OPTIMIZING BREACH NOTIFICATION

Mark Verstraete[*]
*Tal Zarsky***

Our lives depend on digital infrastructure and maintaining data security is now a crucial social objective. An emerging central strategy to promote data security is through breach notification laws, which require firms to give notice upon discovering a security breach. These laws are pervasive and prominent. All fifty states, several federal laws, and the E.U.'s General Data Protection Regulation ("GDPR") and Organisation for Economic Co-operation and Development ("OECD") have incorporated notification schemes into an array of privacy and data security efforts. However, these laws are in flux, with different jurisdictions constantly offering new requirements and exceptions. In view of looming and important regulatory changes, this Article interrogates the structure and efficacy of the diverse set of data breach notification statutes and proposes an optimal regulatory path forward. In doing so, it provides crucial theoretical insights about both data breach notification laws and theories about legal remedies more generally.

The Article begins by introducing the "nuts and bolts" of data breach notification statutes and their normative justifications. It breaks new ground by offering a novel taxonomy of normative justifications. In particular, a data breach notification statute can be justified as set to promote four objectives: deterring firms from applying lax security ex ante, mitigating the harms caused to individuals from the breach ex post, generating information flows regarding security breaches to regulators and experts, and enhancing the autonomy of impacted individuals harmed by the breach. Importantly, different regulatory design strategies promote some of these justifications at the expense of others. Further, this Article assesses the conventional wisdom about breach notification statutes that frames these

[*] Postdoctoral Research Fellow, UCLA Institute for Technology, Law, and Policy.

[**] Visiting Scholar, University of Pennsylvania Carey Law School (2019-2020); Vice Dean and Professor of Law, University of Haifa–Israel. We thank Yifat Aran Anita Allen, Tom Baker, Shyam Balganesh, Steven Bellovin, Brett Frischmann, Jonathan Mayer, Sasha Romanosky, Paul Schwartz, Katherine Strandburg, Salome Viljoen, Gabe Nicholas, Aaron Shapiro, Sebastian Benthall, Ira Rubinstein, Jonathan Weinberg, Yafit Lev-Aretz, Asaf Lubin, Jake Goldenfein, Evan Selinger, Kevin Werbach, Christopher Yoo, Eyal Zamir and the participants of the Northeastern Privacy Law Scholars Conference (Princeton), the Privacy Law Seminar at Berkeley Law School, the Privacy Research Group, NYU Law School, the CTIC Law and Technology Scholarship Colloquium (at PennLaw), the Law, Economics, Technology: Privacy seminar at Villanova Law School and the University of Haifa—Faculty of Law Seminar for their insightful comments. Thank you to the editors at the *University of Illinois Law Review* for their hard work and helpful editing.

unique laws within more traditional legal remedies (such as negligence, reputational sanctions, and strict liability). The Article demonstrates that these traditional legal paradigms fail to capture the unique features of breach notification requirements. As a result, breach notification cannot be subsumed into these well-worn models.

Finally, the Article examines overlooked consequences of breach notification schemes by explaining that the normative and practical foundations of data breach notification statutes are complicated by central yet under-theorized features of both cybersecurity and tort law—unfairness and moral luck and activity levels. The Article then returns to the noted basic justifications and demonstrates how they are impacted by these overlooked theoretical insights. The Article concludes by applying these insights to provide a roadmap for regulators to build a data breach notification statute that aligns with their objectives and allows them to optimize their preferences while assuring fairness and efficiency.

TABLE OF CONTENTS

I. INTRODUCTION

As much of our lives depend on digital infrastructure, the task of maintaining a high level of data security has become crucial, even critical, to our society. Governments worldwide have moved to promote security in a variety of ways. One central measure to do so is through the introduction of breach notification laws.

Data breach notification laws are pervasive and prominent. All fifty states and several federal laws incorporate these statutes into an array of privacy and data security efforts.[1] In Europe, the European Union's ("EU") General Data Protection Regulation ("GDPR") includes broad data breach notification provisions, which are now mandated in all EU member states.[2] The Organisation for Economic Co-operation and Development ("OECD") has recommended implementing these rules as well.[3] Moreover, breach notification statutes are not merely symbolic; they carry substantial fines against firms that violate their reporting obligations.[4] As a result, breach notification laws have certainly caught

[1] At the state level, California enacted the first comprehensive data breach notification statute in 2003. *See* CAL. CIV. CODE §1798.82 (West 2020). Other states have followed suit. Currently, all fifty states have passed similar data breach notification statutes. *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (July 17, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/UW7B-ELGW] (detailing the various state laws that require data breach notification). Federally, data breach notification is, among others, one of the requirements put in place by the Health Insurance and Portability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (1996). *See* 45 C.F.R. §§ 164.400–.404 (2020); Gramm-Leach-Bliley Act, Pub. L. No. 106–102, § 501, 113 Stat. 1338, 1436 (1999). There are also breach notification rules set by the Security and Exchange Commission which will only be discussed incidentally in this Article. *See* Yaki Faitelson, *SEC's New Toughness on Breach Reporting and What It Means for your IT Compliance*, FORBES (Aug. 13, 2018, 8:45 AM), https://www.forbes.com/sites/forbestechcouncil/2018/08/13/secs-new-toughness-on-breach-reporting-and-what-it-means-for-your-it-compliance/?sh=2d828254a67d [https://perma.cc/5VXD-GP6N].

[2] Commission Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1) 85 [hereinafter GDPR].

[3] OECD, THE OECD PRIVACY FRAMEWORK 26 (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [https://perma.cc/G68A-ATFK].

[4] For instance, see GDPR, *supra* note 2, at 82 (Article 83) (detailing penalties for failure to notify after data breaches).

the attention of business leaders, consumer groups, and the press; yet, a complete theoretical analysis of these rules has been somewhat neglected.[5]

As with many innovative legal remedies, breach notification laws are still being formulated and updated.[6] As many privacy scholars and policymakers are suggesting a federal overhaul, we are now facing an opportune moment to examine the wisdom, effectiveness, and design of data breach notification laws.[7] Any federal privacy legislation would likely include a data breach notification provision.[8] Furthermore, given the difference between various state laws and their breach notification requirements, a push for a federal law addressing these matters—while potentially preempting some of the existing regulations—is almost certain, though some states may balk at federalization in order to retain authority.[9]

In view of the looming and important regulatory changes ahead as well as the overall importance of strong data security to society, this Article examines the structure and efficacy of the diverse set of data breach notification statutes and proposes an optimal regulatory path forward. In doing so, this Article adds several crucial innovations to the debate over these legal requirements.

At first blush, the rationale for breach notification requirements seems obvious; after all, if our data is compromised, shouldn't we have a right to know about it? Upon closer scrutiny, however, deconstructing breach notification requirements is quite challenging. This challenge is largely a product of the fact

[5] There are a few notable exceptions to this. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007) (offering the seminal contribution in the debate about data breach notification laws); Jane K. Winn, *Are "Better" Security Breach Notification Laws Possible?*, 24 BERKELEY TECH. L.J. 1133 (2009); FRED H. CATE, INFORMATION SECURITY BREACHES: LOOKING BACK AND THINKING AHEAD, CTR. FOR INFO. POL'Y LEADERSHIP (2008), https://www.repository.law.indiana.edu/facpub/233/ [https://perma.cc/6KD2-863D]; Thomas M. Lenard & Paul H. Rubin, *Much Ado About Notification*, 29 REGUL. 44 (2006); Sasha Romanosky, Rahul Telang & Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGMT. 256 (2011).

[6] For instance, California and New York have both recently updated their breach notification laws. 2019 CA A.B. 1130 (updating the California breach notification statute to cover biometric data); 2019 N.Y. Sess. Laws Ch. 117 (S. 5575–B) (McKinney) (updating the New York breach notification statute to include new and different types of personal information are covered by the breach notification statute).

[7] Ronan Shields, *Privacy Advocates Urge FTC Reform, Call for New Legislation*, ADWEEK (Jan. 17, 2019), https://www.adweek.com/programmatic/privacy-advocates-urge-ftc-reform-call-for-new-legislation/ [https://perma.cc/6A6B-GUXJ] (detailing the growing chorus suggesting the need for a federal privacy overhaul).

[8] For example, Europe's comprehensive data protection law, the GDPR, contains an important breach notification provision. If the United States follows Europe's example of crafting a comprehensive privacy statute, then it is likely that it will contain a breach notification provision as well. *See* GDPR, *supra* note 2, at 83–84 (Article 85).

[9] A recent article cites the disparity between different states' data breach notification statutes as a concern that federal legislation would remedy. *See* Shalin R. Sood, *Could a Federal Data Privacy Law be a Reality in 2019?*, NAT'L L. REV. (2019), https://www.natlawreview.com/print/article/could-federal-data-privacy-law-be-reality-2019 [https://perma.cc/J7YX-3XMG]. There is likely to be pushback against federal preemption of state privacy laws, however, especially by State Attorneys General ("AGs"). Recently, State AGs drafted an open letter against federal preemption of state breach notification laws. *See* Saranna Soroka, *Coalition of 32 State AGs Outline Opposition to Federal Preemption of State Data Breach Notification Laws*, JOLT DIGEST (Apr. 8, 2018), https://jolt.law.harvard.edu/digest/coalition-of-32-state-ags-outline-opposition-to-federal-preemption-of-state-data-breach-notification-laws [https://perma.cc/TL8Z-297H].

that data breach notification is a unique legal remedy. It constitutes an idiosyncratic disclosure requirement.[10] This disclosure requirement enables and facilitates traditional tort remedies (including self-help) and often triggers reputational harms.[11] Thus, an examination of the structure of breach notification laws implicates fundamental concepts of private law, as well as cutting edge issues in law and technology. As a result, it proves to be an intellectual challenge with crucial practical implications and lessons that are relevant to an array of existing legal conundrums.

To begin this analysis, Part II introduces both the "nuts and bolts" of data breach notification statutes and their normative justifications. Part II.A briefly draws out the key elements of these laws, including how these elements differ among jurisdictions. In doing so, we outline several U.S. state-specific regimes and contrast them with the EU's detailed breach notification scheme (as stated in the GDPR).

Section II.B provides the foundation for the discussion to follow by introducing four basic justifications for breach notification requirements: *deterrence*, *mitigation*, *enhancing information flows*, and *promoting autonomy*. The analysis closely examines these justifications while contextualizing them within today's digital age. It highlights that often these normative guideposts for data breach notification laws are inherently at odds; maximizing efforts to achieve one objective often conflict with a different objective.

Section II.C demonstrates that foundational assumptions about legal remedies in general fail to capture the unique features of breach notification requirements. Breach notification is the proverbial square peg that fails to fit the round hole. The analysis shows that framing breach notification rules as merely providing a remedy for *negligence* is an incomplete analogy and addresses how breach notification relates to other liability regimes such as *strict liability*, *reputational sanctions*, and *premises liability*.

In our attempt to formulate an optimal breach notification policy that would balance the possible underlying justifications, Part III turns to overlooked outcomes and consequences of breach notification schemes. Normative foundations of data breach notification statutes are complicated by central, yet undertheorized features of both cybersecurity and tort law—*unfairness and moral luck* and *activity levels*, respectively. The analysis starts out discussing these key concepts of legal theory and then branches out to other uncharted consequences.

[10] *See* Cass R. Sunstein, *Informing America: Risk, Disclosure, and the First Amendment*, 20 FLA. ST. U. L. REV. 653 (1993) (advocating for "informational remedies" like disclosure). *But see* Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647 (2011) (detailing the shortcomings of disclosure remedies).

[11] *See* Herb Weisbaum, *The Total Cost of a Data Breach—Including Lost Business—Keeps Growing*, NBC NEWS (July 30, 2018, 2:15 PM), https://www.nbcnews.com/business/consumer/total-cost-data-breach-including-lost-business-keeps-growing-n895826 [https://perma.cc/T9EJ-AF5G].

Section III.A demonstrates that data breach is often a product of bad luck and inherent leakiness.[12] As a result, whether a firm experiences a particular data breach is, in part, a feature of luck. While moral luck and the effects of luck in general are a common sticking point in tort and criminal law theory, the analysis is particularly complicated for data breach notification.

Section III.B contends that the data breach notification debate has overlooked another foundational inquiry in tort law—activity levels. Many theorists recognize that tort law regulates both duty of care (the precautions that a person must undertake) and activity levels (how often a person undertakes an activity).[13] Thus far, the debate on data breach notification has focused almost exclusively on regulating level of care (such as data security standards),[14] without appreciating the importance of activity levels. To that end, we examine how different activity levels—or opportunities for data breach—are both influenced and influence the effectiveness of data breach notification statutes. To do so, we also explore the proper and unique meaning of "activity level" in this context.

Part IV brings everything together. This Part returns to the justifications and examines how they are shaped by the novel analysis of unfairness/luck and activity levels. Then, building on these insights, it sets forth a blueprint for a more well-informed data breach notification statute.

Before proceeding, a final caveat is due. Breach notification schemes are a costly venture—with some more costly than others.[15] Some costs are one-time and direct, such as mailing out notices. Others are ongoing, such as maintaining a record of clients with updated contact information. And yet others are indirect, such as taxing the mental bandwidth of consumers with ongoing notices.[16] For the sake of this discussion, such costs are taken as a given, as it appears that breach notification schemes are here to stay. And while the costs of the different models vary, we refrain from speculating as to the differences in costs. We do not argue about whether breach notification is truly necessary. Instead, we assume that regulators will continue to implement breach notification laws and we make suggestions towards what an optimal breach notifications statute entails.

[12] *See generally* Dana K. Nelkin, *Moral Luck*, STAN. ENCYC. PHIL. (Apr. 19, 2019), https://plato.stanford.edu/entries/moral-luck/ [https://perma.cc/EA3Y-S5YF#toc] (discussing the philosophical literature of moral luck).

[13] *See* Jules Coleman, Scott Hershovitz & Gabriel Mendlow, *Theories of the Common Law of Torts*, STAN. ENCYC. PHIL. (Dec. 17, 2015), https://plato.stanford.edu/entries/tort-theories [https://perma.cc/K9KJ-GG8A] (discussing activity levels). The "activity level effect" and its relationship to efficiency for particular standards of liability was introduced by Steven Shavell and Mitchell Polinsky in 1980. Nuno Garoupa & Thomas S. Ulen, *The Economics of Activity Levels in Tort Liability and Regulation* 3 (Am. L. & Econ. Ass'n Ann. Meetings, Working Paper No. 132, 2008) (claiming that Shavell and Polinsky independently introduced the problem of activity levels in tort law). For the original papers that ushered in the activity level effect, see Steven Shavell, *Strict Liability Versus Negligence*, 9 J. LEGAL STUD. 1 (1980); A. Mitchell Polinsky, *Strict Liability vs. Negligence in a Market Setting*, 70 AM. ECON. REV. 363 (1980).

[14] *See* GDPR, *supra* note 2, at 16 (Recital 83), 51–52 (Article 32).

[15] Larry Ponemon, *What's New in the 2019 Cost of a Data Breach Report*, SEC. INTEL. (July 23, 2019), https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/ [https://perma.cc/KG8G-VTAH].

[16] *See* CATE, *supra* note 5, at 10 (discussing disclosure fatigue).

II. Breach Notification Laws: Practice and Theory

A. Overview of Breach Notification Rules

While breach notification requirement laws are abundant, they almost always follow a common template. In nearly every case, the statute identifies a set of "personal data" worthy of protection.[17] It then defines what forms of events constitute a "breach" and finally dictates a set of actions the breached party must undertake.[18]

Yet, as always, the devil is in the details. This seemingly simple framework calls for addressing an array of technical questions. While these questions are intellectually intriguing, they are also practically crucial, as different choices for these features correspond to different normative foundations undergirding these laws. The key questions a regulator/legislator must address are:

(1) *What forms of information should be included in the definition of "personal information" that breach notifications protect?* Here, the regulator may choose a broad definition of personal information or, instead, opt for a narrow list of particular types of information.[19]

(2) *What constitutes a breach, triggering the notification process?* Possible responses might include data extraction (where data is removed), data loss (where data is deleted), or data inaccessibility (where data or the system is made inaccessible for a period of time).[20]

(3) *Who must receive the notification?* Here, there are several possible options, such as (a) a governmental entity (which might be a privacy regulator, a law enforcement entity, or a sector-specific regulator, to note a few); (b) the relevant data subject whose data was exposed, or perhaps (c) the public at large, and within it, the media.[21]

Of course, more than one disclosure destination could be designated and required. Additionally, the regulator might require *specific information* to be included within the notifications.[22] The *content* of the different notifications will promote some justifications rather than others.[23]

(4) *How promptly a firm must comply with their disclosure obligations?* The law might set a blurry standard (such as one based on reasonableness) or a specific rule which might be based on hours, days or even weeks and months.

[17] *Id.* at 3; *see* FLA. STAT. ANN. § 501.171 (West 2020).

[18] ALISSA M. DOLAN, CONG. RSCH. SERV., R44326, DATA SECURITY AND BREACH NOTIFICATION LEGISLATION: SELECTED ISSUES 3 (2015).

[19] *See id.* at 7; MASS. GEN. LAWS ANN. ch. 93H, § 1 (West 2020).

[20] GDPR, *supra* note 2, at 34 (Article 4(12)); *see* N.Y. GEN. BUS. LAW § 899–aa (McKinney 2019).

[21] GDPR, *supra* note 2, at 52–53 (Articles 33–34) (mandating personal data breach notice to supervising authority and the data subject, respectively); *see* Schwartz & Janger, *supra* note 5, at 936 (discussing a business's obligation to post public notice of a data breach); BUS. § 899–aa.

[22] *See* CAL. CIV. CODE § 1798.82 (West 2020); 45 C.F.R. § 164.404(a)(2)(c) (2020).

[23] *See* Schwartz & Janger, *supra* note 5, at 956, 962–63.

(5) *What exceptions should be introduced to these requirements?* These might include the waiver of the notification requirement. For example, reporting requirements may be waived if the compromised data was encrypted, or more generally, disclosure may not be necessary if the chance of long-term damage to the data subjects are relatively low.[24] In addition, exceptions may allow firms to delay notification in specific situations (such as assisting law enforcement efforts).[25]

As discussed, there are a broad variety of notification statutes and regulations, presenting an array of responses to these. First, consider the balance between the definition of personal information (Question #1) and the definition of a breach (Question #2). Given its clarity, broad jurisdiction, and substantial fine structure, we will start with the EU's GDPR. The GDPR applies a very broad definition of "personal information," which includes numerous particular factors (such as location data, online identifiers, or factors specific to a natural person's physical or mental identity), as well as general language aiming to include information related to identifiable persons.[26] It also defines breaches broadly to include data destruction, loss, alteration, disclosure, or access to data.[27] Moreover, these actions could be either accidental or unlawful.[28]

In the U.S., data breach notification laws in most states have more lenient reporting obligations given their narrower approach to defining "personal information" and "breach." For example, in defining personal information, most states merely address information linking names to social security numbers, drivers' license number, or financial account information (such as bank account or credit card numbers).[29] California, however, includes a broad array of health data categories, as do other states such as Florida.[30] In addition, California includes usernames and passwords within the category of "personal information" subject to notification requirements.[31]

Additionally, most states employ a narrow definition of "breach" that requires "unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality or integrity of personal information."[32] Yet

[24] Winn, *supra* note 5, at 1145; *see* BUS. § 899–aa.

