

198. *Id.* at 1196 (discussing reasonableness standards as “among the oldest cornerstones of law”).

199. This Article does not take a position on whether disgorgement is an issue for the judge or jury, an issue that “remains unresolved in American law.” Caprice L. Roberts, *Disgorging Emoluments*, 103 MARQ. L. REV. 1, 25 (2019) [hereinafter Roberts, *Disgorging Emoluments*] (providing a discussion of the law–equity classification).

200. *See In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 803 (N.D. Cal. 2019) (“[E]ven if the plaintiffs suffered no economic loss from the disclosure of their information, they may proceed at this stage on a claim for unjust enrichment to recover the gains that Facebook realized from its allegedly improper conduct.”); *Enslin v. Coca-Cola Co.*, 136 F. Supp. 3d 654, 678 (E.D. Pa. 2015) (denying motion to dismiss unjust enrichment claim), *aff’d*, 739 F. App’x 91 (3d Cir. 2018).

201. *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1322 (11th Cir. 2012).

202. *Id.*

203. *Id.* at 1328.

204. *Id.*

frustrate data loss victims' ability to bring unjust enrichment claims. Some courts mistakenly believe that a claim for unjust enrichment is preempted by the mere existence of a contract that touches upon the subject matter in dispute. Just rereading the decisions discussed earlier in this Article shows unjust enrichment can be found between contracting parties.²⁰⁵ Thus, the view that unjust enrichment is incompatible with the existence of a contract cannot be accurate.

It is not the "existence" of a contract that eliminates the right to unjust enrichment; that right is only supplanted when the parties decide that they do not want their relationship governed by unjust enrichment and express that decision in their contract. In other words, the availability of unjust enrichment is no different than many other default rules.²⁰⁶ The default rule applies unless the parties have bargained around it.²⁰⁷ For example, parties can agree to forgo their right to go to court, and instead resolve their disputes through binding arbitration. They can disclaim warranties, and they can limit consequential damages. Unjust enrichment is no different. Contracts can affirm, modify, or disclaim the rights and remedies that unjust enrichment would normally provide.²⁰⁸

Nevertheless, many courts remain confused about the relationship between contracts and unjust enrichment. For example, in *TruGreen Cos. v. Mower Bros.*, the Utah Supreme Court said that restitution is limited to cases where "no express contract is present."²⁰⁹ Courts from other jurisdictions have used similar language.²¹⁰ In New York, one decision stated, "[t]he existence of an express agreement . . . governing a particular subject matter precludes

205. This Article has already discussed many cases that applied unjust enrichment when the parties had a contract. *See, e.g., supra* Section III.A (discussing *May v. Muroff*, *Kansas v. Nebraska* (the states had entered into a "compact" which is essentially a contract), and *Snepp v. United States*).

206. By describing unjust enrichment as a default rule, I do not mean to suggest that it is the preferred remedy for breach of contract. Rather, I use the term "default rule" to suggest that unjust enrichment is generally available as an alternative remedy when circumstances call for it.

207. *See* Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 *YALE L.J.* 87, 87 (1989) ("Default rules fill the gaps in incomplete contracts; they govern unless the parties contract around them.").

208. Section 2 of the *Restatement (Third) of Restitution and Unjust Enrichment* says that, "[a] valid contract defines the obligations of the parties as to matters within its scope, displacing to that extent any inquiry into unjust enrichment." *RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT* § 2(2) (AM. L. INST. 2011).

209. *TruGreen Cos. v. Mower Bros.*, 199 P.3d 929, 933 (Utah 2008) (referring to unjust enrichment as restitution).

210. *See, e.g.,* *Ovation Toys Co. v. Only Hearts Club*, No. 2:14-cv-01711-R, 2015 WL 13439771, at *2 (C.D. Cal. Feb. 4, 2015) ("Plaintiff's claim for unjust enrichment fails as a matter of law because it is not a recognized cause of action in California, particularly when a plaintiff alleges an express contract."), *aff'd in part, vacated in part, rev'd in part*, 675 F. App'x 721 (9th Cir. 2017); *Doss v. Homecomings Fin. Network, Inc.*, 210 S.W.3d 706, 709 n.4 (Tex. App. 2006) (applying unjust enrichment "to disputes where there is no actual contract").

recovery in quasi contract for events arising out of the same subject matter.”²¹¹ The *Restatement* criticized these sweeping statements, saying, “[j]udicial statements to the effect that ‘there can be no unjust enrichment in contract cases’ can be misleading if taken casually.”²¹² But this view persists in several jurisdictions and can thwart the ability of data loss victims to request disgorgement.

Consider *In re Anthem, Inc. Data Breach Litigation*, which concerned a cyberattack on a health insurance company’s database.²¹³ The hackers obtained personal information on as many as 80 million Anthem customers and employees.²¹⁴ The information included names, Social Security numbers, birthdays, home addresses, email addresses, and employment information.²¹⁵ Anthem had several privacy policies that made various representations about the data security precautions the company took.²¹⁶ The plaintiffs alleged Anthem broke these promises and asserted breach of contract and unjust enrichment as well as other causes of action.²¹⁷ The court rejected the breach of contract claims, saying the plaintiffs failed to show the privacy policies were part of the plaintiffs’ contract with Anthem.²¹⁸ It then proceeded to reject the unjust enrichment claims, saying that the plaintiffs were “barred from bringing unjust enrichment claims” where there is a valid and enforceable agreement “which . . . covers the dispute between the parties.”²¹⁹ Thus, even though the privacy policies were not considered part of the contract, the mere existence of a contract was sufficient to deny claims based on promises made outside the contract.²²⁰ This view turns the concept of bargaining around a default rule on its head. When parties fail to bargain around a default rule, the default rules are still preempted.

211. *Morales v. Grand Cru Assocs.*, 759 N.Y.S.2d 890, 890 (App. Div. 2003); *see also* *D’Amato v. Five Star Reporting, Inc.*, 80 F. Supp. 3d 395, 421 (E.D.N.Y. 2015) (explaining *quantum meruit* and unjust enrichment “generally exist only where there is no express agreement between the parties”).

212. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 2 cmt. c (AM. L. INST. 2011).

213. *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 967 (N.D. Cal. 2016).

214. *Id.*; Reed Abelson & Matthew Goldstein, *Millions of Anthem Customers Targeted in Cyberattack*, N.Y. TIMES (Feb. 5, 2015), <https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html> [<https://perma.cc/WRH9-JZGT>].

215. *In re Anthem*, 162 F. Supp. 3d at 966.

216. *Id.* at 979–80.

217. *Id.* at 968–70. Apparently, the plaintiffs did not bring a claim under California law, presumably because for a while California did not recognize unjust enrichment as a separate cause of action. *See infra* note 249 and accompanying text.

218. *In re Anthem*, 162 F. Supp. 3d at 980, 983 (addressing the California and New Jersey breach of contract claims).