[25] Winn, *supra* note 5, at 1142; 2019 CA A.B. 1130 (allowing delayed notification if such would impede an ongoing investigation); *see* BUS. § 899–aa.

[26] GDPR, *supra* note 2, at 33 (Article 4(1)); *see also* EUROPEAN DATA PROT. BD., GUIDELINES: GUIDELINES 01/2021 ON EXAMPLES REGARDING DATA BREACH NOTIFICATION (Jan. 14, 2021), https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_en [https://perma.cc/W9KU-MTXU].

[27] GDPR, *supra* note 2, at 34 (Article 4(12)).

[28] *Id.*

[29] *See* Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH L.J. 449, 479 (2019) (recognizing that breach notification laws only cover "breach[es] of security" where "personal information" is compromised). *See generally* BAKERHOSTETLER, DATA BREACH CHARTS 2 (2018), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf [https://perma.cc/BB6T-LBSP] (noting the "standard definition[] of personal information").

[30] CAL. CIV. CODE § 1798.29(h)(2) (West 2020); FLA. STAT. ANN. § 501.171(1)(g)(1)(a)(IV) (West 2020).

[31] CIV. § 1798.29(g)(2).

[32] *See* BAKERHOSTETLER, *supra* note 29, at 2 (defining the common notions of breach).

a few states, such as Florida, employ a slightly broader definition, which includes mere access to the databases as sufficient for notification requirements.[33]

Breach notification laws provide a variety of responses for who must be notified (Question #3) and how quickly must they be notified (Question #4). For example, the GDPR employs an elaborate two-tiered notification scheme, distinguishing between two types of breaches.[34] For "regular" breaches, the breached entity must report the incident to the local data authority within seventy-two hours of learning that a breach occurred.[35] For breaches that are likely to result in a "high risk to the rights and freedoms of natural persons," the GDPR requires notifications to the affected data subjects "without undue delay."[36]

When notifications "involve disproportionate effort," however, they could be supplanted by a "public communication."[37] In all cases, the communication should include the "likely consequences" of the breach, mitigating measures taken or that can be taken, and the details of the relevant data protection office.[38] When reporting to the authorities, the information should also include detailed information regarding the scope of the attack (such as categories of data and number of individuals affected).[39]

In the U.S, various state laws offer different responses to these two questions. Most states require notifications directly to the individuals.[40] Yet some states require additional disclosures. Florida, for instance, requires reporting to the State Attorney General within thirty days if at least 500 people were affected.[41] In California, when health data is compromised, the Department of Health Services must be informed within fifteen days.[42] In Massachusetts, the firm must inform the Director of Consumer Affairs and Business Regulation (who might forward the information to other relevant entities).[43] Importantly, though, the timeframes under U.S. laws are also usually more lenient than the GDPR.[44]

Finally, regarding exceptions (Question #5), the GDPR states that notification to the data subjects is not required if the personal data compromised was

[33] *Id.* at 3 (describing how Florida employs a broader definition of breach than most other states).

[34] *Compare* GDPR, *supra* note 2, at 52 (Article 33) (requiring notification to the "supervisory authority"), *with id.* at 52–53 (Article 34) (requiring notification to data subjects when the breach "is likely to result in a high risk to the rights and freedoms of natural persons").

[35] *Id.* at 52 (Article 33(1)).

[36] *Id.* (Article 34(1)).

[37] *Id.* at 53 (Article 34(3)(c)).

[38] *Id.* at 52 (Article 33(3)(b)–(c)); *id.* at 53 (Article 34(2)).

[39] *Id.* at 52 (Article 33(3)(a)).

[40] *See e.g.*, CAL. CIV. CODE § 1798.29(a) (West 2020); MASS. GEN. LAWS ch. 93H § 1 (West 2020); MICH. COMP. LAWS ANN. § 445.72 (West 2020).

[41] FLA. STAT. ANN. § 501.171(3)(a) (West 2020).

[42] CIV. § 1798.29.

[43] MASS. GEN. LAWS ch. 93H § 1 (West 2020).

[44] *See generally* PERKINS COIE, SECURITY BREACH NOTIFICATION CHART (June 2019), https://www.perkinscoie.com/images/content/2/2/v4/220987/Security-Breach-Notification-Law-Chart-June-2019.pdf [https://perma.cc/WS5R-L5MB] (outlining the notification deadline for every state and demonstrating that many states have 45–day reporting periods).

rendered "unintelligible" to unauthorized parties (for instance, using encryption)[45] or if steps were taken to ensure that the high risks to the subjects are "no longer likely" to materialize.[46] Similarly, various U.S. states offer "encryption" based exceptions as well (such as Florida, California and Massachusetts).[47]

The different responses given by different regulators are perplexing and seems to reflect an almost random choice. In some instances, that might indeed be the case. However, every design choice will have a substantial impact on the scheme's outcome, impact, and success, as well as other exogenous effects.[48] Therefore, the overall design choices *must* reflect clear policy preferences regarding the objectives of breach notification laws, their specific justifications, and their possible effects. We now turn to address the objectives of breach notification, leaving an analysis of its effects for the next Part.

B. The Normative Justifications for Data Breach Notifications

This Section undertakes a descriptive and normative analysis of the justifications for data breach notification statutes. This taxonomic work provides the groundwork for rigorously assessing each particular justification and its implications. As we will now see, data breach notification statutes derive their normative foundations from an eclectic array of sources, drawing from different regulatory design strategies across an assortment of legal fields.[49] Some of the justifications are instrumental; namely, they recommend breach notification policies to promote other, secondary objectives they find important.[50] Others are foundational, as they consider reporting information regarding the breach a primary, independent objective of its own.[51]

At the most intuitive level, breach notification requirements and laws could be seen as part of broader regulatory schemes which promote disclosure as a compromise between rigorous intervention and inaction.[52] Yet merely promoting the disclosure objective is an insufficient response, especially given the harsh critiques disclosure regulation currently face, which question its effectiveness.[53] This leads us to seek out specific normative goals which breach notifications strive to promote. We focus on four normative values: deterrence, mitigation, information forcing, and autonomy/restorative justice.

[45] GDPR, *supra* note 2, at 53 (Article 34(3)(a)).

[46] *Id.* (Article 34(3)(b)).

[47] *See generally* CYBERSECURITY TEAM, FOLEY & LARDNER LLP, STATE DATA BREACH NOTIFICATION LAWS, https://www.foley.com/en/insights/publications/2019/01/-/media/files/insights/publications/2020/20mc25837-data-breach-chart-010920.pdf (last visited Mar. 27, 2021) [https://perma.cc/75FU-BFV5].

[48] *See* Winn, *supra* note 5, at 1139–40.

[49] Jane Winn suggests that the legislative ancestors of data breach notification laws are "smart regulation" as well as pieces of environmental legislation that mandates disclosure in an array of cases. *See id.* at 1135–43.

[50] *See id.* at 1139–40.

[51] *See id.* at 1160.

[52] Cass Sunstein coined the phrase "regulation through disclosure." *See* Cass R. Sunstein, *Informational Regulation and Informational Standing: Akins and Beyond*, 147 U. PA. L. REV. 613, 613 (1999) (explaining the notion of "regulation through disclosure"). For a similar argument, see CATE, *supra* note 5, at 3.

[53] *See, e.g.*, OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 3 (2014).

As we will now demonstrate, design choices within a specific data breach notification statute support or undermine these justifications. For example, deterrence is better served by broad public disclosure, while mitigation might be best served by anonymous disclosures to regulatory agencies.[54] We detail several other tensions between these normative goals and how this tension is reflected in possible design choices.

1. Deterrence

Notification statutes can be justified by arguing that they will lead to limiting socially undesirable outcomes—that is, inadequate data security measures, breaches of personal data and, in many cases, distribution of leaked data.[55] Deterring bad data security outcomes follows from creating a breach notification scheme that incentivizes firms to implement adequate security practices, which limit the likelihood of breaches. In other words, the underlying assumption of the "deterrence" justification is that firms will invest in adequate security measures *ex ante* because they strive to avoid the reputational penalty and other negative outcomes that follow disclosing a breach *ex post*.[56]

The potential effects of breach notifications should not be underestimated. Firms face real consequences from reputational effects, which may encourage consumers, investors, vendors, and even employees to take their business, capital, and talent elsewhere, resulting in potential lost profits for the firm.[57] Reputational effects may also lead to a corresponding (albeit, often short-lived) drop in the firm's stock price, costing shareholders value and generating negative sentiment.[58] Finally, notifications might bring about the unwanted attention of regulators and legislators, who might consider costly measures against the relevant firm, or reports by the media which lead to ripple effects of the various forms.[59] Similarly, additional attention would also require firms to engage in an internal process of self-reflection regarding the causes of these breaches.

[54] *See* Schwartz & Janger, *supra* note 5, at 932–35.

[55] *See id.* at 934 ("[T]his Article has described the reputational sanction that a breach notice causes as essentially forward-looking; it seeks to influence consumers to shop for data security based on information about security incidents and to encourage firms to safeguard their data to avoid reputational sanction.").

[56] *See id.* at 934–36; *see also* Kilovaty, *supra* note 29, at 469–70; JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRAINTS OF INFORMATIONAL CAPITALISM 102–03 (2019) (noting the deterring power of breach notification yet explaining that the extent of such power is debated). Cohen further notes that breach notification laws are weak and that not much can be done in terms of generating actual deterrence. *Id.*

[57] COHEN, *supra* note 56, at 77.

[58] Note: the empirical evidence demonstrates that data breach incidents reduce stock price only momentarily, with the value eventually recovering. *See* Romanosky et al., *supra* note 5, at 261 (providing a literature review of the relationship between data breaches and stock price); *see also* Sergei Klebnikov*, Companies with Security Fails Don't See Their Stocks Drop as Much, According To Report,* FORBES (Nov. 6, 2019, 3:42 PM), https://www.forbes.com/sites/sergeiklebnikov/2019/11/06/companies-with-security-fails-dont-see-their-stocks-drop-as-much-according-to-report/ [https://perma.cc/66W6-XC4G].

[59] *See* Schwartz & Janger, *supra* note 5, at 955 ("[Breach notification] allows consumers, the media, and legislators to hear a story about data security gone awry. Forced to convey a certain kind of particularized bad news, the breached entity becomes a focal point for consumer resentment, media attention, and legislative scrutiny.").

The effectiveness of deterrence depends on the specific design of the breach notification law.[60] For a maximum deterrent effect, the law must be tailored to maximize the reputational harm that notification will cause.[61] Therefore, the more notifications, the better.[62] This means that "information" and "breach" (as addressed in Questions #1 and #2) should be defined as broadly as possible. Moreover, exceptions to notification (Question #5) should be defined as narrowly as possible to enhance the specter of reputational harm and thus incentivize adequate security practices. Recognize, however, that focusing on deterrence allows for some leniency regarding other design questions. For instance, the notification timeframe (Question #4) need not be urgent and strict. The reputation harm will eventually unfold, sooner or later, and urgent notification will not necessarily make a difference.

Promoting deterrence also requires a nuanced strategy regarding both the recipients and the content of the breach notification (Question #3).[63] In terms of content, the notices should detail potential damage and information about the firm's carelessness, which would enhance the reputational effect. In terms of recipients, the exposure should be as broad as possible so as to possibly catch the public's eye. For firms fearing regulatory and legislative repercussions, disclosures to designated regulators might generate substantial deterrence as well. As a case in point, consider Florida's requirement to report breaches affecting more than 500 Florida residents to the state AG office.[64]

Beyond specific regulatory choices for the breach notification law itself, effective deterrence would depend on the background legal regime.[65] More specifically, deterrent effects will be the strongest when reputational sanctions operate in a legal regime that promotes broad class action rights[66] (ideally to both customers and shareholders).[67] For instance, rules that leniently grant standing

[60] *See, e.g.*, *id.*

[61] *Id.* at 935–36, 970.

[62] We are setting aside, for the moment, the possible prospect of over-deterrence, which we will address in our analysis of activity levels. *See infra* note 376.

[63] *See* Schwartz & Janger, *supra* note 5, at 933, 959.

[64] *See* FLA. STAT. ANN. § 501.171(3)(a) (West 2020); BAKERHOSTETLER, *supra* note 29, at 18.

[65] *See* CATE, *supra* note 5, at 1; BEN-SHAHAR & SCHNEIDER, *supra* note 53, at 745.

[66] The E.U currently does not enable class actions for violations of data protection laws, yet this is destined to change in the near future. *See* ANU BRADFORD, THE BRUSSELS EFFECT 43 (2020); *see also EU Consumers Will Soon Be Able to Defend Their Rights Collectively*, NEWS: EUROPEAN PARLIAMENT (Nov. 24, 2020, 9:33 AM), https://www.europarl.europa.eu/news/en/press-room/20201120IPR92116/eu-consumers-will-soon-be-able-to-defend-their-rights-collectively [https://perma.cc/92AP-ACRV].

[67] Lawsuits by shareholders following substantial breaches of data security is a growing trend in the U.S. following the Equifax debacle. For a discussion of this shareholder's settlement, see Kevin M. LaCroix, *Equifax Data Breach-Related Securities Suit Settled for $149 Million*, D&O DIARY (Feb. 17, 2020), https://www.dandodiary.com/2020/02/articles/securities-litigation/equifax-data-breach-related-securities-suit-settled-for-149-million/ [https://perma.cc/RW67-DXNP]. For a somewhat critical view of this dynamic, see Matt Levine, *Dystopian Future Securities Fraud*, BLOOMBERG OP. (Jan. 5, 2021, 10:59 AM), https://www.bloomberg.com/opinion/articles/2021-01-05/dystopian-future-securities-fraud [https://perma.cc/Y4VR-4766]. Note that these suites, under current case law, might only unfold in a limited set of situations.

to a broad class of plaintiffs and award generous damages supplemented by regulatory fines will produce a significant deterrent effect.[68] At bottom, the deterrent effect of breach notification is stronger when these notices also work in service of broader legal liability or regulatory action.[69]

Yet considering the appropriate design to maximize deterrence introduces a complication. Structuring breach notification laws to promote deterrence inevitably leads firms to act strategically, often to the detriment of data subjects.[70] As Schwartz and Janger explain, the possibility of extensive reputational harms will encourage firms to underreport breaches, especially when there is a colorable case that disclosure is not required.[71] In other words, when breach notification laws are driven by deterrence, firms will tend to under-report—particularly in cases where there is no external reporting requirement. This, in turn, will adversely affect individuals who remain uninformed about a breach and unable to take mitigating measures.[72]

On the other hand, a notification regime that is focused on mitigation strategies could allow firms to anonymously report breach incidents.[73] By insulating firms from possible reputational harm, they will have fewer reasons to prefer concealing, rather than disclosing, breaches.[74] However, one can speculate as to whether the specter of harsh fines and other repercussions will sufficiently deter firms from under-reporting. Nonetheless, it is fair to assume that maximizing deterrence might conflict with other objectives, such as mitigation.

Breach notification models premised on deterrence face several viable critiques. First, the reputational effects (and, by extension, deterrent effects) of disclosure are unclear and unpredictable—and in many cases may be ineffective.[75] This is because the public—and its elected representatives and unelected bureaucrats—may not respond to information about breaches and, in addition, the firm's public relations team might be able to explain away the breach. Indeed, a recent RAND survey indicated that just over 10% of the public opted to leave a service provider or vendor after learning the company experienced a breach and that personal data was compromised.[76] Therefore, firms may learn over time that the threat of reputational harm is overstated and may fail to take proper security measures. The "price" of such breaches in terms of lost clients and business will, in some contexts, prove to be limited. For example, it is unclear if air travelers

[68] *See, e.g.*, GDPR, *supra* note 2, at 53 (Article 83(4)(a)) (listing the extensive fines the breach of the relevant provisions might entail).

[69] *See* CATE, *supra* note 5, at 1; BEN-SHAHAR & SCHNEIDER, *supra* note 53, at 971.

[70] *See* Schwartz & Janger, *supra* note 5, at 937, 959.

[71] *Id.* at 937 (explaining that "the threat of reputational sanction may serve to chill a company's willingness to inform about a security breach"); *see also* CATE, *supra* note 5, at 14.

[72] *See* CATE, *supra* note 5, at 13–14.

[73] Schwartz & Janger, *supra* note 5, at 937 (discussing a breach notification model that shields the identity of the breached firm).

[74] *Id.* at 937, 945.

[75] We discuss this issue more fully below. *See infra* notes 176–80 and accompanying text.

[76] LILLIAN ABLON, PAUL HEATON, DIANA CATHERIN LAVERY & SASHA ROMANOSKY, RAND CORP., CONSUMER ATTITUDES TOWARD DATA BREACH NOTIFICATION AND LOSS OF PERSONAL INFORMATION xi (2016).

will avoid flying British Airways following negative publicity over a reported breach.

Second, even if notifications do create deterrent effects, they are only a second-best option. Deterrence would be more effectively achieved by direct measures, such as regulatory fines, rather than applying an indirect measure with unclear outcomes and substantial costs.[77] There are viable reasons, however, to rely on this indirect measure to encourage data holders to improve their security practices. One drawback of fines is that they require a lengthy procedure, including opportunities for appeal.[78] Nonetheless, notifications may still be best suited to merely supplement a fine system or replace a dysfunctional fine system in order to encourage proper security measures.

Third, the fear of the reputational harm from disclosures (as well as fines, lawsuits, and additional fallout from disclosure) may incentivize firms to take questionable, socially undesirable steps (beyond under-reporting) in the case of ransomware attacks. Ransomware attacks are instances in which an attacker successfully locks users out of their system and demands a payment in order to restore access.[79] While there are many variations of such attacks, they often do not involve the actual theft of the firms' data but merely the loss of access to it.[80]

In some cases, ransomware attacks in jurisdictions with breach notification statutes create perverse incentives.[81] Notification requirements potentially incentivize firms to respond by paying the attacker and quickly ending the event.[82] This is because the initial steps of the successful ransomware event might fail to trigger notification requirements, as access has not been substantially impaired and hackers did not access personal data (yet merely lock out users while the hackers hold the keys to access it again). Yet notification might nonetheless be mandated if payment is not immediately made because this might result in loss of users' accessibility to their data.[83] Accessibility might also be lost if the firm engages in an extensive backup process or negotiation with the hacker – all outcomes which will not follow if the payment is quickly made in full.[84] Even if the

[77] For a discussion of sanctions and fines for security breaches, see *infra* note 209 and accompanying text.