219. *Id.* at 984 (emphasis omitted) (quoting *Clark–Fitzpatrick, Inc. v. Long Island R.R. Co.*, 516 N.E.2d 190, 193 (N.Y. 1987)).

220. *See id.* at 983–84.

The problem is that decisions like *In re Anthem* often take a nuanced rule that allows parties to opt out of unjust enrichment and misinterpret that rule to say contracts broadly supplant unjust enrichment.²²¹ *In re Anthem* relied on *Clark-Fitzpatrick, Inc. v. Long Island Rail Road Co.* for its view of New York law.²²² But *Clark-Fitzpatrick* provided a far more accurate interpretation of that rule than *In re Anthem*. The relevant passage states: “It is impermissible, however, to seek damages in an action sounding in quasi contract where the suing party has fully performed on a valid written agreement, the existence of which is undisputed, and the scope of which clearly covers the dispute between the parties.”²²³

Contrary to the view in *In re Anthem*, this passage does not mean that the existence of a contract and unjust enrichment are “mutually exclusive.”²²⁴ *Clark-Fitzpatrick* expressly states that preemption only occurs when the contract “clearly covers the dispute between the parties.”²²⁵ Indeed, unjust enrichment has been a remedy for breach of contract in New York at least since the time of Judge Cardozo.²²⁶

That means unjust enrichment is only unavailable for some subset of cases where the parties have contracts. *Joseph Sternberg, Inc. v. Walber 36th Street Assocs.* relied on the same passage from *Clark-Fitzpatrick* but used the language to show the difference between a contract that preempts unjust enrichment and one that does not.²²⁷ In this case, the plaintiff, a broker representing a buyer, negotiated a real estate purchase for \$11.5 million.²²⁸ The contract specified his commission would be \$450,000.²²⁹ However, the buyer and seller concluded the negotiations without the broker and arrived at a lower price of \$10.6 million.²³⁰ The broker did not receive any commission, and he sued for breach of contract, unjust enrichment, and fraud.²³¹ The

221. See, e.g., Doug Rendleman, *Measurement of Restitution: Coordinating Restitution with Compensatory Damages and Punitive Damages*, 68 WASH. & LEE L. REV. 973, 988 (2011) (commenting on *TruGreen*, Rendleman says, “The Utah court’s palpable misunderstanding of restitution is illustrated by its misstatements . . . that restitution is used when the parties have no express contract, which is only sometimes true.”).

222. *In re Anthem*, 162 F. Supp. 3d at 984.

223. *Clark-Fitzpatrick*, 516 N.E.2d at 193.

224. *Joseph Sternberg, Inc. v. Walber 36th St. Assocs.*, 594 N.Y.S.2d 144, 145 (App. Div. 1993).

225. *Clark-Fitzpatrick*, 516 N.E.2d at 193.

226. Joseph M. Perillo, *Restitution in a Contractual Context*, 73 COLUM. L. REV. 1208, 1214–17 (1973) (analyzing Judge Cardozo’s opinion in *Buccini v. Paterno Construction Co.*, 170 N.E. 910 (N.Y. 1930), and showing that unjust enrichment has been a contractual remedy in New York for almost a century).

227. *Joseph Sternberg, Inc.*, 594 N.Y.S.2d at 145.

228. *Id.*

229. *Id.*

230. *Id.*

231. *Id.*

court held that the existence of the contract did not bar the quasi-contract claim, saying:

[I]f the brokerage agreement at issue had explicitly stated that, in the event the sale did not proceed at the agreed price, plaintiff would not be entitled to any commission, it would be indisputable that nothing short of a sale at that price would entitle plaintiff to a commission. The contract, however, does not so state and is silent as to the plaintiff's entitlement to a commission in the event a sale occurred for a lesser price.²³²

Properly understood, unjust enrichment is only preempted when the contract clearly demonstrates that the parties have bargained around it. Of course, the flip side of this result is that unjust enrichment can be bargained around. Unequal bargaining power may limit the ability of unjust enrichment to help privacy victims.²³³ In Part IV, this Article delves further into this issue.

C. THE UNJUST ENRICHMENT CAUSE OF ACTION

The preceding Section described how unjust enrichment can serve as a remedy in breach of contract actions. But as discussed earlier, privacy policies are not always considered part of the contract between the business and its customers.²³⁴ Indeed, companies often make representations that may not be considered part of customer contracts. These promises may be found in a privacy policy on the company's website or in a letter to customers as the company changes its privacy policy.²³⁵

Importantly, victims of data losses can resort to unjust enrichment even if the broken promise is not part of a contract. Unjust enrichment is not just a remedy; it can serve as its own cause of action.²³⁶ For example, in *Blue Cross*

232. *Id.* at 146.

233. *See infra* Section IV.B.

234. *See supra* notes 22–23 and accompanying text (identifying cases where privacy policies were not contractual obligations).

235. *See, e.g., Privacy Policy*, GOOGLE (Sept. 30, 2020), <https://policies.google.com/privacy?hl=en-US> [<https://perma.cc/MES3-RU8Y>]; *In re: WhatsApp*, ELEC. PRIV. INFO. CTR., <https://epic.org/privacy/internet/ftc/whatsapp/#transfer> [<https://perma.cc/DWX2-KDUQ>] (discussing WhatsApp's blog post announcing to customers it would share their data with Facebook); *A Message to Our Customers*, APPLE (Feb. 16, 2016), <https://www.apple.com/customer-letter> [<https://perma.cc/7P28-G7U3>] (discussing Apple's privacy promises to customers and refusal to provide personal data to government).

236. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 1 cmt. a (AM. L. INST. 2011) (explaining how unjust enrichment is “an independent basis of liability” which has been “carried forward” from the 1937 *Restatement of Restitution*); LAYCOCK & HASEN, *supra* note 176, at 644 (“Just as there are rules that impose liability in tort and contract, there are rules that impose liability in unjust enrichment.”); Colleen P. Murphy, *Misclassifying Monetary Restitution*, 55 SMU L. REV. 1577, 1582 (2002) (“Restitution as a basis of liability parallel to contract and tort has been called ‘freestanding’ restitution” (quoting Doug Rendleman, *Common Law Restitution in the Mississippi Tobacco Settlement: Did the Smoke Get in Their Eyes?*, 33 GA. L. REV. 847, 886 (1999))).

Health Services, Inc. v. Sauer, the Missouri Court of Appeals awarded a money judgement to an insurance company that had mistakenly paid benefits to the defendant after his policy had terminated.²³⁷ The defendant had not breached a contract nor committed a tort; rather, Blue Cross was able to recover because the defendant was “unjustly enriched.”²³⁸

Privacy claims untethered from other wrongs (including breach of contract) can find support in section 44 of the *Restatement (Third) of Restitution and Unjust Enrichment*, titled “Interference with Other Protected Interests.”²³⁹ Specifically, subsection (1) states: “A person who obtains a benefit by conscious interference with a claimant’s legally protected interests (or in consequence of such interference by another) is liable in restitution as necessary to prevent unjust enrichment, unless competing legal objectives make such liability inappropriate.”²⁴⁰ The comments specifically mention that “[p]rofitable interference with . . . [a] claimant’s right of privacy, gives rise to a claim under § 44 if the benefit to the defendant is susceptible of measurement.”²⁴¹ One illustration explains that when a local pharmacy sells its customers’ prescription records to a national chain without permission, the customers have a cause of action in unjust enrichment against both the local pharmacy and the national chain.²⁴² Importantly, the customers can recover both proceeds of the sale from the local pharmacy and any additional profits the national chain derived.²⁴³

Still some courts have failed to understand that there can be a cause of action for unjust enrichment. Decisions addressing unjust enrichment claims in both California and Texas have been all over the map.²⁴⁴ Intermediate appellate courts in both jurisdictions have stubbornly refused to recognize unjust enrichment as a separate cause of action despite the respective state

237. *Blue Cross Health Servs., Inc. v. Sauer*, 800 S.W.2d 72, 76–77 (Mo. Ct. App. 1990).

238. *Id.* at 75.

239. See RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 44 (AM. L. INST. 2011).

240. *Id.*

241. *Id.* § 44 cmt. b.

242. *Id.* § 44 cmt. b, illus. 10. Illustration 10 is based on *Anonymous v. CVS Corp.*, in which the predicate wrongful act was violating the “pharmacist’s professional obligation of nondisclosure.” *Anonymous v. CVS Corp.*, 728 N.Y.S.2d 333, 340 (Sup. Ct. 2001).

243. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 44 cmt. b, illus. 10 (AM. L. INST. 2011).

244. See Douglas L. Johnson & Neville L. Johnson, *What Happened to Unjust Enrichment in California? The Deterioration of Equity in the California Courts*, 44 LOY. L.A. L. REV. 277, 291 (2010) (discussing California’s “schizophrenic treatment of unjust enrichment”); George P. Roach, *Unjust Enrichment in Texas: Is it a Floor Wax or a Dessert Topping?*, 65 BAYLOR L. REV. 153, 204 (2013) (noting that “[d]espite . . . ten Texas Supreme Court opinions . . . that hold or acknowledge unjust enrichment as a cause of action,” there is a recent controversy over whether it is a cause of action).

supreme courts saying that the cause of action exists.²⁴⁵ This Section will focus on how California has addressed the unjust enrichment cause of action. Given that so many technology companies are headquartered there, many privacy lawsuits take place in federal district courts in California.²⁴⁶

A 1996 California Supreme Court decision, *Ghirardo v. Antonioli*, expressly recognized a cause of action for unjust enrichment, saying “[t]he claim [of unjust enrichment] was adequately pleaded and proved” in a real estate case.²⁴⁷ This statement was not a mere afterthought. The court went into some detail describing the cause of action:

Under the law of restitution, an individual may be required to make restitution if he is unjustly enriched at the expense of another. A person is enriched if he receives a benefit at another’s expense. The term “benefit” “denotes any form of advantage.” Thus, a benefit is conferred not only when one adds to the property of another, but also when one saves the other from expense or loss.²⁴⁸

Nevertheless, subsequent federal and state decisions have repeatedly said that no cause of action for unjust enrichment existed under California law.²⁴⁹ Many of these decisions were privacy cases.²⁵⁰ For example, the plaintiffs in *Fraleley v. Facebook* were not allowed to pursue a cause of action for unjust enrichment when Facebook introduced a “Sponsored Story” advertisement program without the plaintiffs’ consent.²⁵¹ Facebook sold advertisements that showed customers’ names and photos to their friends when they liked a business (e.g., “Angel Frolicker likes Rosetta Stone”).²⁵²

245. For discussion of the California cases, see *infra* notes 249–52 and accompanying text. For discussion of the Texas cases, see Roach, *supra* note 244, at 216 & nn.323 & 325.

246. See Daniel R. Stoller, *California Courts Set Privacy Litigation Standards for Big Tech*, BLOOMBERG L. (Oct. 15, 2019, 3:31 AM), <https://news.bloomberglaw.com/privacy-and-data-security/california-courts-set-privacy-litigation-standards-for-big-tech> [<https://perma.cc/L9DE-86DQ>].

247. *Ghirardo v. Antonioli*, 924 P.2d 996, 1005 (Cal. 1996).

248. *Id.* at 1003 (citations omitted) (quoting RESTATEMENT (FIRST) OF RESTITUTION § 1 cmt. b (AM. L. INST. 1937)).

249. See *Ferrington v. McAfee, Inc.*, No. 10-CV-01455-LHK, 2010 WL 3910169, at *17 (N.D. Cal. Oct. 5, 2010) (“The Court also notes that there is no cause of action for unjust enrichment under California law.”); *Robinson v. HSBC Bank USA*, 732 F. Supp. 2d 976, 987 (N.D. Cal. 2010); *Levine v. Blue Shield of Cal.*, 117 Cal. Rptr. 3d 262, 278 (Ct. App. 2010) (finding “[t]here is no cause of action in California for unjust enrichment” (alteration in original) (quoting *Durell v. Sharp Healthcare*, 108 Cal. Rptr. 3d 682, 699 (Ct. App. 2010))); *Melchior v. New Line Prods., Inc.*, 131 Cal. Rptr. 2d 347, 357 (Ct. App. 2003).

250. See *Pirozzi v. Apple, Inc.*, 966 F. Supp. 2d 909, 924 (N.D. Cal. 2013); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1031 (N.D. Cal. 2012) (“California does not recognize a stand-alone cause of action for unjust enrichment”); *In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *15 (N.D. Cal. Sept. 20, 2011).

251. *Fraleley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 791–92, 814–15 (N.D. Cal. 2011).

252. *Id.* at 791 (quoting Second Amended Class Action Complaint for Damages ¶¶ 65–68, *Fraleley*, 830 F. Supp. 2d 785 (No. 11-CV-01726-LHK)). The court did allow the plaintiffs to request

At the same time, a few decisions including at least one privacy case arrived at the opposite conclusion and recognized unjust enrichment as a distinct cause of action.²⁵³ Douglas and Neville Johnson have provided a thorough account of how California found itself in this mess.²⁵⁴ The story involves following dated appellate court precedent while somehow missing *Ghirardo v. Antonioli*.²⁵⁵ Decisions omitting *Ghirardo* are surprising because *Ghirardo* is controlling precedent from the California Supreme Court and was decided later in time than the precedent courts followed instead.²⁵⁶ This created a split, with some decisions even wrongly arguing that *Ghirardo* did not endorse an unjust enrichment cause of action.²⁵⁷

In 2015, the California Supreme Court appeared to finally put the issue to rest in *Hartford Casualty Insurance Co. v. J.R. Marketing*.²⁵⁸ The court held that an insurer could assert a claim for unjust enrichment directly against *Cumis* counsel to recover any excessive fees.²⁵⁹ Importantly, unjust enrichment was not dependent on some other theory of liability. Citing to both *Ghirardo* and *Restatement* section 1, *Hartford Casualty* said the doctrine applied “even if no contract between the parties itself expresses or implies such a

unjust enrichment as a remedy for some of their other statutory claims that expressly allowed for disgorgement. *Id.* at 815.