[78] *See* CATE, *supra* note 5, at 9.

[79] James A. Sherer, Melinda L. McLellan, Emily R. Fedeles & Nicole L. Sterling, *Ransomware—Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web*, 23 RICH. J.L. & TECH. 1, 1, 6–7 (2017).

[80] *Id.* at 1, 5; *see also* Josh Fruhlinger, *Ransomware Explained: How It Works and How to Remove It*, CSO ONLINE (June 19, 2020, 3:00 AM), https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html [https://perma.cc/P953-9GMQ] (explaining the basic mechanics of a ransomware attack).

[81] *See* CATE, *supra* note 5, at 14; Asaf Lubin, The Insurability of Cyber Risk 21, 51 (2019) (unpublished manuscript) (on file with Berkman Klein Cent. for Internet & Soc'y).

[82] *See* Fruhlinger, *supra* note 80; CATE, *supra* note 5, at 22.

[83] For sources and an extensive discussion of this issue, see Lubin, *supra* note 81, at 51 n.226.

[84] For a possible E.U. position regarding this matter, see The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Guidelines on Personal Data Breach Notification Under Regulation 2016/679*, 31, U.N. Doc. 18/EN (Oct. 3, 2017), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 [https://perma.cc/2B2C-UWMT]. For an updated position, see EUROPEAN DATA PROT. BD., *supra* note 26, at 7–12 (explaining how loss of data availability could require notification to the regulator, and at times even to the data subjects and the broader public).

attack triggers notification requirements, a quick payment isolates the event and keeps it off the books. The resulting incentive structure, which strongly favors payment, is undesirable because it will incentivize hackers to attack again and unjustly enriches these bad actors.[85]

Notification models which do not focus on deterrence minimize the possibility of this outcome.[86] If the fallout from a breach is not severe, firms will not be pressured to comply with the hackers' demands.[87] The complications posed by ransomware are merely one example of the undesirable outcomes which might follow from indirect regulatory schemes, particularly in rapidly changing areas such as cybersecurity.

Before turning our attention to mitigation, it is worth noting that a similar form of justification for notification rules could be premised on the Kantian notion of retribution. Here, we refer to the fundamental notion that the firms should be punished for the wrongs they inflicted on the data subjects, and this punishment is reflected in the harms that follow from the notification process.[88] Since the outcomes of analyzing this justification, as well as its potential pitfalls and critiques, greatly resemble the broader notion of deterrence, we choose to refrain from elaborating on this notion separately.

2. Mitigation

Alongside deterrence, data breach notification statutes can provide an important opportunity to mitigate possible harms from breach incidents. Rather than limiting the number of breaches, these statutes should be understood as a measure which focuses on informing consumers that their data (and thus a segment of their digital lives) is potentially at risk. Therefore, these laws empower citizens to take proactive steps to limit the negative effects of information leakage.[89]

Data breaches can cause significant harm.[90] Awareness of such breaches might potentially enable mitigation.[91] Some of these mitigation measures and

[85] *See, e.g.*, Jessica Davis, *Ransomware Rising, but Where Are All the Breach Reports?*, HEALTHCARE IT NEWS (Mar. 20, 2017, 8:50 AM), https://www.healthcareitnews.com/news/ransomware-rising-where-are-all-breach-reports [https://perma.cc/6N4U-B4PS].

[86] *See* Schwartz & Janger, *supra* note 5, at 959–70; CATE, *supra* note 5, at 14.

[87] *See* CATE, *supra* note 5, at 14.

[88] *See* Alec Walen, *Retributive Justice*, STAN. ENCYC. PHIL. (July 31, 2020), https://plato.stanford.edu/entries/justice-retributive/ [https://perma.cc/7ERH-JEYG] (discussing retributive justice concepts and stating that "those who commit certain kinds of wrongful acts, paradigmatically serious crimes, morally deserve to suffer a proportionate punishment").

[89] *See* Schwartz & Janger, *supra* note 5, at 937 ("Notification about security breaches also serves [an] ex post function of mitigation. It seeks to permit consumers and other data processing institutions to protect themselves from harm caused by a data spill that has already occurred."); *see also* Kilovaty *supra* note 29, at 494–97.

[90] Tiffany Hsu, *Data Breach Victims Talk of Initial Terror, Then Vigilance*, N.Y. TIMES (Sept. 9, 2017), https://www.nytimes.com/2017/09/09/business/equifax-data-breach-identity-theft-victims.html [https://perma.cc/D55C-F6ZN] ("The consequences of cyberattacks can be devastating and take years to untangle, at great financial and personal cost.").

[91] *See, e.g.*, *id.*

strategies have been developed recently, given the rapid spread of breach incidents.[92] Much of the mitigation discussion focuses on the fear of identity theft and its consequences for the individual's finances and credit rating.[93] For instance, when individuals are aware that their information is potentially compromised, they can rely on credit monitoring services that provide alerts about potential usage of their personal information.[94] Breach subjects might also "lock" or "freeze"[95] their credit reports—which prevents using their information to open fraudulent accounts.[96] In addition, they might exercise additional vigilance and caution by frequently examining their financial statements and other financial information.[97]

Other potential mitigation measures might vary depending on the nature of the breach and type of information compromised. For example, when notified about leaked credit card or bank account information, affected individuals can cancel their credit cards and open new bank accounts.[98] Even a social security number could be changed in extreme circumstances.[99] On a more pragmatic level, when individuals are notified that their username and password were compromised, they will know to change their password on other websites in case they (foolishly) chose similar passwords for multiple platforms.[100]

The notion of promoting mitigation is most likely a driving force in the creation of all data breach notification statutes. At least on a rhetorical level, mitigation is often cited as the justification for the notification framework's existence.[101] The EU's GDPR serves as a case in point. In its explanatory comments in Recital 86,[102] the GDPR notes that information regarding the breach should be communicated to the data subjects so that they may "take the necessary precautions." In addition, Recital 85 details several harms that result from data breaches—such as loss of control, limitation of rights, discrimination, identity theft, reversal of pseudonymization, and damage to reputation—which might afflict individuals if "not addressed in an appropriate and timely manner."[103] Thus,

[92] *See, e.g.*, *id.*

[93] *Id.* (describing identity theft in the wake of a data breach).

[94] *See Credit Monitoring Services: How Do They Work?*, NORTON, https://us.norton.com/internetsecurity-id-theft-credit-monitoring-services-how-do-they-work.html (last visited Mar. 27, 2021) [https://perma.cc/89XB-7UZ9].

[95] For an explanation as to the difference between "lock" and "freeze" services, see Octavio Blanco, *Why a Free Credit Freeze Is Better Than a Credit Lock*, CONSUMER REPS. (Sept. 21, 2018), https://www.consumerreports.org/credit-protection-monitoring/why-a-free-credit-freeze-is-better-than-a-credit-lock/ [https://perma.cc/GJ47-Z6YJ].

[96] For the nature of locking service provided by Equifax, see EQUIFAX, https://www.equifax.com/personal/products/credit/credit-lock-alert/ (last visited Mar. 27, 2021) [https://perma.cc/UMH2-UHL9].

[97] *See* Daniel J. Solove & Danielle K. Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 764 (2018).

[98] *Id.* at 757.

[99] *Frequently Asked Questions: Can I Change My Social Security Number?*, SOC. SEC. ADMIN. (Nov. 29, 2019), https://faq.ssa.gov/en-US/Topic/article/KA-02220 [https://perma.cc/39J5-V9RN].

[100] *See* CATE, *supra* note 5, at 6.

[101] *Id.* at 7.

[102] GDPR, *supra* note 2, at 17 (Recital 86).

[103] *Id.*

the unstated assumption behind the GDPR's breach notification provision is that data breach harms can be mitigated if they are addressed quickly.

Mitigation is often effectively pursued in tandem with deterrence.[104] Or rather, breach notification works in service of deterrence and mitigation at the same time. This means that advancing both deterrence and mitigation will lead to similar responses to our design questions. Similar to deterrence, mitigation would be advanced by broad definitions of both "personal information" and "breaches" (Questions #1 and #2). And, as with deterrence, it would benefit from broad dissemination of information regarding the breach (Question #3). To demonstrate, consider again the California data breach notification statute. California requires public disclosure which leads to reputational sanctions and deterrence.[105] Public disclosure also facilitates mitigation efforts because potentially affected individuals can take steps to minimize their exposure risks.[106]

Yet achieving mitigation often calls for a nuanced response to at least some of the regulatory design questions and, further, these might not be the responses that optimally enhance deterrence. First, notification recipients must include the affected individuals directly, in order to ensure that those impacted by the breach will take action to remedy potential harms.[107] While U.S. breach notification schemes almost always require notifying impacted individuals, the GDPR only requires notification when the breach results in a "high risk," thus at times leaving data subjects out of the loop.[108]

In addition, some U.S. states require notification to other entities that might assist with mitigation. For instance, Florida requires notifying credit agencies.[109] These additional notifications will arguably assist individuals, as the credit agencies will be alerted to the chance of wrongful reporting concerning impacted individuals. Importantly, however, these disclosures do not necessarily enhance deterrence.[110]

Second, consider requirements regarding the notification's language. In contrast to notifications that maximize deterrence, which might emphasize the firm's wrongdoing, breach notifications that promote mitigation should focus on how people can protect themselves from downstream harms. In the U.S., several states have designed their notification requirements to do just that. For instance, New York's amended breach notification law requires providing information about state agencies that can help data subjects protect themselves from identity

[104] Schwartz & Janger, *supra* note 5, at 934.

[105] CAL. CIV. CODE § 1798.29(a) (West 2020).

[106] Schwartz & Janger, *supra* note 5, at 936.

[107] *Id.* at 937.

[108] GDPR, *supra* note 2, at 17 (Recital 86).

[109] FLA. STAT. ANN. § 501.171(5) (West 2020)

[110] Schwartz & Janger, *supra* note 5, at 941.

theft and related harms.[111] Similarly, California requires providing contact information for credit agencies in some cases.[112] And finally, the amended Massachusetts law requires that breach notifications inform affected individuals that they can request a credit freeze, while also emphasizing that this and similar services are free.[113]

The GDPR appears to move in a similar direction yet uses broader language to signal its intentions and achieve these objectives. Article 34 requires that disclosures include a statement about the likely consequences of a breach and the importance of taking steps to mitigate these harms.[114] Similarly, Recital 86[115] recommends communicating specific mitigative steps to affected parties. As discussed, the specific and somewhat limited information needed to achieve effective mitigation has even led Schwartz and Janger to recommend anonymous notifications which do not include the name of the breached firm, but merely instruct the affected individual about potential steps to mitigate harms.[116]

Third, consider response times (Question #4). Effective mitigation requires a tight reporting schedule.[117] The fourteen- to thirty-day time period allotted in most U.S. laws (which might fit the deterrence objective just fine) might be too lenient.[118] California's requirement to provide notice "in the most expedient time possible" seems more effective at promoting mitigation.[119] Similarly, the GDPR's requirement to inform affected individuals "without undue delay" is focused on providing information to impacted individuals quickly so they can protect themselves.[120] Finally, when focusing on mitigation, breach notification requirements could include broad exceptions and exemptions (Question #5). Indeed, when the risk of harm is limited and no mitigation would be needed, notifications might be suspended (even though a lapse in security did occur and publication would enhance deterrence).

On its face, advancing mitigation seems to be an unalloyed good with few critics. Yet the prospect of mitigation is not without problems. The effectiveness of mitigation as a foundation for data breach notification relies on a couple of contested assumptions. First, mitigation depends on whether individuals can, in

[111] N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019).

[112] Note that California's breach notification law goes even further to require, in specific cases, that the firm offer those whose data was breached some form of mitigation service for twelve months. CAL. CIV. CODE § 1798.29 (West 2020). As this issue goes beyond the notion of actual disclosures, it will not be further discussed.

[113] Off. Att'y Gen. Maura Healey, *Reporting Data Breaches to Affected Residents*, MASS.GOV, https://www.mass.gov/service-details/reporting-data-breaches-to-affected-residents (last visited Mar. 27, 2021) [https://perma.cc/3UNS-BSEU].

[114] GDPR, *supra* note 2, at 53 (Article 34(2)).

[115] *Id.* at 17 (Recital 86).

[116] Schwartz & Janger, *supra* note 5, at 916.

[117] *Id.* at 960.

[118] *See* BAKERHOSTETLER, *supra* note 29, at 23–27.

[119] CAL. CIV. CODE § 1798.29(a) (West 2020).

[120] See GDPR, *supra* note 2, at 52 (Article 34(1)). While the Article does not set a clear timeframe, the seventy-two-hour time frame for reporting to the government indicates the overall expectation of swift responses. *Id.*

fact, take effective steps to protect themselves after a data breach.[121] This is debatable. Empirically, it is unclear whether (or which) steps an individual can take that will be effective.[122] While applying credit monitoring or credit locking are important and might assist in mitigating harm, one might question the importance and significance of receiving a large number of notifications, especially given the fact that they are not costless.[123]

There are several reasons for this skepticism. First, applying credit freezes, locks (at least when credit requests are not anticipated), and monitoring are important practices that should be followed at all times by everyone.[124] And indeed, hopefully this practice becomes commonplace (in part thanks to breach notifications).[125] Once the public begins exercising these practices regularly, the added value of every marginal notification sharply decreases.[126] This same logic holds for notifications individuals receive after already being notified of previous breaches, particularly if the individual has already undertaken important steps towards mitigation (a very likely scenario given the number of existing databases our data rests at and the vast number of reported breaches).[127]

Another context in which the effectiveness of mitigation is contested are cases where a breach occurred in the past but is only revealed much later. Disclosures that occur after substantial delays will not provide for meaningful mitigation because, in all likelihood (but not always, as we discuss below), mitigation at this point would be an exercise in futility; the harms would have most likely already occurred, or the threat of harm from the breach has already dissipated.[128]

Let us now consider the opposite scenario. Many mitigation strategies focus on avoiding harm that follows in the immediate aftermath of the data breach.[129] As noted above, that often is the case, yet not always. Criminals purchasing some forms of stolen personal data on black markets might choose to wait, using it after the credit monitoring subscriptions and the data subjects' attention spans have long expired.[130]

Finally, other concerns are significantly harder to mitigate. For instance, uses of leaked data to discriminate against individuals or the psychological harms

[121] Schwartz & Janger, *supra* note 5, at 918.

[122] There is some limited evidence that data breach notification reduces the probability of identity theft. *See* Romanosky et al., *supra* note 5, at 260. Romanosky et al., however, also claim that there is little existing empirical work on the efficacy of these laws. *Id.* at 256.

[123] *See* CATE, *supra* note 5, at 12.

[124] *Id.* at 7.

[125] This already might be occurring. *See* Brian Krebs, *Survey: Americans Spent $1.4B on Credit Freeze Fees in Wake of Equifax Breach*, KREBS ON SEC. (Mar. 22, 2018, 10:08 AM), https://krebsonsecurity.com/2018/03/survey-americans-spent-1-4b-on-credit-freeze-fees-in-wake-of-equifax-breach/ [https://perma.cc/AW8Q-E3UT] (indicating that 20% of Americans froze their credit cards after the Equifax breach).

[126] *Id.*

[127] Schwartz & Janger, *supra* note 5, at 946.

[128] *See* Hailey Fuchs, *A Decade Later, Yale Discovers Major Data Breach*, YALE DAILY NEWS (Aug 2, 2018, 10:58 PM), https://yaledailynews.com/blog/2018/08/02/a-decade-later-yale-discovers-major-data-breach/ [https://perma.cc/X833-JJ5Z] (noting an instance where a breach was disclosed after a significant delay).

[129] Schwartz & Janger, *supra* note 5, at 918.

[130] Note that some information might "expire," such as credit card numbers, addresses, and other personal details, and therefore, substantial delays in using stolen personal data might render it almost useless.

from feelings of losing control over personal information have no easy solution.[131] The fact that an individual knows they might occur does not really equip her with any effective antidote.

Even considering these arguments, one might still argue that notifications are still important to achieve whatever mitigation is possible.[132] Yet adhering to notification requirements comes at a cost which must be considered. Beyond actual out-of-pocket costs (which this Article chooses to set aside) the constant flow of disclosure notices may actually cause people stress and anxiety.[133] It might also lead individuals to disengage from technology.[134] Or, alternatively, additional disclosures may have the opposite effect on other individuals (with a different set of attributes). The constant barrage of notifications may lead individuals to disregard security notices and security risks generally, thus rendering notices largely ineffective (what some have called "data breach fatigue").[135] For these reasons, the capacity for breach notification to promote mitigation is limited. Therefore, balancing mitigation against competing interests (such as deterrence) or the costs of implementing breach notification itself is challenging.

Our discussion regarding the limits of mitigation comes with two caveats. First, there are a few instances in which mitigation is simple and effective, and therefore should be facilitated and promoted. When usernames and passwords are leaked or stolen from one website, informed individuals can quickly change similar passwords they might have chosen for other usernames and platforms. Indeed, California's law requires that breach notifications recommend this practice.[136]

Second, the utility derived from the ability to mitigate the damages of security breaches is not equally distributed. Some individuals have a greater interest in taking mitigative steps as well as a greater ability to do so successfully.[137] This might be a function of the individual's interest or sophistication. Clearly, this tendency will not be distributed equally across the population of data subjects. Therefore, providing the ability to mitigate would most likely lead to an uneven spread of benefits throughout society, and the resulting fairness concerns require further analysis.[138] On the other hand, the fact that only a portion of the population will be interested and able to mitigate effectively might lead to a more

[131] *See* Solove & Citron, *supra* note 97, at 745 (describing the psychological costs of data breach).

[132] *See* Ponemon, *supra* note 15 and accompanying text.

[133] *See* Solove & Citron, *supra* note 97, at 745.

[134] *Id.*

[135] Andrew Bolson, *If Not All Data Breaches Are Created Equal, Why Are All Data Breach Notifications Treated the Same?*, INT'L ASS'N PRIV. PROS. (Oct. 28, 2014), https://iapp.org/news/a/if-not-all-data-breaches-are-created-equal-why-are-all-data-breach-notifications-treated-the-same/ [https://perma.cc/5LMR-27ZZ] (detailing a study that suggests a high rate of disclosure fatigue); *see also* Schwartz & Janger, *supra* note 5, at 916 (discussing the phenomenon of disclosure fatigue).