253. *Hernandez v. Path, Inc.*, No. 12-CV-01515 YGR, 2012 WL 5194120, at *8 (N.D. Cal. Oct. 19, 2012) (regarding data privacy issues, “there is a cause of action for unjust enrichment under California law”); *see also Paracor Fin., Inc. v. Gen. Elec. Cap. Corp.*, 96 F.3d 1151, 1167 (9th Cir. 1996) (“Under both California and New York law, unjust enrichment is an action in quasi-contract . . .”); *Hawthorne v. Umpqua Bank*, No. C-11-6700 YGR, 2012 WL 1458194, at *2 (N.D. Cal. Apr. 26, 2012) (“The weight of authority . . . supports a determination that ‘unjust enrichment’ is a proper claim for relief, or cause of action, under California law.”); *Peterson v. Cellco P’ship*, 80 Cal. Rptr. 3d 316, 323 (Ct. App. 2008) (reciting the elements of an unjust enrichment claim); *Hirsch v. Bank of Am.*, 132 Cal. Rptr. 2d 220, 229–30 (Ct. App. 2003) (finding that plaintiffs stated a valid claim for unjust enrichment where banks collected and retained excessive fees passed through to plaintiffs by title companies); *Lectrodryer v. SeoulBank*, 91 Cal. Rptr. 2d 881, 882–83 (Ct. App. 2000) (finding that the evidence supported the jury’s verdict of unjust enrichment).

254. *See generally* Johnson & Johnson, *supra* note 244 (analyzing the evolution of unjust enrichment as a cause of action in California courts).

255. *Id.* at 287–88. Johnson and Johnson discuss how the U.S. District Court for the Eastern District of California failed to cite *Ghirardo v. Antonioli* in *Walker v. USAA Casualty Insurance Co.* *Id.*; *see Walker v. USAA Cas. Ins. Co.*, 474 F. Supp. 2d 1168, 1174 (E.D. Cal. 2007), *aff’d sub nom. Walker v. Geico Gen. Ins. Co.*, 558 F.3d 1025 (9th Cir. 2009).

256. Johnson & Johnson, *supra* note 244, at 287.

257. *Id.* at 288–89; *see, e.g., Vincent Consol. Commodities, Inc. v. Am. Trading & Transfer, LLC*, No. 07-CV-20 W (LSP), 2007 WL 9646371, at *3 (S.D. Cal. July 24, 2007) (dismissing claim because “California does not recognize a separate claim for unjust enrichment” and inaccurately stating that the *Ghirardo* court “merely mentioned a ‘cause of action for unjust enrichment’ in passing” (quoting *Ghirardo v. Antonioli*, 924 P.2d 996, 1003 (Cal. 1996))).

258. *Hartford Cas. Ins. Co. v. J.R. Mktg., LLC*, 353 P.3d 319, 332 (Cal. 2015).

259. *Id.* at 321–22. When an “insurer initially refuse[s] to defend [an] insured against a third-party lawsuit” and is compelled by court order to do so, the independent counsel hired by the insurer under a reservation of rights is often called *Cumis* counsel. *Id.* at 321.

[restitutionary] duty.”²⁶⁰ These citations are significant because both the *Restatement* and *Ghirardo* recognize a cause of action for unjust enrichment. Most subsequent courts applying California law now recognize that unjust enrichment is a cause of action.²⁶¹

This recognition has the potential to reinvigorate privacy claims in California. For example, *In re Facebook, Inc., Consumer Privacy User Profile Litigation*, the plaintiffs raised a number of claims based on the improper disclosure of their information to third parties as part of the Cambridge Analytica scandal.²⁶² Citing to *Hartford Casualty, inter alia*, the decision denied the defendant’s motion to dismiss the unjust enrichment claim.²⁶³ Importantly, a passage from the decision noted that “even if the plaintiffs suffered no economic loss from the disclosure of their information, they may proceed . . . on a claim for unjust enrichment to recover the gains that [the defendant] realized from its allegedly improper conduct.”²⁶⁴ This passage reveals why the nature of an unjust enrichment claim can avoid many pitfalls associated with other claims. Even when the harm to the victims is intangible, the unjust enrichment claim can successfully help privacy victims.²⁶⁵

D. STANDING ON DEFENDANT’S GAIN

Another advantage of relying on unjust enrichment is that standing should not be a serious obstacle. Because the monetary remedy is based on the defendant’s unjust gain and not the victims’ injuries, courts cannot point to the amorphous nature of privacy victims’ injuries to dismiss their cases for lack of standing. Importantly, privacy victims may not just have standing to bring unjust enrichment claims, they may be able to bootstrap unjust enrichment to gain standing to recover statutory damages.

A group of leading restitution and remedies scholars has previously made these arguments in an amicus brief in *Spokeo, Inc. v. Robins*.²⁶⁶ As an initial

260. *Id.* at 326.

261. *Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1057 (N.D. Cal. 2018) (noting that California has clarified its position and now allows a claim for unjust enrichment); *In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1233–34 (C.D. Cal. 2017) (denying defendants’ motion to dismiss plaintiffs’ California unjust enrichment claims). *But see* Brodsky v. Apple Inc., No. 19-CV-00712-LHK, 2019 WL 4141936, at *10 (N.D. Cal. Aug. 30, 2019) (failing, still, to recognize unjust enrichment “as a stand-alone cause of action” and dismissing claim).

262. *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 776 (N.D. Cal. 2019).

263. *Id.* at 803.

264. *Id.*; *see also Williams*, 384 F. Supp. 3d at 1050 (“The complaint need not include economic injury to establish standing for . . . unjust enrichment claims.”).

265. This decision also takes a less restrictive view of how the plaintiffs’ injuries fit into other doctrines like standing and breach of contract. *In re Facebook*, 402 F. Supp. 3d at 785–87, 802.

266. Brief of Restitution and Remedies Scholars as Amici Curiae in Support of Respondent, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (No. 13-1339), 2015 WL 5302537, at *1–3 [hereinafter Restitution and Remedies Scholars’ Brief]. The brief was written by Douglas Laycock, Mark Gergen, and Doug Rendleman. Both Laycock and Rendleman have written

matter, the Restitution and Remedies Scholars' Brief explained what is required to show standing for unjust enrichment: "Standing to sue in unjust enrichment requires plaintiff to show that he is the source of defendant's enrichment, either in the sense that he suffered a loss that corresponds to defendant's gain, or in the sense that defendant's gain was acquired by violating plaintiff's rights."²⁶⁷ Notice what is not mentioned. Standing for restitution does not require that plaintiffs establish that they were injured or harmed.²⁶⁸ That is because restitution is based on the defendant's gain, not the plaintiff's loss. This point is uncontroversial and a foundational tenet of restitution.²⁶⁹

Numerous causes of action allow a plaintiff to recover the defendant's unjust enrichment without requiring the plaintiff to show additional harm. The Restitution and Remedies Scholars' Brief identified ten diverse categories of lawsuits that illustrate this principle and described examples in each category. These categories are: (1) commercial bribes and kickbacks; (2) business opportunities; (3) other conflicts of interest; (4) misuse of confidential information; (5) forfeiture of fees; (6) intellectual property infringement; (7) trespass; (8) conversion; (9) rescission; and (10) the slayer rule.²⁷⁰

The rules are straightforward and intuitive. Consider bribes and kickbacks. A company can recover the wrongdoer's gain even if the company was unharmed.²⁷¹ The same principle applies to wrongdoing by different types of fiduciaries.²⁷² Companies can recover profits their agent made from wrongfully taking a corporate opportunity without showing the company would have actually taken advantage of that opportunity had it been

leading casebooks in this area. *Id.* at app. *1A–2A. The signatories also included Andrew Kull, the Reporter of *Restatement (Third) of Restitution and Unjust Enrichment*, and several Advisers and Members Consultative Group participants for that *Restatement*. *Id.*

267. *Id.* at *3 (emphasis omitted).

268. See *Williams*, 384 F. Supp. 3d at 1050 ("The complaint need not include economic injury to establish standing for . . . unjust enrichment claims.").

269. See DOBBS & ROBERTS, *supra* note 112, § 1.1, at 4 ("[R]estitution is measured by defendant's gains, not by plaintiff's losses."); 1 GEORGE E. PALMER, *THE LAW OF RESTITUTION* 51 (1978) ("[I]n the damage action the plaintiff seeks to recover for the harm done to him, whereas in the restitution action he seeks to recover the gain acquired by the defendant through the wrongful act.").

270. Restitution and Remedies Scholars' Brief, *supra* note 266, at *7–18.

271. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 43 cmt. d, illus. 17–19 (AM. L. INST. 2011) ("The taking of a bribe or 'secret commission' is condemned, without regard to economic injury, because it poses a risk of divided loyalty."); *id.* § 44 cmt. b, illus. 9 & reporter's note b.

272. RESTATEMENT (THIRD) OF AGENCY § 8.02 cmt. b (AM. L. INST. 2006) ("To establish that the agent is subject to liability, it is not necessary that the principal show that the agent's acquisition of a material benefit harmed the principal.").

available.²⁷³ One prominent example of this principle is found in *Jackson v. Smith*. In that case, the receiver for the plaintiff arranged to sell the plaintiff's land at auction.²⁷⁴ A group that included the receiver was the highest bidder and later resold the land for a profit.²⁷⁵ Even though the Supreme Court recognized "that the sale was fairly conducted[,] that there was competitive bidding," and "the estate may not have been injured," the Court awarded the plaintiff the defendants' entire profits based on breach of fiduciary duty.²⁷⁶ In short, disgorgement was awarded even though there was no evidence that the defendants' conduct made the plaintiff worse off. In fact, by making the highest bid, the defendants may have actually made the plaintiff better off.

Claims of conversion are also analogous to the claims data privacy victims make because successful conversion plaintiffs need not show harm. In a typical conversion case, a defendant uses the plaintiff's property without permission. This is similar to privacy cases where companies use or sell their customers' data without customer permission. As in many privacy cases, the conversion plaintiff may have suffered no concrete injury. Yet under the law of restitution, the plaintiff can still recover based on unjust enrichment.²⁷⁷ For example, in *Ollwell v. Nye & Nissen Co.*, the plaintiff's egg-washing machine was stored next to the defendant's premises.²⁷⁸ The defendant proceeded to use the machine for three years without permission.²⁷⁹ The plaintiff eventually learned of the defendant's conversion and sued for unjust enrichment.²⁸⁰ In response, the defendant argued the plaintiff was not damaged because the plaintiff had not been using the machine during the three-year period.²⁸¹ The Supreme Court of Washington rejected this argument, finding injury in the defendant's violation of the plaintiff's property rights.²⁸²

273. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 43 cmt. d, illus. 15 (AM. L. INST. 2011) (showing corporation allowed to recover wrongful gain even though both parties conceded that corporation would not have taken advantage of the opportunity).

274. *Jackson v. Smith*, 254 U.S. 586, 587 (1921).

275. *Id.* at 587–88.

276. *Id.* at 587, 589.

277. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 40 cmt. c, illus. 3 (AM. L. INST. 2011). In this illustration, the developer temporarily stores dirt on the owner's lot without permission. *Id.* Even though the owner "has suffered no quantifiable injury," the developer is liable in restitution "measured by the rental value of [the property] during the months the dirt was present, liberally estimated." *Id.*

278. *Ollwell v. Nye & Nissen Co.*, 173 P.2d 652, 652 (Wash. 1946).

279. *Id.* at 653.

280. *Id.* The plaintiff waived his cause of action based on the tort of conversion and elected to pursue unjust enrichment, presumably because the remedy in restitution was more valuable in this case. *See id.* at 654.

281. *See id.* at 653.

282. *Id.* at 654; *see also* RESTATEMENT (SECOND) OF TORTS § 7 cmt. a (AM. L. INST. 1965) ("[A]ny intrusion upon land in the possession of another is an injury, and, if not privileged, gives rise to a cause of action even though the intrusion is beneficial, or so transitory that it constitutes no interference with or detriment to the land or its beneficial enjoyment.").

These are but a few of the many unjust enrichment examples the Restitution and Remedies Scholars' Brief describes in detail. The entire group of examples is diverse along several dimensions. These examples span tort, contract, property, and agency law.²⁸³ Decisions are found in state and federal court (including the U.S. Supreme Court) cases decided in each of the last four centuries.²⁸⁴ In short, there is an incredibly well-established body of law that demonstrates that courts have adjudicated claims for unjust enrichment despite lack of harm to the plaintiff. The vast majority of these cases do not even mention standing because it is taken as a given.

Standing should operate no differently for plaintiffs in privacy cases that bring claims based in unjust enrichment. As the Supreme Court established in *City of Los Angeles v. Lyons*, standing depends on the relief sought.²⁸⁵ Thus, plaintiffs' lack of standing to recover compensatory damages should not affect their standing with respect to claims for unjust enrichment. Indeed, in *Lexmark International, Inc. v. Static Control Components, Inc.* the Supreme Court found that the plaintiff had standing to seek disgorgement of the defendant's profits even when it could not "quantify its losses with sufficient certainty to recover damages."²⁸⁶ Because the plaintiff, Static Control, was pursuing false advertising claims under the Lanham Act, the decision dealt with standing in the context of statutory violations,²⁸⁷ but the larger point remains: standing for a claim seeking disgorgement does not require any harm to the plaintiff.