[136] CAL. CIV. CODE § 1798.29(i)(4) (West 2020).

[137] *See* Jane Bambauer & Tal Zarsky, *The Algorithm Game*, 94 NOTRE DAME L. REV. 1, 28–29 (2018).

[138] For a similar analytical move and discussion, see *id.* at 28.

nuanced and tailored form of disclosure (which would balance costs and other potential drawbacks).[139]

3. *Information Forcing*

Information forcing is a less obvious value of and justification for data breach notification statutes. While some commentators have recognized the benefits of additional information flows that result from breach notifications, earlier discussions have failed to suggest information forcing as a primary goal of data breach notification laws.[140]

The benefits of information forcing operate on two different time horizons: short and long.[141] The immediate benefits of the information flows from data breach notification include recognizing patterns in attacks that can be used to identify other potential targets before they are compromised.[142] Information forcing also adds benefits on a longer time horizon.[143] Here, aggregate patterns help security experts and regulators improve security standards and other guidelines, as well as provide greater insight about the risks to cybersecurity and how they might be effectively pooled.[144] Naturally, both of these objectives require a different regulatory design.

Breach notifications in the wake of successful cyberattacks can generate immediate and short-term benefits. The information flows that result from breach disclosures can enable updating potential targets about looming attacks and security vulnerabilities.[145] For instance, if adversaries are particularly interested in certain targets, possibly because of the data or position that they hold, firms can learn—via pooling—that they may be at risk because other firms in the same industry (such as airlines or hotel chains) have been attacked.[146] Similarly, if firms are aware that entities in similar sectors and using similar systems are vulnerable given a novel attack vector, they could try and apply defensive measures (such as applying missed patches or encrypting data) as well as exercise greater caution.

[139] Ariel Porat & Lior Jacob Strahilevitz, *Personalizing Default Rules and Disclosure with Big Data*, 112 MICH. L. REV. 1417, 1470–76 (2014) (proposing a new method of disclosure that is tailored to smaller subpopulations).

[140] *See* Schwartz & Janger, *supra* note 5, at 955 (detailing how data breach notification can provide information to journalists).

[141] *See id.* at 971.

[142] *See id.*

[143] *See id.*

[144] *See id.*; Porat & Strahilevitz, *supra* note 139, at 1439.

[145] Information about targeting particular industries or companies is already shared. For instance, Airbus was the target of several hacking attempts. Zak Doffman, *Chinese Hackers Suspected of Airbus Cyberattacks—A350 Among its Targets*, FORBES (Sept. 26, 2019, 10:16 AM), https://www.forbes.com/sites/zakdoffman/2019/09/26/china-suspected-of-multiple-airbus-cyberattacksa350-among-targets/#4cdbfe8de630 [https://perma.cc/HH9Q-4L6Q]. In the wake of these attacks, Airbus notified its subcontractors about these attempts and took the necessary steps to make sure that they were secure as well. *Id.*

[146] *See* sources cited *supra* note 145.

In addition, breach notifications can generate intermediate and long-term benefits. Many of the benefits of breach-related information pooling are particular to the idiosyncrasies of cybersecurity. In cybersecurity, unlike other fields, the standards of reasonable security measures are rapidly evolving both technically and legally.[147] Like other repeat games, adversaries introduce new tactics and security experts respond to these new threat vectors.[148] Therefore, security experts are constantly learning about adversarial methods and inherent weaknesses in security systems. In response, security experts update their protocols and practices.[149] A pool of cyber-security related information might generate a "knowledge commons" (which does not imply the information is available to all) to facilitate research and progress in this unique context.[150]

Information pooling about the sources of breach, the strategies that were used to breach the systems, and information about the adversaries, allows both firms and security consultants to perform these updates. The standards adopted and applied by security experts will naturally have a (somewhat delayed) impact on the law. The legal standards of cybersecurity are constantly updated to meet new and existing practices.[151] In fact, the duty of data security also evolves in response to new threats and security practices.[152]

Information flows created through breach notifications may determine legal standards on several levels. They can provide input for judges examining *ex post* if contested practices are acceptable.[153] Yet more importantly, they can provide regulators with insights as to what recommendations and even obligations they should issue regulated entities. This is vitally important for the regulatory structure in the United States, where general regulators—such as the Federal Trade Commission ("FTC")—are responsible for overseeing cybersecurity and effectively deciding what practices are acceptable.[154] By requiring the notification of the FTC and other regulatory bodies, these regulatory agencies gain valuable expertise and knowledge.

[147] *See generally* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1156 (2019) (describing the process by which "reasonable security . . . practices" are defined and developed).

[148] Indeed, some commentators have turned to game theory to better model cybersecurity conflicts. *See* Amadi Emmanuuel Chukwudi, Udoka Felista Eze & Charles Ikeronwu, *Game Theory Basics and Its Application in Cyber Security*, 3 ADVANCES WIRELESS COMMC'NS & NETWORKS 45, 48 (2017).

[149] *See id.* at 45.

[150] UNDERSTANDING KNOWLEDGE AS A COMMONS: FROM THEORY TO PRACTICE 13–14 (Charlotte Hess & Elinor Ostrom eds., 2007). *See generally* GOVERNING KNOWLEDGE COMMONS (Brett M. Frischmann et al. eds., 2014).

[151] Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1587–88 (2005).

[152] *Id.* at 1557 (arguing for a new tort that would subject software manufacturers to liability for cybercrime); McGeveran, *supra* note 147, at 1143 (describing extant "reasonable" security practices).

[153] Judges could use this information to determine outcomes in tort cases, particularly if there was a breach of duty by the data holder.

[154] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 625 (2014) (describing how the FTC's jurisprudence in privacy cases mirrors the organic, iterative approach of common law).

The focus on information sharing is already commonplace for private industry—and, particularly, critical infrastructure—in the United States.[155] A suite of legislation and executive orders established both Information Sharing and Analysis Organizations ("ISAOs") and Information Sharing and Analysis Centers ("ISACs").[156] ISAOs are communities that share information about emerging cyber threats.[157] ISACs are trusted entities that conduct risk assessment research and analysis.[158] The results of such data aggregation initiatives are shared with relevant industry players as well as the government.[159] Interestingly, these two types of organizations and initiatives account for short-term and long-term information sharing. ISAOs appear to focus on alerting potential targets of immediate threats, while ISACs conduct detailed analysis and operate on a longer time horizon.[160]

With regard to short term objectives, breach notification seems to be a poor fit for information sharing goals. This is mostly for institutional reasons. Cyberattacks require immediate responses and, therefore, data sharing must be conducted through highly specialized entities and measures.[161] The existing laws requiring disclosures to state A.G.s and other consumer protection entities which are accustomed to longer response times cannot provide an appropriate remedy. These short-term objectives are better reflected are better reflected in other data sharing regimes (most of them voluntary and sector specific) which provide Computer Emergency Response Teams ("CERTs")[162] with real time data which

[155] *See* Derek E. Bambauer, *Sharing Shortcomings*, 47 LOY. U. CHI. L.J. 465, 465–66 (2015).

[156] Federal Information Security Modernization Act of 2014, Pub. L. No. 113–283, § 2, 128 Stat. 3073, 3084 (2014) (establishing an information sharing regime between the government and private sector); Exec. Order No. 13,691, 80 Fed. Reg. 9349 (Feb. 20, 2015) (establishing information sharing procedures between private companies and the government).

[157] *Information Sharing and Analysis Organizations (ISAOs)*, CYBERSECURITY & INFRASTRUCTURE AGENCY, https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos (last visited Mar. 27, 2021) [https://perma.cc/E25M-TRTL] (describing ISAOs). Importantly, ISAOs encourage sharing beyond industries that have been designated as "critical infrastructure." *Id.*

[158] *About ISACs*, NAT'L COUNCIL ISACS, https://www.nationalisacs.org/about-isacs (last visited Mar. 27, 2021) [https://perma.cc/V5S8-YKUX] ("Information Sharing and Analysis Centers (ISACs) help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency.").

[159] *Id.*

[160] *See* sources cited *supra* notes 156–58.

[161] Relying on breach notification to protect against immediate threats is inapposite because breach notification is often slow and may not alert potential targets before these attacks are undertaken. Delays in reporting are currently a major problem with breach notification regimes. *See* Hayley Tsukayama, *Why It Can Take So Long for Companies to Reveal Their Data Breaches*, WASH. POST (Sept. 8, 2017, 9:05 AM), https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/why-it-can-take-so-long-for-companies-to-reveal-their-data-breaches/ [https://perma.cc/4D7E-3Q5B].

[162] *See US-CERT Federal Incident Notification Guidelines*, CYBERSECURITY & INFRASTRUCTURE AGENCY (Apr. 1, 2017), https://www.us-cert.gov/incident-notification-guidelines [https://perma.cc/82T9-2DXC]. CERTs receive mandatory reports from federal civilian agencies and voluntary reports from others. For more information about reporting in the EU, see Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L 194), 1, 17 (addressing the requirement to set up computer security incident response teams).

is shared across industries. Therefore, the need to pass information between industry players and the government cannot be a sufficient justification for these forms of disclosure.

As for the long-term objectives, promoting information sharing through breach notification requires certain specific design choices. Returning to the five-question taxonomy addressed above, in order to promote long-term goals of information sharing, the definitions of personal information and breach (Questions #1 and #2) should be relatively broad to assure as many incident reports as possible.[163] They might even need to include "near misses," in addition to successful attacks, in order to provide an even richer array of relevant information.[164]

Similarly, regarding exceptions and exemptions (Question #5), the information sharing justification requires applying them as narrow as possible.[165] In contrast to mitigation, the fact that no individuals were ultimately harmed does not reduce the need to share information about the attack and prepare other potential victims, especially those that might not be sufficiently prepared.

In terms of timing (Question #4), the real-time response objective calls for a short notification timeline, which requires reporting within minutes, rather than days. Yet, as explained above, this short window of time is unreasonable for the regulatory entities here discussed. However, achieving the intermediate and long-term informational objectives could be accomplished under more lenient time frames, such as those existing under current laws.

The key design challenge for implementing an information forcing regime is deciding which entities should be notified and what information should be included in these notifications (Question #3). For information forcing to be effective, breach notifications must be sent to regulators and cybersecurity experts so that they can update security standards and share information with others. Yet, unlike regulation—which strives to promote deterrence, shaming the breaching firm is not an objective, and broad disclosure to the public is unnecessary. Therefore, structuring a notification scheme that caters to the information forcing rationale is by far cheaper than its alternatives. Notifying the affected individuals offers little benefit. The notification process is limited, and moreover, the costs associated with maintaining a database of updated consumer contact information are unnecessary.[166]

As for the type of information disclosed, this feature departs radically from other foundational values of breach notification. Deterrence, for instance, merely requires the existence of a breach and the identity of the firm are disclosed publicly (and possibly in some cases the form of the security lapse to demonstrate

[163] Here, the definition of "breach" should be limited to more severe incidents so as to limit the over-reporting and cluttering of the entity pooling information. However, given the risk that setting a threshold too high will lead to the loss of timely reports, this notion should most likely be set aside.

[164] Jonathan Bair, Steven M. Bellovin, Andrew Manley, Blake Reid & Adam Shostak, *That Was Close! Reward Reporting of Cybersecurity "Near Misses*,*"* 16 COLO. TECH. L.J. 327, 329 (2018).

[165] *See, e.g.*, GDPR, *supra* note 2, at 53 (Article 34).

[166] This also supports a data minimization model because a firm does not need to keep records for its users in order to contact them in the event of a data breach.

the firm's recklessness).[167] Information forcing requires much more nuanced information.[168] This includes identifying the vulnerability exposed and abused, what types of information were compromised, and any other information that can be used to identify attack patterns or improve the state-of-the-art surrounding cybersecurity best practices—and all of these factors should be described in detail. Yet, as opposed to disclosures serving mitigation goals, the information need not include recommendations detailing how harms could be lessened and privacy restored.

Some data breach notification statutes appear to already incorporate this normative goal, at least to a limited extent. For instance, Massachusetts's notification statute collects information about the specifics of the breach, including some information on what type of information was breached and specifics on how the breach occurred.[169] In particular, the statute requires "[a] detailed description of the nature and circumstances of the breach of security or unauthorized acquisition or use of personal information."[170] Furthermore, the state set up a website with forms enabling quick and easy reporting of these elements.[171] It is unclear how the state uses the aggregated data from these forms, but future uses, such as those envisioned here, should not be ruled out. It appears that California is already striving to apply aggregated breach information to formulate overall recommendations.[172]

Many other notification schemes, however, are not attuned to this justification and concern. The GDPR requires notification of various data points including the nature of the breach and measures taken to address the breach,[173] yet it is clearly focused on achieving other objectives rather than enhancing data flows.[174] California law requires that the firm provide information as to "What Happened"; yet, this would only require "a general description of the breach incident, if that information is possible to determine at the time the notice is provided"—which would not provide substantial insight to promote security objectives.[175]

We therefore see that the "information forcing" objective calls for a different regulatory design from the one required to enhance deterrence or mitigation. Yet again, it is important to emphasize that optimizing any specific justification

[167] *See* Schwartz & Janger, *supra* note 5, at 955.

[168] *See, e.g.*, Off. Consumer Affs. & Bus. Regul., *Requirements for Data Breach Notifications*, MASS.GOV., https://www.mass.gov/info-details/requirements-for-data-breach-notifications (last visited Mar. 27, 2021) [https://perma.cc/3HBF-6UE4]).

[169] *Id.*

[170] *Id.*

[171] *Id.*

[172] KAMALA D. HARRIS, CAL. DEP'T JUST., CALIFORNIA DATA BREACH REPORT 2012–2015, 27–38 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf [https://perma.cc/Q342-LQPB].

[173] GDPR, *supra* note 2, at 52 (Article 33(3)).

[174] GDPR's Recital 49 specifically states that processing information by public authorities and computer security incident response teams for the strict purpose of ensuring information and network security would be considered a "legitimate interest" and thus, permitted. *Id.* at 9 (Recital 49). In this, the GDPR clearly signals its understanding that cyber-risks are a crucial issue, yet perhaps beyond the scope of this regulation. *See id.*

[175] CAL. CIV. CODE §§ 1798.29(d)(1)–(2)(e) (West 2020).

may lead to internal conflicts.[176] Designs that promote strong deterrence might incentivize underreporting and thus a loss of crucial information.[177] Designs that promote mitigation will potentially mobilize users to seek redress and, again, potentially lead to underreporting.[178] The objectives of an information forcing scheme might be satisfied through anonymous reports sent to a central repository, thus limiting the risk of reputational harm to the firm.[179] Furthermore, optimizing the notification process might call for providing some form of immunity to the reporting entity (which runs contrary to the legal strategies surveyed thus far).[180] This form of balancing and compromise has been incorporated in other arenas as well. For instance, within medical care, scholars have pointed out the tension between liability rules and information sharing norms between patients and medical professionals.[181] Here, when litigation risks are high, medical professionals seek to insulate themselves from legal liability by disclosing less information to clients.[182] This dynamic has led scholars to recommend no-fault compensation schemes.[183] And further, this intuition is strengthened by findings that harms are often caused by non-negligent errors—a dynamic that unfolds within cybersecurity as well.[184]

We conclude this segment by openly revisiting and reexamining the utility of information sharing generally. Although the potential informational benefits of a mandatory notification scheme are apparent, some scholars question whether they are somewhat overblown. Derek Bambauer has argued that firms have substantial incentives to voluntarily share information among themselves and the government (with the expectation of reciprocity).[185] Bambauer notes that cybersecurity incidents often target vulnerabilities that are widely known and where patches exist.[186] In these cases, information forcing provides little additional benefit.

Steven Bellovin and his coauthors, on the other hand, assert that an aggregated database of incidents is vitally important.[187] They emphasize the need for a more complete picture of incidents, including "near misses," while noting the

[176] Schwartz & Janger demonstrated the perils of unrestrained maximization of possible justifications for data breach. Schwartz & Janger, *supra* note 5, at 937 ("[T]he threat of reputational sanction may serve to chill a company's willingness to inform about a security breach. This inhibiting effect may limit the ability of customers, other institutions, and regulators to reduce the harm flowing from the breach.").

[177] *Id.*

[178] *Cf.* Bair et al., *supra* note 164, at 335, 337.

[179] *Id.* at 331, 333–34; Schwartz & Janger, *supra* note 5, at 940.

[180] Bair et al., *supra* note 164, at 352–53.

[181] Sagit Mor & Orna Rabinovich-Einy, *Relational Malpractice*, 42 SETON HALL L. REV. 601, 627 (2012).

[182] *Id.* at 609.

[183] *Id.* at 638.

[184] *Id.* at 628, 640.

[185] Bambauer, *supra* note 155, at 470–72 (describing the current landscape of information sharing between private firms as well as between private firms and government actors).

[186] *Id.* at 473–76.

[187] Bair et al., *supra* note 164, at 329–47.

benefit of such databases in other industries and contexts.[188] Yet, they are reluctant to advocate for a mandatory scheme and contemplate the benefits of a purely voluntary one.[189]

While accounting for both positions, we tend to agree with the latter regarding the benefit and utility of information forcing and sharing, yet we acknowledge that additional research regarding this issue is necessary. Returning to the "knowledge commons" concept, creating additional information through breach notification will generate substantial positive externalities to regulators and academics.[190] Therefore, those holding the information will not be substantially incentivized to share the information and therefore, must be forced to do so to enable this overall good. We also note that a compromise will potentially call for information sharing requirements about sophisticated attacks, yet we understand that drawing a distinction between simple and sophisticated attacks might lead to bias in reporting and a skewed mapping of overall cyber-risks. We, however, tend to believe that mere voluntary databases will be insufficient and provide only a partial view of the cyberattack landscape.

Finally, a rich database of breach information is essential because it provides a valuable input to the development of cyber-insurance. As we will explain below,[191] cyber-insurance is a crucial yet underdeveloped piece of the overall cybersecurity puzzle. A key problem with cyber-risk insurance is the difficulty in assessing risk, among others, because of the lack of aggregated data on attacks, their nature and success.[192] Information sharing schemes can help close this gap.

[188] *Id.* at 331–33.

[189] *Id.* at 330–33.

[190] Yochai Benkler, *Between Spanish Huertas and the Open Road*, *in* GOVERNING KNOWLEDGE COMMONS, *supra* note 150, at 69, 88–90 (discussing the relationship between promoting and maintaining commons and the existence of positive externalities).

[191] *See infra* notes 336–44 and accompanying text.

[192] *See* McGeveran *supra* note 147, at 1172 n.206.