In most privacy cases, the defendant's enrichment is certainly concrete and should satisfy standing's injury in fact requirement. For example, if a company sells customer data in violation of its own privacy policy, the proceeds from that sale constitute the company's wrongful gains and should confer standing on the plaintiffs. This theory emerged in 2020 when the Ninth Circuit became the first federal court of appeals to base standing in a privacy case on unjust enrichment. In *In re Facebook, Inc. Internet Tracking Litigation*, the plaintiffs alleged that Facebook impermissibly sold user data to advertisers.²⁸⁸ Facebook contended "that unjust enrichment is not sufficient to confer standing" and that the plaintiffs must demonstrate some harm to themselves.²⁸⁹ The Ninth Circuit rejected this argument stating that the

283. Restitution and Remedies Scholars' Brief, *supra* note 266, at *6–21. *See generally, e.g.*, *Mobil Oil Expl. & Producing Se., Inc. v. United States*, 530 U.S. 604 (2000) (breach of contract); *Edwards v. Lee's Adm'r*, 96 S.W.2d 1028 (Ky. 1936) (property); *Tarnowski v. Resop*, 51 N.W.2d 801 (Minn. 1952) (agency); *Raven Red Ash Coal Co. v. Ball*, 39 S.E.2d 231 (Va. 1946) (tort).

284. *See* Restitution and Remedies Scholars' Brief, *supra* note 266, at *6–21; *see, e.g.*, *Mobil Oil*, 530 U.S. at 607; *Edwards*, 96 S.W.2d at 1032–33; *Ex p Lacey* (1802) 31 Eng. Rep. 1228, 1228; 6 Ves. Jun. 626, 626; *Keech v. Sandford* (1726) 25 Eng. Rep. 223, 223; Sel. Cas. T. King 61, 61.

285. *City of Los Angeles v. Lyons*, 461 U.S. 95, 105 & n.6 (1983) (differentiating between standing to seek an injunction and standing for money damages).

286. *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 135 (2014).

287. *Id.* at 122–23.

288. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 600 (9th Cir. 2020).

289. *Id.* at 599.

“[p]laintiffs sufficiently alleged a state law interest [namely, unjust enrichment] whose violation constitutes an injury sufficient to establish standing to bring their [state statutory claims and common law claims].”²⁹⁰ The same kind of analysis should confer standing to victims of data breaches. In these cases, the unjust enrichment would simply be the wrongful savings the company enjoyed because it did not deploy reasonable data security precautions. These remedies are all concrete and should provide privacy plaintiffs with constitutional standing.

Importantly, unjust enrichment may give standing to privacy victims when they seek statutory damages. Consider the Cable Communications Policy Act, which requires cable companies to destroy personally identifiable information after it “is no longer necessary for the purpose for which it was collected.”²⁹¹ The statute gives individuals a private cause of action and allows them to recover “actual damages but not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher.”²⁹² When plaintiffs brought class action lawsuits alleging two different cable companies violated this statute, both the Seventh and Eighth Circuits dismissed the complaints based on standing.²⁹³ Because there was no evidence that the plaintiffs’ information had been misused, there were no injuries to provide standing.

Unjust enrichment can change that analysis. The *Restatement* explains that the violation of a statutory duty can support a claim for unjust enrichment.²⁹⁴ Relying on this theory, plaintiffs can recast their allegations in ways that confer standing.²⁹⁵ Under the Cable Communications Policy Act, the defendants had a statutory duty to institute a program that regularly deleted unnecessary personal information.²⁹⁶ They did not do so. Consequently, the defendants unjustly saved money by refusing to provide the services they were obligated to supply. Even if the savings are small, unjust

290. *Id.* at 601.

291. 47 U.S.C. § 551(e) (2018).

292. *Id.* § 551(f)(2)(A).

293. *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 913 (7th Cir. 2017) (“[T]he absence . . . of any concrete injury inflicted or likely to be inflicted on the plaintiff . . . requires that we affirm the district court’s judgment dismissing the plaintiff’s suit for want of standing.”); *Braitberg v. Charter Commc’ns, Inc.*, 836 F.3d 925, 930 (8th Cir. 2016) (holding that plaintiff lacked standing “without a plausible allegation that [defendant’s] mere retention of the [personal] information caused any concrete and particularized harm to the value of that information”).

294. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 44 cmt. b (AM. L. INST. 2011) (“[C]ompetitive practices prohibited by law, such as deceptive marketing, support a claim in restitution by the rule of this section.”).

295. This tactic is different from simply pursuing a claim for unjust enrichment based on a statutory violation. While section 44 certainly does provide for that possibility, disgorgement “is not available where the claim would conflict with limits imposed by other law on the defendant’s liability or on the claimant’s remedies for the wrong.” *Id.* § 44 cmt. d.

296. *Gubala*, 846 F.3d at 910; *Braitberg*, 836 F.3d at 927.

enrichment provides a path to statutory damages. Of course, this tactic does not just apply to the Cable Communications Policy Act. Standing presents an obstacle to recovering damages under many privacy statutes including, for example, the Fair Credit Reporting Act, Washington, D.C.'s Use of Consumer Identification Information Act, and the Stored Communications Act.²⁹⁷ Unjust enrichment has the potential to aid plaintiffs seeking statutory damages in all these contexts.

IV. COMPLICATIONS

The law of restitution and unjust enrichment is flexible and far reaching. Part IV discusses various complications that would accompany the use of unjust enrichment in privacy law. These include: (1) potential extensions of the theory; (2) an important limitation: the ability to contract out of some parts of unjust enrichment; and (3) complications with calculating unjust enrichment.

A. OTHER BASES FOR UNJUST ENRICHMENT

This Article has focused on using unjust enrichment to respond to broken privacy promises. Consequently, the Article has described how unjust enrichment can serve as a remedy for breach of contract and as an independent cause of action based on a broken promise. However, unjust enrichment as a cause of action is not limited to addressing broken promises. Many other “wrongful” acts have potential to trigger an unjust enrichment claim.

Sections 40–44 of the *Restatement* describe various types of these wrongful acts.²⁹⁸ They range from trespass to interference with intellectual property rights. But two particular wrongs stand out as potential bases for unjust enrichment in the privacy context. They are statutory violations²⁹⁹ and breach of fiduciary or confidential obligations.³⁰⁰

As mentioned earlier, the violation of a statutory duty can support a claim for unjust enrichment.³⁰¹ Moreover, the list of statutes protecting data privacy is expanding rapidly. There are now statutes that deal with how companies

297. See Haley, *supra* note 9, at 1225–29 (assessing when plaintiffs were denied standing when bringing various different statutory claims); see also, e.g., *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1545 (2016) (remanding for further consideration of standing requirements where a plaintiff sued for violations of the Fair Credit Reporting Act); *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 512 (D.C. Cir. 2016) (denying standing to plaintiffs who asserted violations of Washington, D.C.'s Use of Consumer Identification Information Act).

298. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT §§ 40–44 (AM. L. INST. 2011). The Restitution and Remedies Scholars' Brief in the *Spokeo* case also surveys many of the wrongs that can lead to unjust enrichment claims. See *supra* notes 266–70 and accompanying text.

299. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 44 (AM. L. INST. 2011).

300. *Id.* § 43.

301. See *supra* notes 294–95 and accompanying text.

handle credit reports, record credit card information, store personally identifiable information, or even use biometric data.³⁰² The violation of any of these statutes can potentially trigger a cause of action in unjust enrichment. Importantly, some of the statutes do not just apply to companies that have a relationship with the aggrieved party, but to third party data brokers. For example, the new California Consumer Privacy Act allows individuals to demand that data brokers delete their personal information.³⁰³

To be sure, the viability of an unjust enrichment claim depends on the statute. Disgorgement is not available where the claim would conflict with limits imposed by a given statute.³⁰⁴ In other words, legislatures can draft statutes to opt out of unjust enrichment. Presumably, that means that an unjust enrichment claim is not viable if the legislature barred a private cause of action. But what if the statute is silent? Frankly, most legislators probably are not thinking of unjust enrichment as they draft privacy laws.³⁰⁵ In these cases, the default rule is that there is a claim for unjust enrichment because there is no conflict with the statute.

Finally, Jack Balkin has recently argued that companies that keep individuals' private information should be considered information fiduciaries.³⁰⁶ Alicia Solow-Niederman has expanded this idea, suggesting "data confidant" as a new category of fiduciary that could be tailored to fit commercial holders of consumer data.³⁰⁷ Like other fiduciaries, data confidants would be legally obligated to securely maintain consumer data regardless of whether they had explicit contractual agreements with the data owner.³⁰⁸ That certainly is not the law now. The act of storing a consumer's data imposes no fiduciary duties on companies like Google, Facebook, or American Express. But if the law moves in that direction, there are important implications for restitution and unjust enrichment. Historically, unjust enrichment has been a common

302. See *supra* note 297 and accompanying text; 740 ILL. COMP. STAT. ANN. 14/20 (West 2008).

303. See Press Release, State of Cal. Dep't of Just., Attorney General Becerra Reminds Consumers of Data Privacy Rights Under the California Consumer Privacy Act (June 30, 2020), <https://oag.ca.gov/news/press-releases/attorney-general-becerra-reminds-consumers-data-privacy-rights-under-california> [<https://perma.cc/3Z9R-7KUR>]; see also Scholz, *supra* note 43, at 663–81 (discussing how restitution and unjust enrichment might apply to third party data traffickers even before the enactment of statutes like the California Consumer Privacy Act).

304. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 44 cmt. d (AM. L. INST. 2011).

305. As mentioned earlier, most attorneys, lawmakers, and judges are no longer familiar with restitution and unjust enrichment. See *supra* note 106 and accompanying text.

306. See Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016); cf. Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 500–02 (2019) (identifying supporters of the information fiduciary concept but then criticizing the theory).

307. Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE. L.J.F. 614, 625 (2018).

308. *Id.*

remedy for breaches of fiduciary duties.³⁰⁹ Therefore, if a company breaches its duty as an information fiduciary and there are either wrongful gains or savings associated with that breach, there should be a viable unjust enrichment claim. In short, this Article's focus on applying unjust enrichment to broken promises is simply the first step in reviving unjust enrichment more generally in the privacy context.

B. CONTRACTING AROUND UNJUST ENRICHMENT

I do not want to overstate the benefits of the use of restitution and unjust enrichment in privacy law. It is not a panacea for all the problems that privacy victims face. If victims begin successfully asserting unjust enrichment against companies, the inevitable response will be efforts to limit liability. To the extent that unjust enrichment serves as a remedy for a breach of contract, it can plainly be bargained around.³¹⁰ This would obviously limit the benefits of the current proposal.

Indeed, "bargaining" is a misnomer as applied to customer adhesion contracts; contracting out of unjust enrichment will not be difficult. That is precisely what happened in *In re Sony Gaming Networks*.³¹¹ Sony's PlayStation Network allowed Sony console owners to purchase videogames and play multiplayer games.³¹² Unfortunately, hackers broke into the system and were able to obtain personal information on over 75 million accounts worldwide.³¹³ The hackers not only took basic identifying information like names, addresses, email addresses, and birthdates, but they may have also taken credit card information and answers to security questions.³¹⁴

The plaintiffs brought a class action against Sony alleging a variety of causes of actions including negligence, breach of contract, unjust enrichment, and various statutory violations.³¹⁵ As usual, tort claims were dismissed because

309. See *supra* notes 272–76 and accompanying text (discussing *Jackson v. Smith*, 254 U.S. 586 (1921)); see also RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 43 (AM. L. INST. 2011) ("A person who obtains a benefit . . . in breach of a fiduciary duty . . . is liable in restitution to the person to whom the duty is owed."); Roberts, *Disgorging Emoluments*, *supra* note 199, at 22 ("A classic basis for wrongfulness [for disgorgement] is a fiduciary breach.").

310. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 2(2) (AM. L. INST. 2011) ("A valid contract defines the obligations of the parties as to matters within its scope, displacing to that extent any inquiry into unjust enrichment.").

311. *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 984 (S.D. Cal.), *order corrected*, MDL No. 11md2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014); see also *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1040–41 (N.D. Cal. 2019) ("[Plaintiffs'] four breach of contract claims and the breach of confidence claim cannot move forward because of the limitation-of-liability clause.").

312. *In re Sony Gaming Networks*, 996 F. Supp. 2d at 953.

313. Emily Chung, *PlayStation Data Breach Deemed in 'Top 5 Ever,'* CBC (Apr. 27, 2011, 10:59 AM), <https://www.cbc.ca/news/technology/playstation-data-breach-deemed-in-top-5-ever-1.1059548> [<https://perma.cc/3L4F-2FEL>].

314. *Id.*

315. *In re Sony Gaming Networks*, 996 F. Supp. 2d at 959.

those data losses were not cognizable injuries.³¹⁶ In support of its contract and unjust enrichment claims, plaintiffs alleged that Sony broke its promise to provide adequate security, a representation that Sony made in its privacy policies.³¹⁷ The court dismissed these claims because Sony's privacy policy expressly disclaimed responsibility for keeping its customers' data safe.³¹⁸

While *In re Sony Gaming Networks* illustrates the limits of unjust enrichment, it is unlikely that all companies would be willing to disclaim responsibility for taking reasonable data security measures. Sony's services concerned gaming where consumer expectations of privacy may not be as strong as they are with respect to essential services. Consumers likely have higher expectations of privacy from banks, health care providers, and companies entrusted with particularly sensitive information. In industries where part of the core business is to safeguard customers' private information, companies may be less able to disclaim data protection responsibility.