4. *Autonomy, Control, and Restorative Justice*

Breach notification can also serve and promote important autonomy-related values. On the most basic and fundamental level, breach notifications facilitate the data subject's control over their personal information.[193] "Control" over personal data is often understood as justifying notice prior to data processing and the ability to block unwanted uses and transfers.[194] Yet, it certainly can also call for informing subjects of their data's whereabouts after a breach, as a (somewhat limited) measure of control over data that has been compromised. Furthermore, information regarding breaches might provide data subjects a glimpse of the extent of the surveillance infrastructure lurking in the background, often without their knowledge.[195]

The right of control can be deduced from the fundamental autonomy rights individuals should have concerning their personal data (as an extension of their bodies and selves).[196] Personal data is intimately tied to the person, as it contains information about our personalities and habits.[197] Indeed, as Danielle Citron and Daniel Solove explain, data breaches cause psychological distress and anxiety.[198] Thus, on a practical level, this justification would be met by purely informational notifications which details the data's "whereabouts" in an attempt to empower the data subject. To some extent, the noted autonomy interests might resemble similar right assumed in a "property"-like context. Just as property owners would expect to be informed of trespass to their land, individuals will expect the same regarding their own data.[199]

Beyond a "rights" based justification for providing notice, the notification itself might directly mitigate the autonomy-based harm breaches cause while taking a more instrumental role. The psychological experience of being wronged

[193] The notion of privacy as control is an early view of privacy that has been endorsed by more recent commentators. In an early formulation of the legal right to privacy, Warren and Brandeis implicitly endorse a version of "privacy as control." *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195–99 (1890). Another leading privacy theorist, Alan Westin, recounts a view of privacy that prioritizes control. *See generally* ALAN F. WESTIN, PRIVACY AND FREEDOM (1967). More recent commentators have defended notions of privacy as control as well. Charles Fried, *Privacy*, 77 YALE L.J. 475, 482–83 (1968). However, there are several critiques of privacy as control. *See* Lisa M. Austin, *The Problem of Theorizing Privacy: Rereading Westin*, 20 THEORETICAL INQUIRIES L. 53, 54 (2019) (arguing that privacy as control is incomplete and privacy should focus on securing meaningful privacy choices); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 1–2 (2010) (arguing that privacy requires appropriate flows of information, rather than control).

[194] Notice and consent regimes in privacy find their origin in the Fair Information Practice Principles (FIPPs) originally in the Health Education and Welfare Report. *See* U.S. DEP'T HEALTH, EDUC. & WELFARE, U.S. DEP'T OF JUST., RECORDS COMPUTERS AND THE RIGHTS OF CITIZENS xxiv (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf [https://perma.cc/4YM2-Z6YS].

[195] *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019). We thank Brett Frischmann for this point.

[196] *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1377 (2000); *see also* Mark Verstraete, *Inseparable Uses*, 99 N.C. L. REV. 427 (2021).

[197] *Id.* at 1378.

[198] Solove & Citron, *supra* note 97, at 745.

[199] We thank Kevin Werbach for this point.

through data breach maps to other contexts where victims benefit from *restorative processes*.[200] Similarly, restorative processes can also serve to reform the wrongdoers (breached firms) through the process of drafting and delivering breach notifications.[201]

To further explain this point, consider the fundamental definition of "restorative justice." John Braithwaite—a leading theorist of restorative justice—endorses a view of such justice that requires a "process whereby all the parties with a stake in a particular offense come together to resolve collectively how to deal with the aftermath of the offense and the implications for the future."[202] He further notes that this process includes core values, such as apology (by wrongdoers), dialogue (by both wrongdoers and victims), and forgiveness (by victims).[203] Ultimately, restorative justice is about "restoring victims, restoring offenders, and restoring communities."[204]

The possibility that data breach notification statutes may serve autonomy interests through restorative justice mechanisms is wholly overlooked by commentators and therefore requires a closer examination. The central functions of restorative justice that a data breach notification law may incorporate are apologies and making amends. We will now briefly address both, as well as the balances they entail and the policy steps they require.

Data breach notifications may mirror *apologies* in important respects. The core features of apologies are an acknowledgement of wrongdoing, an acceptance of responsibility by the wrongdoer, and a demonstration of remorse.[205] Apologies require that the wrongdoer is aware of their wrongdoing and recalls the specific act, leading to the possibility of better conduct in the future.[206] Apologies are also expected by (or perhaps even owed to) the victims who may find comfort in these remedial rituals.[207] Therefore, apologies are intended to transform both the wrongdoer and victim.

Crafting a data breach notification regime that optimally achieves apology goals is potentially in tension with other justifications. For example, the requirement that firms accept responsibility and provide an acceptable and convincing apology is likely to be implausible if deterrence goals are aggressively pursued through the application of legal liability with extensive damages.[208] This is because firms are unlikely to admit wrongdoing and offer apologies if this renders

[200] Restorative processes are most commonly used in response to criminal justice violations. *See* Andrew Ashworth, *Responsibilities, Rights and Restorative Justice*, 42 BRIT. J. CRIMINOLOGY 578, 578 (2002).

[201] John Braithwaite*, Restorative Justice: Assessing Optimistic and Pessimistic Accounts*, 25 U. CHI.: CRIME & JUST. 1, 17 (1999).

[202] *Id.* at 5 (endorsing this definition of restorative justice).

[203] *Id.* at 5–6.

[204] *Id.* at 6.

[205] NICHOLAS TAVUCHIS, MEA CULPA: A SOCIOLOGY OF APOLOGY AND RECONCILIATION 14–26 (1991).

[206] Alfred Allan & Robyn Carroll, *Apologies in a Legal Setting: Insights from Research into Injured Parties' Experiences of Apologies After an Adverse Event*, 24 PSYCHIATRY, PSYCH. & L. 10, 15 (2017).

[207] *Id.* at 12.

[208] *See* Bair et al., *supra* note 164, at 335.

them liable for compensation through litigation or fines.[209] Therefore, legal systems which enable standing for most security breaches, allow for class actions to proceed for such wrongs,[210] assign significant damage awards in private lawsuits over breaches, and levy imposing administrative fines will undermine restorative justice objectives.

This is particularly true if statements in notification letters serve as precursors to legal liability. In such a regime, firms are unlikely to admit wrongdoing, limiting the possibility of an effective apology.[211] The GDPR, for instance, might therefore fail to promote restorative justice for this reason; while the breach notification requirements shower data subjects with an abundance of information in accordance with Article 34, the joint effect of Article 32 (mandating "security of processing") and Article 83(4)(a) (assigning hefty fines in the case of a breach) will incentivize firms to be extremely cautious with the disclosure policies rather than sincere and open with their apologies.[212]

Firms may use breach notification letters to serve another important restorative justice value: repairing their relationship with the data subject. Commonly, restorative justice theorists discuss "*making amends*" as a potential avenue to restore the relationship between wrongdoers and victims.[213] For instance, to facilitate the process of making amends, firms could offer discounts on future purchases or some other compensation. The move to offer discounts in the wake of data breaches is already a common (and largely criticized) practice.[214] For example, the online shoe retailer Zappos offered customers a ten-percent off coupon for their next purchase after experiencing a data breach.[215] And while such offers could be viewed as an empty, even cynical gesture, restorative justice suggests that the discounts for future purchases or similar offers are not a meaningless remedy.[216]

Some restorative justice skeptics (particularly as it is incorporated in breach notification) might be unpersuaded about the potential benefits of incorporating these goals into breach notification regimes. These critics are likely to view restorative justice efforts as incomplete, insincere, or even manipulative.[217] But there are real benefits that can be derived both systemically and individually from

[209] *See, e.g.*, Maurice E. Schweitzer, Alison Wood Brooks & Adam D. Galinsky, *The Organizational Apology*, HARV. BUS. REV.: MAG. (Sept. 2015), https://hbr.org/2015/09/the-organizational-apology [https://perma.cc/DM97-35Q2].

[210] *See supra* note 66 and accompanying text.

[211] *See* Bair et al., *supra* note 164, at 335.

[212] *Compare* GDPR, *supra* note 2, at 51–52 (Article 32) (mandating security of processing), *with id.* at 82 (Article 83(4)(a)) (assigning hefty fines in the case of breach).

[213] *See* Braithwaite, *supra* note 201, at 6.

[214] Josephine Wolff, *The Chintzy Way Zappos Wants to Compensate Victims of a 2012 Data Breach*, SLATE (Oct. 17, 2019, 6:23 PM), https://slate.com/technology/2019/10/zappos-amazon-data-breach-settlement-coupon.html [https://perma.cc/CVF2-9E2F].

[215] *Id.*

[216] *See id.*; *see also* THEO GAVRIELIDES, EUROPEAN INST. CRIME PREVENTION & CONTROL, RESTORATIVE JUSTICE THEORY AND PRACTICE: ADDRESSING THE DISCREPANCY 35 (2007) (noting the goal of restorative justice is providing meaningful community-driven consequences rather than relying on criminal sanctions).

[217] *See generally* M. Eve Hanan, *Decriminalizing Violence: A Critique of Restorative Justice and Proposal for Diversionary Mediation*, 46 N.M. L. REV. 123 (2016) (outlining restorative justices' shortcomings).

incorporating restorative justice interests into a notification scheme. First, restoring a relationship between firm and consumer could be individually and socially beneficial. Consumers may benefit from repairing their relationship with the breaching firm, rather than taking their business to a new firm (as deterrence models envisions) or continuing as a disgruntled customer with no other choice. Data breach notification is a noisy signal as it is often influenced by luck (as we explain below).[218] Therefore, if indeed inclined to switch on the basis of the notification received, a consumer might switch to a competitor that is equally as likely to experience a breach.[219] And in other scenarios, if the consumers are doomed to remain in a relationship with the breaching party given a lack of options, perhaps it is more important to improve the relationship between them.[220]

Second, consumers may also benefit from repairing a relationship with the breached firm because this cuts down on their activity levels and therefore, the chance of being subjected to a breach. By switching services, consumers risk having their personal data stored in a new location which, again, increases their security risks.[221]

To promote something akin to apologies, a breach notification regime would need to be designed in order to maximize this value. Most prominently, this would likely require specific regulatory design answers regarding which entities should receive notifications (Question #3). Ideally, an apology-focused breach notification scheme would require a firm to send notifications to the data subjects whose information was put at risk while also identifying the responsible party. While this practice is already incorporated in several major data breach notification laws (such as California's breach notification law), it differs from several other existing regulatory models.[222] Some models call for limited notification to a regulatory entity in non-severe and limited cases.[223] Other contemplated models call for anonymous notices which hide the identity of the firm.[224] If breach notification letters act as forms of apology, then the firm's identity should be revealed, as anonymous apologies seem ineffective at best, and conceptually incoherent at worst, especially given the lack of sincerity this might reflect.[225] Additionally, for breach notifications to function as apologies, supplemental information should be included, such as an admission of responsibility by the firm and explanation of how the data subject's information was compromised.[226]

[218] NATE SILVER, THE SIGNAL AND THE NOISE: WHY SO MANY PREDICTIONS FAIL—BUT SOME DON'T 21, 162 (2012).

[219] *See* Kenneth A. Bamberger & Orly Lobel, *Platform Market Power*, 32 BERKELEY TECH. L.J. 1051, 1068–69 (2017).

[220] The lack of meaningful alternatives is particularly acute in the platform economy. *See id.* at 1053.

[221] *Id.* at 1089–91.

[222] *See* CAL. CIV. CODE § 1798.29(a) (West 2020).

[223] *See, e.g.*, GDPR, *supra* note 2, at 52–53 (Article 34) (limiting the requirement to communicate to the data subjects if there is a limited chance of harm).

[224] Schwartz & Janger, *supra* note 5, at 937.

[225] *Id.*

[226] *See id.* at 932–35.

Additionally, the definition of personal information (Question #1) should conform to the definitions of personal information that is protected under current privacy law. This means that all personally identifiable information should be protected under breach notification statutes because this information implicates autonomy and restorative justice concerns. By contrast, data breach notification should likely not extend to deidentified data or encrypted data because people have limited individual interest in controlling these uses (thus allowing a specific set of exceptions and providing a response to Question #5).

The GDPR and California law reflect this response. In fact, the GDPR uses the same definition of personal information in privacy and security contexts.[227] However, in the majority of state data breach laws, the type of information that is protected by the breach notification statute is narrower than what is protected under privacy law.[228] As a result, many states fail to adequately promote the autonomy-based interest because of the narrow definition of personal data.

Similarly, the definition of a "breach" (Question #2) could be calibrated to promote autonomy and restorative justice values. To do so, data breach notification only needs to cover "breaches" where the data subjects lose control of their data. This reflects the wrong that undergirds both autonomy and restorative justice. For instance, breaches where data is removed is the most obvious case where autonomy and restorative justice are implicated. By contrast, in cases of data loss (where data is deleted) or data inaccessibility (where access is limited), autonomy claims are significantly weaker. Thus, a data breach notification statute that promotes autonomy must capture data extraction, but it does not necessarily need to account for data loss or data inaccessibility.

Finally, autonomy and restorative justice do not require specific design choices for how promptly notification must occur (Question #4). There is a colorable argument that autonomy interests of the data subject require that firms disclose breach incidents promptly, yet this does not seem crucial. Similarly, restorative justice efforts can take place whether the data subject learns of the breach in a matter of days, months, or even years.

C. Notification Laws and Existing Paradigms: Square Pegs and Round Holes

To conclude this Part, it is important to examine several legal paradigms which could potentially illuminate and justify breach notification laws. Ultimately, however, none of these paradigms are a perfect fit. Instead, breach notification bears a slight resemblance to several salient, yet competing legal constructs. As a result, this Article's analysis breaks new ground as breach notification is a novel construct requiring a close examination of its internal balances. The following segment, therefore, strives to meet two objectives by detailing several dominant theories for tort liability: it emphasizes this Article's

[227] *Compare* GDPR, *supra* note 2, at 33 (Article 4(1)) (defining "personal data"), *with id.* at 34 (Article 4(12)) (defining "personal data breach").

[228] *See* BAKERHOSTETLER, *supra* note 29, at 1 (detailing the most typical definition of "personal information" in breach notification statutes).

innovations given these other theories' inability to address the specific issue before us, and it provides important analytical building blocks for the discussion below.

1. Negligence-Based Tort Theories

Negligence is currently the driving force behind data breach litigation. In much of the U.S.[229] and the EU,[230] firms are subject to liability when they fail to exercise a reasonable level of care and this failure causes a breach resulting in harm. Breach notification might appear to be a natural extension of this requirement that is premised on the same foundational principles. But breach notification laws are *not* mere instances of negligence-based liability. As a result, the potential convergence (or conceptual overlap) between breach notification and negligence theories of liability requires closer scrutiny.

To start, viewing breach notification as a negligence-based liability could be inspired by and derived from at least two sources. One would be the standard negligence framework from tort law, which would be expanded to data security.[231] This would require that data holders meet reasonable security standards.[232] Alternatively, breach notification liability might be derived from "premises liability"—a legal doctrine that attributes liability to a landlord for third-party criminal acts that transpire on the landlord's property and harm a tenant (or their guests).[233] Yet, breach notification laws are an imperfect analogue for both traditional negligence liability and premises liability.

Intuitively, a "general" duty of care—akin to traditional negligence liability—could be applied to data breaches. General liability rules are intended to place the burden of care on the most efficient risk bearer, risk minimizer, or risk spreader—which will often be the firm collecting personal information.[234] Further, attributing potential liability for security breaches to firms is fair and efficient given the alternative risk bearers; data subjects have little information about the security practices of firms that collect and store personal information, and attributing liability to hackers is usually fruitless (and ineffective) as their detection is costly and, in many cases, impossible.[235] Therefore, notification rules might be justified along similar lines as general negligence liability because they

[229] *See generally* McGeveran, *supra* note 147, at 1196 (providing an overview of data protection laws in the United States).

[230] *See* GDPR, *supra* note 2, at 52 (Article 32(2)) (detailing the requirement for "appropriate" level of security).

[231] *See* Henry T. Terry, *Negligence*, 29 HARV. L. REV. 40, 42 (1915) (defining instances of negligence as departures from the "reasonable person" standard); *see also* Benjamin C. Zipursky, *Reasonableness in and out of Negligence Law*, 163 U. PA. L. REV. 2131, 2134 (2015).

[232] Terry, *supra* note 231, at 41.

[233] Robert S. Driscoll, *The Law of Premises Liability in America: Its Past, Present, and Some Considerations for its Future*, 82 NOTRE DAME L. REV. 881, 883 (2006) (overview of United States premises liability law).

[234] Frank H. Easterbrook & Daniel R. Fischel, *Limited Liability and the Corporation*, 52 U. CHI. L. REV. 89, 102 (1985) (discussing the desirability of placing liability on the most efficient risk bearer).

[235] *See, e.g.*, Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011), https://www.scientificamerican.com/article/tracking-cyber-hackers/ [https://perma.cc/Y78U-9T78].

incentivize firms to provide adequate security standards to the extent that these measures are efficient and possible.

Upon closer scrutiny, however, breach notification laws are an imperfect match for the justifications that support imposition of general negligence liability. In fact, breach notification flouts the central driving force behind negligence—duty of care. More specifically, breach notification requires disclosures and might lead to negative consequences even if the firm complied with the standard of care and took every possible effort to secure the information and infrastructure.[236] Of course, incorporating robust security standards would reduce the likelihood of breaches (and notifications);[237] yet, data breaches may still occur. Therefore, breach notification laws transcend the accepted application of negligence-based rules.

Alternatively, some commentators have considered *premises liability* as a helpful analogy for assigning liability for data breaches.[238] These scholars suggest that we apply a similar rule online to the one that the court crafted in the famous premises liability case, *Kline v. 1500 Mass Ave. Apartment Corp.*[239] There are substantial similarities between data breaches and premises liability.[240] In theory, a website should be required to protect information of its users and customers in a manner similar to the duty a landlord had in this case to protect tenants from criminal activity on his property.

Assessing breach notification through the prism of premises liability reveals a potential shortcoming. Premises liability is based on predictable risks which the landlord could conceivably limit.[241] Indeed, in their analysis of this issue, Rustadt and Koening concede that premises liability is a poor fit for online liability.[242] More specifically, they explain that premises liability requires evidence (and knowledge) of crimes in the surrounding area before finding the landlord's liability for third-party acts.[243] They further explain that because prior knowledge of a cybercrime threat from a specific individual is unlikely, this doctrine would not lead to a duty to protect from existing cyberthreats, which are often changing.[244] And, of course, some cyberthreats are novel and fall outside any reasonable expectation of the platform controller. Therefore, while breach notification shares many similarities to existing negligence regimes, some complications make breach notification unique and worthy of independent analysis.

[236] Schwartz & Janger, *supra* note 5, at 937.

[237] *See* McGeveran, *supra* note 147.

[238] Rustad & Koenig, *supra* note 151, at 1559 (proposing premises liability as an analogy for data breaches).

[239] *See id.* at 1584; Kline v. 1500 Ma. Ave. Apartment Corp., 439 F.2d 477, 483 (D.C. Cir. 1970).

[240] Rustad & Koenig, *supra* note 151, at 1582.

[241] *See id.* at 1583.

[242] *Id.*

[243] *See id.*

[244] *See id.*

2. *Strict Liability*

On their face, notification rules are a form of strict liability—they generate a sanction irrespective of the level of care the firm applied in practice.[245] The only consideration for whether a notification is required is the existence of a breach.[246] Inevitably, some firms will be forced to provide notifications in situations where there was a breach, yet the firm is not at fault because it complied with security best-practices.

Indeed, some commentators have suggested that data breach notification statutes are instances of strict liability. Jane Winn, for instance, suggests that the California data breach notification statute imposes liability without considering fault or whether the firm contributed to the breach.[247] This is largely because the California law requires that firms "shall disclose any breach of the security system following discovery or notification of the breach in the security of the data."[248] Thus, the justifications for breach notifications could be integrated into a broader discussion as to when strict liability rules are appropriate, and more specifically, if and when they are appropriate for data security.[249]

Several scholars suggest that strict liability is the most appropriate liability regime for harms in cyberspace.[250] For instance, Danielle Citron argues that applying strict liability will allow for avoiding several pitfalls that attend negligence standards, such as the lack of clear standards, fear of over-enforcement, and unwillingness to share data.[251] At bottom, Citron argues that strict liability would simplify enforcement of data security for regulators and courts.[252]

In this Article, we do not take a position as to whether and when strict liability should be applied to security lapses and breaches. Rather, we merely point out that most breach notification statutes *cannot* be considered a clear manifestation of a strict liability regime. As explained above, breach notification laws do not impose liability. Instead, these laws require notification, which triggers a chain of events that might lead to various forms of damages.[253] Moreover, unlike strict liability, the extent of the damages resulting from the remedy might be directly related to the existence of reasonable measures and even efforts to meet security standards.[254] Meeting such standards will determine the extent of regu-

[245] *See id.* at 1587.

[246] Granted, there are exceptions. *See supra* notes 44–47 and accompanying text.

[247] Winn, *supra* note 5, at 1144 ("[data breach notification laws] draw on several legislative models including . . . . strict liability in tort law.").

[248] CAL. CIV. CODE § 1798.29(a) (West 2020).

[249] Shavell, *supra* note 13, at 1 (comparing "strict liability and negligence rules on the basis of the incentives they provide to 'appropriately' reduce accident losses").

[250] Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 243 (2007); *see also* Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 682–83 (2013) (discussing the need for lesser intent requirements for cybersecurity liability).

[251] Citron, *supra* note 250, at 263.

[252] *Id.*

[253] *See, e.g.*, *id.* at 294 n.313 (explaining the nature of notification statutes as they relate to data breaches).

[254] *See id.* at 271.

latory fines the firm might receive, the firm's ability to respond to public complaints and outcry, and the firm's ability to defend tort claims launched by those notified of the breach.[255]

That being said, there are indeed substantial similarities between breach notification laws and strict liability schemes, and these will be taken into account in parts of the analysis below.[256]

3. Shaming Sanctions

At first glance, breach notification requirements resemble a form of governmental or regulatory shaming—a common practice across several contexts.[257] As with shaming, breach notification laws do not "punish" the firms directly. Instead, notification laws initiate the publicizing of a firm's failure, which allows society to enforce reputational sanctions against the firm.[258]

While breach notification laws share some similarities with shaming sanctions, they cannot be perfectly subsumed within the shaming paradigm. But some of the arguments and analyses from discussions about shaming are instructive for debates about breach notification. For example, the effects of breach notification—akin to the effects of shaming—are unpredictable and may spiral out of control.[259] Likewise, the effects of breach notification (and regulatory shaming) might vary based on the firm's size.[260]

Shaming has been used as an alternative measure of punishment and correction for thousands of years.[261] It has mostly been applied as a measure in criminal law.[262] Beyond ancient times, it was also applied towards corporations as part of the regulatory process.[263] Recent examples of regulators applying shaming-like remedies and sanctions include OSHA, the FDA, and the SEC.[264] While using shaming has been debated in the academic literature, it has been endorsed by some commentators as an efficient form of sanctioning.[265]

Although breach notifications mirror shaming sanctions in many respects, yet they depart from it in significant ways. Most shaming schemes involve dis-

[255] Note that some scholars have set forth more nuanced forms of strict liability for this context, which indeed might be a closer fit to the breach notification paradigm. *See* Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614, 627 (2018).

[256] *See* discussion *infra* Section II.B.1.

[257] Dan M. Kahan, *What Do Alternative Sanctions Mean?*, 63 U. CHI. L. REV. 591, 611 (1996).

[258] *See id.* at 632–33.

[259] Sharon Yadin, *Regulatory Shaming*, 49 ENV'T L. 407, 442 (2019).

[260] *Id.*

[261] *See id.* at 413.

[262] *Id.*

[263] *Id.* at 420.

[264] *Id.* at 421.

[265] *See id.* at 415 (noting the shift in Dan Kahan's work, first being in favor of and then opposing these sanctions and that other scholars that find these measures to be efficient and appropriate); *see also* Kahan, *supra* note 257, at 591–93.

closures published by the regulators, which often provide some form of annotations, such as rankings.[266] By contrast, breach notification mostly involves mandatory disclosures made by private parties.[267] In addition, most shaming involves publication to the public, as opposed to merely the person who was harmed by the action (here, the data subject).[268]

* * *

As this analysis shows, enacting and structuring breach notification schemes is a complex task which calls for recognizing what objectives notifications will support. We will now turn our attention to two underappreciated implications that ultimately should influence the effectiveness of different normative foundations for data breach laws.

III. Breach Notification: Underappreciated Outcomes and Implications

This Part details two underappreciated outcomes resulting from adopting data breach notification statutes—unfairness (which is related to the notion of moral luck) and distortions in activity levels. While both concepts are carefully discussed in tort theory literature, they have not yet found their way into discussions about data breach notification statutes and policy.

Nonetheless, these two concepts bring important insights for data breach notification laws, particularly regarding their implications and effectiveness. These insights unfold along two distinct dimensions. First, unfairness/luck-related concerns and activity levels examinations complicate some of the underlying normative justifications for data breach notification laws.[269] Second, different data breach notification statutes implicate these two concepts in different, yet unique ways.[270] Thus, legal architects should design data breach notification statutes with these implications in mind.

A. Breach Notification, Unfairness, and Luck

Data breach notification laws are an attempt to offset the harms that arise from data breaches.[271] Yet is it possible that these laws lead to unfair outcomes for some firms that are forced to provide notification in the wake of a breach? Exploring this notion brings us to the concept of *luck*. Luck, in general, and moral luck, in particular, have generated interest[272] and proved puzzling for tort law, as legal liability often seems to be a product of bad luck, rather than bad actions or

[266] Yadin, *supra* note 259, at 425–26.

[267] *Id.* at 426 (explaining shaming could include both forms of situations).

[268] *Id.* at 429–31.

[269] *See* Benjamin C. Zipursky, *Two Dimensions of Responsibility in Crime, Tort, and Moral Luck*, 9 THEORETICAL INQUIRIES L. 97, 99–100 (2008).

[270] *See id.* at 104.

[271] *See* Yadin, *supra* note 259, at 428.

[272] Zipursky, *supra* note 269, at 98; David Enoch, *Moral Luck and the Law*, 5 PHIL. COMPASS 42 (2010); Emily Sherwin, *Interpreting Tort Law*, 39 FLA. ST. L. REV. 227, 230 (2011); Tom Baker, *Liability Insurance, Moral Luck, and Auto Accidents*, 9 THEORETICAL INQUIRIES L. 165 (2008).

bad character.[273] Breach notification requirements and the liability that follows are susceptible to luck in three distinct ways. Two of these are applications of the general "moral luck" literature,[274] while the third pertains to data breach notification specifically.

1. Causal Luck

A primary element of tort liability is that an individual causes an injury.[275] Yet whether a person ultimately causes an injury is often principally a product of fortune.[276] This feature, often referred to as "causal luck," is described by Jeremy Waldron in a famous hypothetical example. Here, two drivers (Alice and Bob) both carelessly divert their eyes from the road for a brief second.[277] However, as chance would have it, only Bob causes an accident that results in an injury.[278] Here, Waldron claims that Alice and Bob's actions are morally equivalent (both drove carelessly), but their liability is not (only Bob will be potentially legally liable as Alice caused no harm); and importantly, the difference in liability is largely determined by luck.[279]

Let us now apply this paradigm to data breaches. Whether a data breach occurs results from the level of security implemented and maintained by any given firm.[280] Nonetheless, luck plays a major role given the nature of data and its inherent leakiness. That is, data leaks might happen despite reasonable security practices, and this potentially generates unfair outcomes.[281] At this point, we concede that the classical discussion of "moral luck" is only partially relevant. Given the novelty and uncertainty regarding data security norms, it is difficult to identify when moral culpability attaches, and therefore when inequality and unfairness will arise in the moral context. Nonetheless, luck itself is clearly playing a role in the extent of liability. For that reason, we refrain from referring to "moral luck" and frame our arguments broadly, referring to "luck" in general.[282]

This argument about the enhanced role of luck in data breaches is strengthened by surveys indicating that many cybersecurity experts consider data breaches "inevitable."[283] For instance, 86% of the Chief Information Officers

[273] John C.P. Goldberg & Benjamin C. Zipursky, *Tort Law and Moral Luck*, 92 CORNELL L. REV. 1123, 1124 (2007).

[274] *Id.* at 1126 (distinguishing between "causal luck" and "compliance luck" in tort law).

[275] *Id.* at 1125.

[276] *Id.* at 1124.

[277] Jeremy Waldron, *Moments of Carelessness and Massive Loss*, *in* PHILOSOPHICAL FOUNDATIONS OF TORT LAW 387 (David G. Owen ed., 1995).

[278] *Id.*

[279] *Id.*

[280] CATE, *supra* note 5, at 7.

[281] *See id.*

[282] We thank Shyam Balganesh for this point.

[283] *See* CATE, *supra* note 5, at 14.

("CISOs") surveyed in a recent report from Kaspersky Labs confirmed the inevitability of breaches.[284] For these security experts, data breaches are a question of "when," not "if."[285] The inevitability of data breaches necessarily implies that the prospect of a breach is partly out of the firm's control and subject to external factors, such as luck, especially if the hacker is determined and persistent.[286]

Other security experts make similar claims about the intrinsic difficulties of securing against data breaches, such as arguing that achieving perfect security is impossible.[287] While the impossibility of perfect security is universally true (from securing vehicles to structuring dams), it has greater salience for data security. This is because security threats are ever changing, and adversaries are constantly finding and exploiting flaws in security systems.[288] Thus, with data security, even if a firm uses the most advanced security practices available at the time of implementation, it cannot totally foreclose the risk of a data breach.

Finally, computer security expert Bruce Schneier puts a finer point on the inherent imperfections of cybersecurity. Schneier claims that "everything is hackable," yet goes on to clarify this does not necessarily mean that everything will, in fact, be hacked.[289] To Schneier, what separates hackable systems from systems that have been (or eventually will be) hacked is a mix of factors (which we discuss more fully in the next Subsection).[290] Yet the essential point is that the difference between a hackable system and a hacked one is based on factors that are influenced largely by luck or other unpredictable elements beyond the control of the data collector.

To demonstrate this point, consider the massive 2018 Marriott data breach that led to significant fines against the hotel conglomerate.[291] Top government

[284] Kaspersky Labs surveyed over 250 Chief Information Security Officers (CISOs). *See* Andrey Evdokimov, *What It Takes to Be a CISO: Success and Leadership in Corporate IT Security*, KASPERSKY DAILY (Oct. 25, 2018), https://usa.kaspersky.com/blog/ciso-report/16480/ [https://perma.cc/W3FM-S4HB].

[285] David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 936 (2016).

[286] We map out the various hacker motivations below. *See infra* notes 385–98 and accompanying text.

[287] Shuman Ghosemajumder, *You Can't Secure 100% of Your Data 100% of the Time*, HARV. BUS. REV. (Dec. 4, 2017), https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time [https://perma.cc/BN9B-7ND9].

[288] *Id.*

[289] Bruce Schneier, *Can Consumers' Online Data Be Protected*?, SCHNEIER ON SEC. (Feb. 14, 2018, 6:43 AM), https://www.schneier.com/blog/archives/2018/02/can_consumers_o.html [https://perma.cc/ECU9-NNFT] ("But just because everything is hackable doesn't mean everything will be hacked. The difference between the two is complex, and filled with defensive technologies, security best practices, consumer awareness, the motivation and skill of the hacker and the desirability of the data.").

[290] *Id.*

[291] Kate O'Flaherty, *Marriott Faces $123 Million Fine For 2018 Mega-Breach*, FORBES (July 9, 2019, 11:49 AM), https://www.forbes.com/sites/kateoflahertyuk/2019/07/09/marriott-faces-gdpr-fine-of-123-million/#4c4fabc84525 [https://perma.cc/X9H9-LMWJ]. Marriott's fine was reduced from the proposed £99 million fine. *See ICO Fines Marriott International £18.4 Million for Security Breach*, HUNTON ANDREWS KURTH: PRIV. & INFO. SEC. L. BLOG (Oct. 20, 2020), https://www.huntonprivacyblog.com/2020/10/30/ico-fines-marriott-international-18-4-million-for-security-breach [https://perma.cc/S3FM-AAVM].

officials confirmed that the Marriott data breach was a product of hacking operations by the Chinese government, the motivations of which are still unclear.[292] Because of the technological sophistication of the Chinese hackers,[293] there is arguably no security measure that Marriot could have taken to prevent that breach. The adversary was simply too sophisticated and determined to be stopped by conventional cybersecurity measures.[294] Unfortunately for Marriott, it happened to be selected as a target (another hotel chain could have been selected just as well).[295] Note, however, that this analysis of the Marriott breach must be taken with a grain of salt. In early 2020, Marriott reported yet another large data breach, this time resulting from the compromising of two employee logins.[296] These repeated breaches might be indicating other reasons (perhaps related to the firm's culture) for the Marriott breaches.[297]

2. *Compliance Luck*

Legal theorists have also described a second element of luck, "compliance luck," which considers people's abilities to conform to objective standards of behavior.[298] Compliance luck might have an impact on the fairness of the breach notification scheme. As Richard Posner demonstrates, tort liability is an objective standard, so situations arise where a person tries their best to "avoid an accident and just happens to be clumsier than average."[299] Framing this argument for breach notification implies that a person's ability to regulate their behavior according to the law is a product of their innate talents, which is largely outside of their control. For instance, the security executive at the small corporation may intend to install state of the art security software but errs in the installation and leaves segments of the system vulnerable given their lack of specific experience. The normative upshot of this is that Posner uses the existence of compliance luck to drive another wedge between everyday morality and tort law. To some extent, this notion also applies to breach notification.

It is reasonable to speculate that compliance luck will increase the role of luck in contributing to data breaches, thus exacerbating unfairness concerns. Moreover, the role of compliance luck is likely substantial where objective standards of care need to be implemented using software.[300] Because of the technological gap between a firm's duties and the technological implementation of

[292] Doreen McCallister, *Chinese Hackers Are Likely Responsible for Marriott Data Breach, Reports Say*, NPR (Dec. 12, 2018, 6:07 AM), https://www.npr.org/2018/12/12/675983642/chinese-hackers-are-responsible-for-marriott-data-breach-reports-say [https://perma.cc/8CWZ-86YS].

[293] *Id.*

[294] *See id.*

[295] For those uncomfortable with the classification of this example as mere luck, we offer an alternative analysis in our discussion of "activity levels" below. *See infra* Section III.B.1.

[296] Raymond L. Grp. LLC, *Marriott Has Another Data Breach*, NAT'L L. REV. (Apr. 8, 2020), https://www.natlawreview.com/article/marriott-has-another-data-breach [https://perma.cc/FM96-44HB].

[297] *See id.*

[298] *See* Goldberg & Zipursky, *supra* note 273, at 1126.

[299] Richard A. Posner, *A Theory of Negligence*, 1 J. LEGAL STUD. 29, 31 (1972).

[300] *See* James Grimmelmann*, Regulation by Software*, 114 YALE L.J. 1719, 1732–33 (2005).

these duties, complying with a standard of care using software architecture is highly challenging and might result in multiple errors even if a firm has the right intentions.[301] The opaque nature of programming and the difficulties in testing a software system's resilience lead to luck contributing to the existence of breaches and therefore potentially unfair outcomes.

3. Remedial Luck

A far more relevant fairness-based concern follows from the remedial structure of data breach notification schemes, which are uniquely sensitive to luck.[302] With many criminal and civil penalties, the fine (or other punishment) is relatively fixed.[303] For instance, speeding violations often carry a fixed fine based on how far over the speed limit a driver was traveling.[304] Even if penalties vary slightly among wrongdoers (for instance, given the specific nature of the victims and their needs), such variance is relatively predefined and thus rests on moral and legal justifications.[305] Judicial processes are unpredictable as well, yet they are mostly bound by the language of the law, judicial precedent, and the experience of judges.[306] All of these elements limit the potential variation inherent in fines, rulings, and remedies—and, therefore, the role of luck.

The severity of the reputational sanctions and other damages that firms face after data breach notification, however, do not follow from fixed, predictable penalties; they result from unpredictable external effects. These effects are not subject to constraints that typically limit judicially imposed penalties. Following breach notification, firms may also be subjected to another set of more predictable harms such as governmental fines and customer lawsuits, yet it is often the

[301] *Id.* at 1737.

[302] The effect of luck on the overall extent of damages paid is part of the broader discourse on moral luck, yet the breach notification context provides important elements. *See, e.g.*, Goldberg & Zipursky, *supra* note 273, at 1140 (discussing tort law's tolerance for moral luck in determining damages under doctrines such as the thin-skull rule).