Moreover, there are limits to the ability of companies to contract out of their obligations. Unjust enrichment claims may be based on the violation of statutes or even on negligence. In these cases, it is far less clear that companies can avoid unjust enrichment by simply adding a clause in an adhesion contract. Most states do not allow parties to contract out of gross negligence.³¹⁹ Some states even limit the ability of parties to contract out of negligence when there is an adhesion contract.³²⁰ Furthermore, clauses that seek to contract out of statutory obligations are also unenforceable.³²¹ Thus, while the first step in raising unjust enrichment claims may lie in contract, the future of this theory may depend on the ability of privacy victims to find other "wrongs" that cannot be contracted around.

C. CALCULATING UNJUST ENRICHMENT

If there is widespread adoption of unjust enrichment and restitution in privacy cases as this Article advocates, courts will have to determine precisely how much money to disgorge. Many of these calculations will not be as simple

316. *Id.* at 966–73.

317. *Id.* at 982.

318. *Id.* at 983.

319. *See* *Jones v. Dressel*, 623 P.2d 370, 376 (Colo. 1981) (en banc) (“An exculpatory agreement . . . [may not] shield against a claim for willful and wanton negligence.”); RESTATEMENT (SECOND) OF CONTS. § 195(1) (AM. L. INST. 1981) (“A term exempting a party from tort liability for harm caused intentionally or recklessly is unenforceable on grounds of public policy.”).

320. *See, e.g.,* *Hanks v. Powder Ridge Rest. Corp.*, 885 A.2d 734, 747 (Conn. 2005) (acknowledging it was adopting a minority view and finding that a clause in an adhesion contract that sought to absolve the defendant for negligence was unenforceable as violating public policy).

321. *See, e.g.,* 1 B.E. WITKIN, SUMMARY OF CALIFORNIA LAW § 679 (11th ed. 2017) (“[In California,] contract exempting from liability for ordinary negligence is valid where no public interest is involved But there can be no exemption . . . for . . . gross negligence, or violation of law.” (citations omitted)).

as they might appear. This Section does not purport to provide a comprehensive description of how to make these calculations. Instead, this Section merely identifies some issues that will likely arise as courts seek to determine how to calculate disgorgement in privacy cases.

Courts will have to determine how much money the defendant would have made had it not committed a wrong. That is because the amount disgorged is based on the money the defendant made from the wrongful conduct. Presumably, a court will simply subtract the money the defendant would have made in the absence of wrongful conduct. But this exercise in “but for” causation is not that simple.

Litigants will undoubtedly argue over what would have happened if the defendant had not engaged in any wrongful conduct. There are often many possible “counterfactuals” to select from. Consider a situation where a company sells both customers’ location data and purchase history. Assume selling the customers’ location information was wrongful (perhaps, because it violated its own privacy policy or a statute), but selling the customers’ purchase history was permissible. There are at least two potential counterfactuals.

First, the company might not have sold any customer information. In this case, a court could disgorge all the profits from the sale. However, the *Restatement* says that courts “may make such apportionments [and] may recognize such credits or deductions . . . as reason and fairness dictate.”³²² Thus, a court could seek to estimate how much profit is attributable to the location information and only award that amount. But that approach is not automatic. The *Restatement* says that “fairness” should be considered. Mark Gergen takes this suggestion one step further and argues that courts should consider the necessity of deterring wrongdoing and not awarding “gain from trade” (meaning wealth attributable to both the wrong and wealth the claimant may have earned absent the wrong).³²³ Under this approach, awards could be “reasonable multiples” of what the parties would have negotiated.³²⁴ Plainly, courts will have to address what factors warrant applying (or not applying) apportionments and credits.

Another counterfactual helps us understand causation in restitution. The same company might seek to prove that it simply would have changed its privacy policy to permit the sale and that customers would nonetheless have agreed to that change (as they often do with adhesion contracts). Under this last scenario, the company would have made precisely the same amount of

322. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 51(5) (AM. L. INST. 2011).

323. Gergen, *supra* note 134, at 850. The *Restatement* also rejects apportionment in some cases. Section 51, comment f explains that where “the defendant embezzles \$100 and invests the money in shares that he later sells for \$500,” the claimant should recover \$500 partly based on causation and partly because of deterrence. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 51 cmt. f (AM. L. INST. 2011).

324. Gergen, *supra* note 134, at 850.

money if it had not broken its promise. Thus, the defendant could reasonably argue that there are no profits to disgorge.

Now one might think that choosing between these two counterfactuals is merely an exercise in proof. In other words, the counterfactual that can be shown to be the one that was most likely to have occurred in the absence of wrongdoing is the one the court should use. However, Gergen has persuasively argued that is not what courts actually do. Instead, courts resolve causal uncertainty “against a wrongdoer when [the] conduct is ‘deemed wrongful precisely because it has a strong propensity to cause the type of harm that ensued.’”³²⁵ For the company that wrongfully sells customer data, that would suggest that courts should ignore the second counterfactual (company changes privacy policy to allow what it did). That is true even if the evidence shows that counterfactual was more likely to occur. Instead, courts should use the first counterfactual (company does not sell data) to calculate disgorgement. That is because to award nothing fails to provide any deterrence.³²⁶ The primary point of this example is to show that calculating the proper amount of money to disgorge is more than simply looking at causation. Courts should look to both fairness and equity to determine the end amount.

V. CONCLUSION

This Article seeks to address a set of data privacy law’s most intractable problems. Traditional legal claims are poorly suited for handling privacy losses. Contract and tort claims suffer from a variety of problems including: privacy policies are not part of consumer contracts; consumers rarely read or rely on privacy policies; the inability to trace harm to any specific data breach (i.e., causation); and the economic loss rule. Even worse, courts have also said that privacy injuries are not sufficiently concrete to serve as an element of damages for various causes of action. Courts have even held that many of these injuries fail to satisfy the Constitution’s basic standing requirement.

Fortunately, the law of restitution and unjust enrichment has the potential for breaking through this gauntlet. But courts have frequently misunderstood this often-neglected doctrine, causing it to languish. This Article clarifies various important misconceptions and explains why unjust enrichment is well suited for addressing modern privacy wrongs. It explains how unjust enrichment can serve as both a stand-alone cause of action and a remedy for other claims. Properly understood, unjust enrichment should allow privacy victims to disgorge the wrongful gains companies earn when they break their privacy promises. This also means that victims are entitled to recover any wrongful savings these companies retain when they use deficient

325. *Id.* at 840 (quoting *Liriano v. Hobart Corp.*, 170 F.3d 264, 271 (2d Cir. 1999)).

326. *Id.* at 835 (saying that “wrongdoer[s] [are often] denied the opportunity to argue the counterfactual involving the competing cause” based on policy and fairness considerations).

cybersecurity. Ideally, increased understanding and implementation of unjust enrichment will incentivize companies to take their privacy promises seriously or finally face consequences.