[303] For federal criminal penalties, there is some flexibility in sentencing because of the ruling in *United States v. Booker*, which provided judges the latitude to impose sentences outside of the range suggested by the Federal Sentencing Guidelines. 543 U.S. 220, 226–27 (2005). Still, the variance in criminal sentencing is likely to be constrained, as it is subject to a "reasonableness" review. Piper Aircraft Co. v. Reyno, 454 U.S. 235, 257 (1981). Reputational sanctions are not bound by any limiting principle, so sanctions may not materialize in some cases where they are obviously warranted and vice versa. *See* Liam Murphy, *The Artificial Morality of Private Law: The Persistence of an Illusion*, 70 U. TORONTO L.J. 453, 454 (2020) ("In big societies . . . the effectiveness of reputational sanctions will be limited to discrete industries, with repeat players."). At the state level, many penalties are fixed. *See* COUNCIL ECON. ADVISERS, WHITE HOUSE, FINES, FEES, AND BAIL: PAYMENTS IN THE CRIMINAL JUSTICE SYSTEM THAT DISPROPORTIONATELY IMPACT THE POOR 1 (2015), https://obamawhitehouse.archives.gov/sites/default/files/page/files/1215_cea_fine_fee_bail_issue_brief.pdf [https://perma.cc/DQ5M-D4H4]. This is particularly true for traffic infractions and some other infractions. *See id.* at 2. Often, these penalties are set by the State Supreme Court. *See, e.g.*, Va. Sup. Ct. R. 3B:2–3C:2 [hereinafter Va. Rule 3]; *see also* Goldberg & Zipursky, *supra* note 273, at 1141.

[304] *See* Va. Rule 3, *supra* note 303.

[305] Some criminal justice theorists have suggested that "day fines" (which are derived from the offender's income) would be a superior alternative to fixed fines. *See* Beth A. Colgan, *Graduating Economic Sanctions According to Ability to Pay*, 103 IOWA L. REV. 53, 56 (2017).

[306] *See* Larry Alexander, *Constrained by Precedent*, 63 S. CAL. L. REV. 1, 16–17 (1989).

reputational harms that provide the strongest disciplinary effect.[307] These include instances in which clients, suppliers, and future employees may choose to avoid the firm, or the firm's stock price falls after the breach is disclosed.

The extent of the reputational harm that a firm experiences and suffers after a data breach is a result of many factors, including luck, which leads to fairness concerns. As Roy Shapira notes, reputational effects are not wholly determined by the fact that a firm caused a bad outcome.[308] Some corporate misbehavior, such as reckless environmental pollution, often carries little reputational harm.[309] As chance would have it, a firm's disclosure of a data breach might be overshadowed by other news that just happens to occur around the same time as the disclosure.

Furthermore, the damages resulting from reputational sanctions are partially determined by how and whether a certain event is covered by the media, which is often subject to luck.[310] For instance, the severity of harm may be influenced by whether those in charge of the initial security structure are still employees of the firm.[311] In other situations, reputational harm depends on whether news outlets suggest the firm was at fault.[312] Thus, the reputational sanctions across firms which experience breaches are likely to be inconsistent, noisy, and thus, unfair.[313]

Alongside these problems that lead to uncertain reputational effects, firms do not simply stand aside and let consumers form opinions that lead to reputational harm. Firms affirmatively try to control the narrative and present their own version of the story.[314] Companies routinely invest in coordinated public relations campaigns to downplay the significance of their misconduct.[315] Firms could even time disclosures when reputational effects will be minimized, such as disclosing right after, rather than before, an earnings report. The success of these tactics is unclear, yet it might lead to unfair outcomes as well. It is important to recognize that the flexibility in breach reporting obligations provided by many U.S. states enables this form of gaming and exacerbates the role of luck.[316]

Finally, the actual harm that consumers face is a matter of luck. Moreover, because luck underlies the strength of reputational and other sanctions, these penalties depend largely on fortune. For instance, if a data breach occurs and a large percentage of individuals whose data was breached experience quantifiable harms, as in identity theft cases, then they are likely to form and disseminate

[307] *See* Roy Shapira, *Reputation Through Litigation: How the Legal System Shapes Behavior by Producing Information*, 91 WASH. L. REV. 1193, 1195 (2016).

[308] *Id.* at 1202.

[309] *Id.* (claiming that firms face very little reputational harm from getting caught polluting the environment or bribing government officials).

[310] *Id.* at 1226 (describing the complex web of factors that produces reputational harm after airline crashes).

[311] *See id.* at 1202.

[312] *Id.* at 1226.

[313] *Id.* at 1200.

[314] *Id.* at 1198.

[315] *Id.*

[316] See *supra* notes 40–44 and accompanying text.

stronger negative opinions about the breached firm, leading to stronger reputational sanctions. Of course, this requires that harms from data breach be traceable to specific breach incidents, which is difficult. Indeed, consumers might attribute identity theft incorrectly or to firms which exposed their information most recently.[317] This would lead to even more unpredictability (and chance) in the effects of reputational sanctions. And while some forms of personal information are more sensitive than others, luck will account for a great deal of variance between similar firms and situations.

In addition to remedial luck's role in creating reputational costs, the tertiary effects of notifications follow a similar logic. These might include the damage resulting from the analysis of these events by journalists, the interest of regulators, and the attention of legislators and their staffs. These are all dynamics that cannot be taken lightly and, according to Schwartz and Janger, will prove influential.[318] Reporter interests, however, as well as those of regulators and legislators, are fickle and very difficult to predict. And while the severity of the breach will no doubt have an impact on the potential attention of these actors (as well as the firm's media savviness in timing and delivering the information), many external circumstances can influence the outcome here as well.[319] This all leads, again, to substantial fairness concerns that firms behaving similarly will suffer different outcomes.

4. *Caveats and Workarounds*

The focus on unfairness issues (many of which derived from the concept of moral luck) might seem vexing to some readers, as they have been for some tort theorists. Others, however, might be quite underwhelmed given several intuitive responses. We explore these responses, as well as their strengths and weaknesses.

a. Data Breaches Under Reasonable and Unreasonable Security Standards

The analysis above addresses the potential unfairness resulting from luck-driven hacks. It, however, arguably conflates at least two different sets of institutional actors that have different levels of blameworthiness—those who practiced reasonable security and those who did not. Arguably, acceptable unfairness-based concerns only arise in the former cases, where the firm is not blameworthy yet faces reputational sanctions after notification.

To further explain, consider the following scenarios. First, a firm may exercise an inappropriately low level of security, which leads to a breach. Here, the firm acted wrongly and is forced to follow notification procedures leading to reputational sanctions. Alternatively, a firm may follow best security practices and may design their digital systems accordingly. Nonetheless, given the specific attributes of the digital age discussed above, this firm's systems might still be

[317] *Cf.* Shapira, *supra* note 307, at 1205.

[318] Schwartz & Janger, *supra* note 5, at 955–56.

[319] *See id.*

breached, particularly by highly skilled adversaries, such as nation states.[320] Although this firm has not acted wrongfully, it is forced to follow notification procedures and bear those associated costs. We concede that the "unfairness" argument is more intuitive and persuasive in the latter case.

Even in cases where firms fail to exercise adequate security standards, luck is still a principal factor in determining if a breach occurs, yet the strength of the fairness-based argument is undermined. Nonetheless, just because a firm fails to take adequate security steps, a breach is far from guaranteed. Many firms that have inadequate security systems will not experience a breach. This is largely because cyberattacks are often random.[321] Therefore, a similar firm exercising security measures that are just as poor will suffer no consequence (akin to the reckless driver who, fortuitously, did not cause an accident in the famous Waldron hypothetical).[322]

While luck does play a role in the outcome when a firm is at fault, one would be pressed to find this outcome unfair given the firm's poor practices. To some degree, this dynamic mirrors the outcomes of selective enforcement and auditing initiatives, which are an integral part of regulation and enforcement.[323] In all these cases, specific firms are singled out as wrongdoers and sanctioned (although, with selective enforcement, this is done intentionally for efficiency reasons, rather than randomly for luck-related reasons). Partial enforcement and punishment are generally considered acceptable if they are not driven by corruption or an ulterior motive.[324]

A possible unfairness argument might still arise if the harm to the breached (yet negligent) party is disproportionate to the actual wrongs to the various affected parties. Yet this is only rarely considered a constraint (limited to situations in which the consequences are especially dire).[325] In addition, and as the discussion on compliance luck earlier makes clear, there is some limited sense of unfairness in situations where a firm strives to meet objective security standards yet fails—and is later breached. Here, the unfairness is in comparison to firms that were successful in meeting the accepted security standards.

The fairness argument, however, has greater bite in situations where two or more firms exercise proper security standards, yet only one experiences a breach and the others do not. Here, again, luck is playing a substantial part, yet many would agree that the outcome is unfair. Not only is a firm subjected to the harsh

[320] For more on these forms of attacks, see *infra* notes 395–98 and accompanying text.

[321] *How Cyber Attacks Work*, NAT'L CYBER SEC. CTR. (Oct. 14, 2015), https://www.ncsc.gov.uk/information/how-cyber-attacks-work [https://perma.cc/H3L6-G5BM].

[322] *See supra* notes 270–81 and accompanying text.

[323] Ronen Perry & Tal Z. Zarsky, *"May the Odds Be Ever in Your Favor": Lotteries in Law*, 66 ALA. L. REV. 1035, 1073–77 (2015).

[324] For instance, in the context of profiling, which is feared to be driven by racial bias. *See id.* at 1076; *see also* FREDERICK SCHAUER, PROFILES PROBABILITIES AND STEREOTYPES 177 (2003).

[325] *See* Perry & Zarsky, *supra* note 323, at 1076; *see also* Youngjae Lee*, The Constitutional Right Against Excessive Punishment*, 91 VA. L. REV. 677, 683–87 (2005). See *State Farm Mut. Auto. Ins. Co. v. Campbell*, 538 U.S. 408, 429 (2003) for information on the upper level of punitive damages (which is quite high) and thus another form of disproportionate punishment.

realities of breach notification, it has carefully practiced adequate security just as others that have not been affected.

b. The Adequacy of Fairness

In addition, some readers will question the appropriateness of this fairness (luck-related) concern altogether. Indeed, the strength of this concern depends principally on one's underlying theoretical view of tort law. According to many perspectives, luck is a feature of tort law, rather than a bug. The concern over fairness is likely to be felt most strongly through corrective justice visions of tort law that justify the tort system on thick moral concepts, such as fairness and wrongs.[326] By contrast, consequentialist views of torts—such as those embodied by law and economics, which focus primarily on ensuring appropriate incentive structures—are less likely to be concerned about the potential for unfair outcomes due to moral luck.[327]

Further, under a consequentialist understanding of tort law, the potential unfairness that results from sanctioning a single firm that failed to implement reasonable security practices and experienced a breach, while other similarly situated firms were not breached, is muted. Here, the principal justification for data breach notifications is whether these laws promote better security practices.

Assessed through this prism, breach notification is likely to be an important intervention because it appears to incentivize firms to make investments in data security.[328] Consequentialists might struggle to justify breach notification in instances where firms maintain adequate security practices and yet suffer breaches. They might nonetheless be in favor of this regulatory scheme, however, because notification provides even greater incentives for security. Such incentives are important in an environment which seems to lean towards underinvestment and generates substantial negative externalities.[329]

Alongside consequentialist views of torts, civil recourse theory manages to sidestep the luck-related conundrum.[330] Civil recourse theory applies to the foundations of tort law by explaining that torts provide an avenue for aggrieved parties to vindicate wrongs against them.[331] Thus, it could be naturally deduced that when a potential tortfeasor acts negligently but—as luck would have it—there is no damage and no aggrieved party, tort law does not apply.[332] Therefore, on a theoretical level at least, the luck factor does not generate a substantial fairness challenge. According to civil recourse theory, the firm that fails to implement

[326] *See generally* Ernest J. Weinrib, *Corrective Justice in a Nutshell*, 52 U. TORONTO L.J. 349, 349 (2002) (providing an overview of corrective justice).

[327] *See* William M. Landes & Richard A. Posner, *The Positive Economic Theory of Tort Law*, 15 GA. L. REV. 851, 851 (1981).

[328] *See* Winn, *supra* note 5, at 1133.

[329] This argument runs parallel to the discussion of strict liability. *See supra* notes 245–56 and accompanying text.

[330] Goldberg & Zipursky, *supra* note 273, at 1135–38.

[331] Benjamin C. Zipursky*, Civil Recourse, Not Corrective Justice*, 91 GEO. L.J. 695, 738 (2003); *see also* John C.P. Goldberg & Benjamin C. Zipursky, *Accidents of the Great Society*, 64 MD. L. REV. 364, 402–03 (2005).

[332] Goldberg & Zipursky, *supra* note 273, at 1138–39.

proper security but experiences a breach is different in kind from the set of firms that act unreasonably but are not breached.[333] As a result, breach notification does not treat equivalent firms differently because one firm has wronged consumers by exposing their information.

Wrongs in the breach notification context, however, might present a unique challenge to civil recourse theory, thus bringing back the analytical difficulties moral luck imposes. Even in cases where a firm stores information in a reckless fashion (without breach), there still may be a wronged party.[334] Data subjects' information has been stored in an unprotected setting, thus compromising their data protection rights. They, however, are blocked from receiving a remedy due to luck. This argument would work particularly well in the EU, which recognizes a fundamental right of data protection, including the right of data security.[335] Note, however, that those subscribing to the civil recourse theory may still reject the moral luck-based argument when firms meet reasonable security standards. This is because it is quite difficult to conceptualize harm to the data subjects in this case. It should also be noted that breach notification laws are not necessarily a subset of tort law, thus tempering this critique (which is of more limited force in the criminal law context).

c. Risk Pooling Response and its Limits

Practically, moral luck arguments and the fairness concerns that follow are often mitigated by pooling risk through insurance. If all risks are pooled, then the impact of luck is sharply mitigated.[336] Lucky firms share the burden with the unlucky ones.[337] The introduction of insurance limits critiques premised on unfairness resulting from luck (or lack thereof), especially for repeat players that contribute to an insurance pool over extended periods of time.[338] In other words, the existence of insurance measures allows tort law to contain the potential unfairness of luck-related harms.

Simply falling back on insurance to offset potential unfairness issues in this specific context, however, is likely to be ineffective or normatively undesirable, at least in the short run. First, data breach notification statutes impose and generate non-economic costs on firms that experience data breaches.[339] As other forms of reputational harms, they are difficult to quantify and assess in advance,

[333] Zipursky, *supra* note 331, at 747–48.

[334] Arthur Ripstein performs a similar analytical move in discussing whether civil recourse theory must account for the "wrong" that results from creating risk even though no injury occurs. *See* Arthur Ripstein, *Closing the Gap*, 9 THEORETICAL INQUIRIES L. 61, 68 (2008).

[335] GPDR, *supra* note 2, at 36 (Recital 39) (indicating that personal data shall be processed "in a manner that ensures appropriate security of the personal data").

[336] Baker, *supra* note 272, at 171.

[337] *Id.*

[338] *Id.*; *see also* LEE ANNE FENNELL, SLICES AND LUMPS: DIVISION AND AGGREGATION IN LAW AND LIFE 200 (2019).

[339] Winn, *supra* note 5, at 1144.

and therefore are very challenging to pool.[340] They are incomplete and unreliable.[341] These future harms therefore might be excluded by insurers. Alternatively, the inherent difficulty of underwriting insurance policies to protect against breach events might lead to disfunction in the overall market for cyber-insurance.[342] Second, notifications exacerbate the chance of being subjected to fines, which might not be covered by insurance policies, creating a risk that cannot be pooled.[343]

These problems, however, may be transitional. Over time, the negative stigma and harm to reputation from breaches might slowly disappear as breaches become common and widespread. Ironically, broad breach notification might even contribute to this outcome. In addition, the fallout from breaches might be easier to assess, model, and predict given the additional data and experience gathered, making them more amenable to insurance.[344] Yet, given the dynamic nature of this context, risks might also continue to change, leaving the option to pool effectively constantly behind keeping this critique applicable.

B. Activity Levels

1. Firm/Tortfeasor Activity Level

An additional set of complications arises from examining how breach notification laws relate to activity levels. Similar to luck-related critiques, activity level is a foundational concept in tort theory.[345] To understand the notion of activity level, consider an unsophisticated observer of tort law who might wrongfully conclude that rules defining reasonable levels of care (such as breach notification rules) merely govern the standard of care firms choose to exercise. Yet a more nuanced view recognizes that tort law and other regulatory measures influence the relevant firm's level of activity as well.[346]

Liability is in fact a function of both the standard of care and the firm's activity.[347] Even if the standard of care the firm adopts remains stable, greater activity would lead to greater liability and associated costs (and reduced activity will lessen the overall liability).[348] For this reason, tort theorists have been quick

[340] Yet insurance companies are beginning to meet this challenge and offer reputation policies. For scholarship addressing this new trend, see BROKING FAC. NEW GENERATION GRP., CHARTERED INS. INST., REPUTATION RISK IN A SOCIAL MEDIA CULTURE: HOW WELL IS THE INSURANCE MARKET RESPONDING? 6 (2015), https://www.cii.co.uk/media/6834133/reputation_risk_in_a_social_media_culture_1.pdf (last visited Mar. 27, 2021) [https://perma.cc/K5JD-3SPF] (discussing scholarship addressing this new trend); *see also* DANUTA SZWAJCA & SOŇA CHOVANOVÁ SUPEKOVÁ, REPUTATION RISK INSURANCE AS A NEW PRODUCT ON THE INSURANCE MARKET 56 (2018), https://papers.wsb.poznan.pl/sites/papers.wsb.poznan.pl/files/ZN_WSB_P_ART/ZNPoz_79_D_Szwajca_S_Chavanova_Supekova.pdf [https://perma.cc/FC7C-ZLNG].

[341] *See* McGeveran *supra* note 147, at 1172.

[342] *See* Lubin, *supra* note 81, at 27.

[343] *See id.* at 56–58 (discussing the challenge of insuring against the prospect of fines in this context).

[344] *See* McGeveran, *supra* note 147, at 1172.

[345] *See* Shavell, *supra* note 13, at 7.

[346] *See id.*

[347] *Id.* at 2–6.

[348] *See id.*

to point out that setting various standards of care indirectly regulates firms' activity levels.[349] The opposite is true as well, higher/lower levels of activity (of various forms we will discuss below) will lead to higher/lower levels of damages awarded, even when the level of care remains constant.[350] The analysis here assumes that firms believe that maintaining a stable level of care is possible. And further, given the technical form of this context, this belief is reasonable.[351]

These insights directly lead to several context-specific conclusions and policy recommendations, depending on whether the activity produces beneficial or harmful externalities. In other words, depending on our economic assessment and social view of the activities the firm performs, we can attach a value to the activity (either positive or negative) and incorporate it into an overall equation which includes standards of care and damages.[352]

Generally, tort theorists explain that standards of reasonableness encourage firms to over-perform their activity once they meet the standard of care (thus engaging in over-activity of a risky action).[353] For instance, when operators of a motor pool adopt and comply with a "reasonableness" standard of care, they will likely implement all the minimum security requirements in their trucks to assure they are not found to be liable, and then set their trucks on the road to the greatest extent possible.[354] By contrast, under a strict liability regime (i.e. where liability is exclusively a product of causing a bad outcome), tort liability will usually lead to reduced activity, possibly even to a sub-optimal level.[355] As demonstrated by these examples, tort law has substantial difficulties calibrating and achieving optimal activity levels. Therefore, additional regulation is often necessary to properly calibrate activity level.[356]

Let us now return to understanding the impact of breach notification laws and properly calibrating them to achieve social objectives. The precise impact of the levels of activity in the analysis depends on whether the standard of care is either negligence or strict liability. As we explained above, breach notification is often categorized as the latter,[357] yet it does not easily fit within either paradigm. For the purpose of this analysis, however, we will assume that breach notification

[349] *See id.*

[350] *See supra* note 13 and accompanying text.

[351] *See* FENNELL, *supra* note 338, at 196–99. Fennell goes on to explain that the literature draws a distinction between automated and manual care that should therefore call for different tort regime. *Id.* Given the fact that data security calls for a specific mix of both, we choose to refrain from implementing this strain of the literature to our analysis.

[352] Landes & Posner, *supra* note 327, at 877.

[353] For a recent review of this literature, see FENNELL, *supra* note 338, at 196.

[354] *See* ROBERT COOTER & THOMAS ULEN, LAW & ECONOMICS 234 (6th ed. 2016), http://www.econ.jku.at/t3/staff/winterebmer/teaching/law_economics/ss19/6th_edition.pdf [https://perma.cc/982E-4HSA] ("If the legal standard is set at the social optimum, then exceeding the legal standard of precaution has more social costs than benefits. For the actor, however, private benefits increase significantly when his precaution reaches the legal standard because he escapes liability.").

[355] Keith N. Hylton, *The Theory of Tort Doctrine and the Restatement (Third) of Torts*, 54 VAND. L. REV. 1413, 1419 (2001).

[356] David Gilo & Ehud Guttel, *Negligence and Insufficient Activity: The Missing Paradigm in Torts*, 108 MICH. L. REV. 277, 288–89 (2009).

[357] *See* Winn, *supra* note 5, at 1144.

regulation resembles strict liability, given its focus on outcome rather than on the actual levels of care taken.[358]

With this in mind, let us examine the incentives of firms operating in a few possible legal jurisdictions. In the absence of breach notification requirements, data security would be left to governmental regulation and private litigation—but solely driven by a reasonableness standard.[359] Therefore, one might speculate that firms will tend to engage in "over-activity." That is, firms will excessively collect and analyze data because they are insufficiently deterred by the standard of care.[360] Even though personal data collection and analysis carries some value, we will assume that this conduct can potentially generate substantial social drawbacks.[361] Enter breach notification laws. These add an additional layer of (to some extent) strict liability and might therefore contribute to optimizing the activity levels of firms.

According to this analysis, the implications of breach notification laws are significant: they optimize overall activity and, therefore, the actual extent of data security risks and breaches. Admittedly, there are other ways to achieve this same objective—notably, by enacting specific laws regulating data usage.[362] Indeed, this response is already in place in some legal regimes.[363] The GDPR, for instance, includes a "purpose minimization" principle which requires that data collection should be limited to what is necessary.[364] California's recently enacted CCPA limits the "sale" of personal information to external entities.[365] Therefore, with such laws in place, breach notification laws might be unnecessary to calibrate proper activity levels. Breach notifications, however, are nonetheless essential for calibration at this time, at least in the U.S. as laws regulating data collection and use are not on the books in most U.S. states. Even with data-usage laws in place, their enforcement is quite challenging.[366] Thus, the strict liability-like regime breach notification laws bring about is necessary to ensure that firms keep their activity level socially optimal.

It is also possible that an opposite problem could occur. Firms might respond to data security rules which set reasonable standards by decreasing their activity levels rather than improving their security.[367] In discussing this option, the activity level literature also distinguishes between regimes with different

[358] *See supra* notes 245–256 and accompanying text.

[359] As is the case in most jurisdictions. *See* discussion in *supra* notes 229–230 and accompanying text.

[360] *See* FENNELL, *supra* note 338.

[361] This notion might be challenged under the argument that excessive collection and analysis of personal information is socially beneficial given the various advantages they might produce. Clearly, that perspective would lead to a very different analysis.

[362] *See infra* notes 363–366 and accompanying text.

[363] *See, e.g.*, GDPR, *supra* note 2, at 7 (Recital 39) ("The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed.").

[364] *Id.* at 35 (Article 5(1)(c)).

[365] CAL. CIV. CODE § 1798.135(a)(1) (West 2020).

[366] *See generally* Sangchul Park, *Why Information Security Law Has Been Ineffective in Addressing Security Vulnerabilities: Evidence from California Data Breach Notifications and Relevant Court and Government Records*, 58 INT'L REV. L. & ECONS. 132 (2019).

[367] *See* Gilo & Guttel, *supra* note 356, at 296–297.

costs of precautions for risk avoidance.[368] Data security is most likely achieved by high fixed costs and low marginal costs.[369] For such cases, the literature suggests that negligence-based rules might lead firms to merely decrease activity rather than to adopt proper precautions.[370] This would be an unfortunate outcome for individuals whose data is being collected and held in an insecure system, as they will face a heightened risk of data breach (and its subsequent pain). In short, this response limits the number of people whose data is collected but increases the risks to those included in the database.

In this scenario, let us consider the impact of breach notification laws (and their strict liability-like attributes). Yet again, they prove to play an important role. The prospects of notifications will incentivize firms to engage in higher levels of security regardless of their low activity levels – leading to an optimal outcome.[371] As above, similar objectives could be met by direct regulatory intervention, such as regulation ensuring optimal security levels by audits and *ex post* fines.[372] Similar laws exist in the EU[373] and in many U.S. states.[374] Yet, again, these latter regulations might be faulty and limited in scope (given the substantial challenges to effective enforcement as well as possible problems with standing).[375] Therefore, the broad application of breach notification law might achieve proper security even for firms that chose to scale back their activity levels.[376]

Applying the activity level perspective opens the door to a broad set of questions and possible distinctions. For instance, firms might engage in activity level adjustments in other dimensions (beyond the *extent* of collecting personal data). Such adjustments might include increasing or limiting the customer base or tinkering with the overall number of transactions. Yet, because projections of what firms might choose to do is highly speculative, we refrain from further developing this notion. The same could be said regarding the users' activity. Information regarding breaches might impact the user's consent to provide personal

[368] *Id.* at 296.

[369] *Id.*

[370] *Id.* at 291–92.

[371] UNIV. OF CAL. BERKELEY SCH. OF L., SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS 14 (2007) [hereinafter SECURITY BREACH NOTIFICATION LAWS], https://www.law.berkeley.edu/files/cso_study.pdf [https://perma.cc/2JFM-2H9H] ("Requiring organizations to give notice of breaches exposes them to potential liability, which in turn may encourage them to translate this risk into heightened data protection.").

[372] *See id.* at 15 ("[S]ecurity breach notifications did not top the list of drivers behind security investment decision, but neither were they completely ignored . . . . Most information officers interviewed were more concerned about the regulatory scrutiny of other agencies such as the Securities Exchange Commission . . . the Department of Health and Human Services . . . or one of the financial agencies . . . .).

[373] *See* GDPR, *supra* note 2, at 51–52 (Article 32).

[374] *Security Breach Notification Laws*, *supra* note 1.

[375] Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295, 339–43 (2019) (discussing issues with legal standing).

[376] There is yet an additional option–that breach notification laws will provide over-deterrence, leading firms to engage in sub-optimal data analysis practices. Given the substantial negative externalities associated with excessive data retention, as well as the difficulties surrounding this assertion, we leave its exploration for another time.

information, or their contribution to such database.[377] Again, given the speculative nature of this analysis, we choose to set it aside.

Firm size raises another complication for the activity level analysis. Again, given the highly speculative nature of such an analysis, we merely outline some basic intuitions. It is possible that breach notification notices generate greater incentives to larger firms (*i.e.*, firms with greater activity levels) in comparison to smaller ones. This is due to the more substantial fallout notifications of breaches would entail for them.[378] Here, Schwartz and Janger have already asserted that reputational effects are not uniform across industry players.[379] They suggest that larger firms may place a higher value on their reputation, investing more resources in safeguarding this valuable asset.[380]

Yet firm size may actually cut in the opposite direction. Smaller firms without an established reputation may fear reputational sanctions because this could be the only information that consumers or investors have about them.[381] Moreover, small firms may have a harder time establishing consumer goodwill after a data breach because they are likely to have fewer brand-loyal customers.[382] We therefore remain inconclusive as to the relation between firm size, activity levels, and incentives to secure data. Yet once clear evidence unfolds, the overall legal regime should be calibrated to assure optimal activity levels by setting different legal rules for the different sized firms.

2. *Hacker "Activity"*

The "classic" tort theory literature on activity levels goes beyond an analysis of the actions of the tortfeasors and their relation to liability. It also examines the interactions between the victims' level of activity, the tort regime, and damages.[383] Breach notification, however, brings forward yet another factor into the equation—the activity of the hacker. Breaches are different in kind from accidents or natural disasters. They are not only a result of the actions or omissions of the tortfeasor but also the efforts of an adversary—the hackers.[384] The more

[377] *See* Sasha Romanosky et al., *supra* note 5, at 257 (2011) ("[T]he US Government Accountability Officer (GAO) has stated that 'notification to the individuals affected . . . has clear benefits, allowing people to the opportunity to take steps to protect themselves against the dangers of identity theft.'").

[378] *See* SECURITY BREACH NOTIFICATION LAWS, *supra* note 371, at 36 ("The larger the organization, the more important a brand name and reputation becomes to its ultimate success . . . . Smaller businesses . . . are also less likely to be caught if they choose not to notify.").

[379] Schwartz & Janger, *supra* note 5, at 930 (discussing large firms, like Lotus, which place a higher premium on their reputation).

[380] *Id.*

[381] *See* Yadin, *supra* note 259, at 442–43.

[382] *See id.*

[383] Shavell, *supra* note 13.

[384] As discussed above, this situation somewhat resembles that of premises liability. *See supra* note 233 and accompanying text.

they attempt to attack, the greater chance they will have to succeed and thus generate liability for the relevant platform.[385] In the wake of successful attacks, mandatory notifications will follow and cause substantial damage to affected firms.

On its face, it is unclear how this dimension of activity might generate normative concerns. From an efficiency-based standpoint, greater hacking risk should generate the prospect of greater liability. Breach notifications would direct liability to the firms which are often the most efficient bearers and spreaders of risks to invest in security measures. Fairness concerns also should not necessarily arise, as the firms subjected to greater liability have caused greater harm which they should have anticipated. Yet, as we will now demonstrate, the hacking activity level follows unique patterns that are at times unpredictable, and thus might lead to market distortions and inefficiencies.[386] They might also lead to unfairness when similar entities are subjected to different risks and liability prospects.

While the level of hacker activity is impossible to establish *a priori*, we can introduce several rules of thumb to predict them. To do so, we must account for the different motivations for "black hat" hacking (as well as the identity of such hackers). These include monetary gain (by selling data on the black market for future identity theft or other abusive actions), bragging rights, going after "low hanging fruit" (easy hacks), or operations by governments and their agents.[387] When considering these motivations and hacker profiles, several heuristics regarding hacker activity naturally follow.[388]

First, hackers are likely to be drawn to databases containing information which has a high value on secondary black markets.[389] Such data would most likely be of the greatest subjective value to the data subjects. This would include

[385] *See* GABRIEL WEIMANN, U.S. INST. PEACE, SPECIAL REPORT NO. 119, CYBERTERRORISM: HOW REAL IS THE THREAT? 6 (2004) ("[T]he variety and number of targets are enormous. The [hacker] could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so forth. The sheer number and complexity of potential targets guarantee that [hackers] can find weaknesses and vulnerabilities to exploit.").

[386] *See generally* James Daly, *Mitigating Risk: A Day with a Cybersecurity Analyst*, WIRED (Nov. 2016), https://www.wired.com/brandlab/2016/11/mitigating-risk-day-cybersecurity-analyst/ [https://perma.cc/Y36D-AP4X] ("Staying ahead of malicious hackers means staying on your toes. Some of the most sophisticated hackers rely on the use of so-called 'zero day' exploits, unique attacks that take advantage of previously unknown software holes to get into systems before the vender has a chance to fix them.").

[387] For a similar taxonomy, see Steven Bellovin's hacking "threat matrix" which includes joy hacks, opportunity hacks, targeted attacks and advanced persistent threats (organized along the axes of skill and degree of focus). STEVEN M. BELLOVIN, THINKING SECURITY: STOPPING NEXT YEAR'S HACKERS 34–35 (Brian W. Kernighan ed., 2015); *see also* Justin (Gus) Hurwitz, *Response to McGeveran's The Duty of Data Security: Not the Objective Duty He Wants, Maybe the Subjective Duty We Need*, 103 MINN. L. REV. HEADNOTES 139, 148–51 (2019).

[388] Lillian Ablon et al., Rand Corp., Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data, Testimony before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance (Mar. 15, 2018), https://www.rand.org/pubs/testimonies/CT490.html [https://perma.cc/K7MY-LMW5] (describing, in detail, the various motivations that underlie data breaches).

[389] *Id.* at 4.

identifying and financial data (enabling theft or identity theft) and perhaps intimate and health-related data (enabling blackmail and extortion).[390] In this case, the prospects of hacker overactivity are quite predictable. Therefore, relevant and rational firms should engage in greater security investment and reduced collection—all steps to limit the prospects of a potential breach and subsequent notification. As these dynamics and outcomes are predictable, they seem efficient and fair. A similar analysis unfolds when considering the enhanced activity of hackers motivated by bragging rights. They would intuitively be drawn to highly secured databases—such as those controlled by military and governmental entities, or health related facilities.[391] Again, such enhanced activity is predictable, and the additional risk of notification, as well as the enhanced steps firms will take in response, are efficient, fair, and socially valuable for the reasons we mention.

Second, hackers might flock to targets that have already been identified as vulnerable either publicly by the firm itself (evidence of a previous breach) or after being identified as vulnerable by the hacking community.[392] These targets are "low hanging fruit."[393] It is hard to find the additional exposure such firms will face given the prospect of notification to be problematic. In these cases, additional liability is fair given that it results from the firm's recklessness. And even if we consider firms that have improved security following an initial breach, the enhanced liability (given greater activity) leads to efficient outcomes; greater liability will incentivize such firms to take greater security measures in a case where these are needed.[394]

Finally, hackers might choose to focus on specific targets after being directed to do so by governmental entities.[395] Several high-profile hacks of recent years have been attributed to nation states.[396] Consider, for instance, the famous Sony Picture hack attributed to North Korea, allegedly in retaliation to some unflattering depictions of the North Korean leader in several motion pictures.[397] Hollywood studios are not often considered as "hard targets" within the crosshairs of governmental hackers and their counterparts. Neither are hotel chains (as discussed in the Marriott example above).[398]

Here, breach notification outcomes are unfair because of this enhanced form of activity and, by extension, are potentially inefficient. These outcomes

[390] *See* Eric Basu, *Cybersecurity Lessons Learned from the Ashley Madison Hack*, FORBES (Oct. 26, 2015, 11:55 AM), https://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/#2204b124c82b [https://perma.cc/5GK9-RLUZ].

[391] *Id.*

[392] *Id.*

[393] *See supra* note 387 and accompanying text.

[394] *Id.*

[395] *Id.*

[396] *See, e.g.*, Adam Janofsky, *Experts Warn: Pandemic Is 'Perfect Time' for Foreign Hackers to Strike*, PROTOCOL (Mar. 20, 2020), https://www.protocol.com/coronavirus-hackers-nation-state-sponsored [https://perma.cc/P2N4-DCP4]

[397] Richard Stengel, *The Untold Story of the Sony Hack: How North Korea's Battle with Seth Rogen and George Clooney Foreshadowed Russian Election Meddling in 2016*, VANITY FAIR: HIVE (Oct. 6, 2019), https://www.vanityfair.com/news/2019/10/the-untold-story-of-the-sony-hack [https://perma.cc/TDU7-2K3L].

[398] *See supra* notes 291–297 and accompanying text.

are inefficient because they may subject firms to a risk of substantial liability, leading to (arguably) over-investment in security,[399] or significantly less data analysis and usage. Moreover, the outcomes are unfair as the fallout resulting from the breach notification process will be very different than the outcomes (or lack thereof) impacting other similar entities exercising similar level of security. Here, additional activity leads to the breach and the notification requirement.

Regarding this latter example and argument, we concede some redundancy and inconsistency in our discussion. In our analysis above, we categorized this same example (the first Marriott breach) as a manifestation of (bad) luck, and therefore unfair. Here, we reexamined this issue through the lens of activity levels and categorized it as a result of hacker hyperactivity. This dual perspective is warranted. At times, nation state attacks are random and nothing more than bad luck. Yet in other cases—such as Sony Pictures—the target selection was not random but reflected a calculated, even predicable, plan of attack.[400] Nonetheless, Sony needed to report the breach.[401] Thus, the collateral damage that followed was unfair to Sony, given its line of business and customary set of adversaries.[402]

We conclude with a final caveat: our analysis of hacker activity and breach notification policies failed to address possible implications and effects one might have on the other. This intentional omission is due to the highly speculative nature of this analysis. Here, one might speculate that breach notification policies might encourage hacking, as the notification requirement will publicize a successful hack thus encouraging hackers to attack prime targets and own coveted bragging rights. Yet on the other hand, notifications might lead to heightened security. Additional speculations might consider the possible migration of hacking activities from one context to another. Yet these basic intuitions should be confirmed through empirical testing.

IV. Bringing It All Together

A. Rethinking Justifications

Let us now briefly examine how our recent analysis of the somewhat overlooked outcomes and effects of breach notifications influences the four key justifications for applying these laws, as well as the interaction between them.

[399] FENNELL, *supra* note 338, at 218 (explaining that the role of law is also to limit instances of too much care).

[400] *See* Stengel, *supra* note 397.

[401] *See id.*; *see also supra* note 1 and accompanying text.

[402] The unfairness stemmed from the fact that, as opposed to other studios with similar security, Sony was targeted because of the specific content that it produced.

1. Deterrence

While deterrence seems to be a primary justification for breach notifications,[403] its justification is potentially compromised by potential unfair outcomes. Deterrence strives to ensure that breached firms suffer reputational sanctions.[404] At times, this might occur irrespective of whether the firms acted recklessly.[405] Some commentators have been quick to point out that treating all breached firms equally—whether they are blameworthy or not—is potentially unfair.[406] Our analysis follows this argument by detailing the extent of unfairness in the *unequal* treatment of firms with very similar security practices (while distinguishing between reasonable and unreasonable security). Similarly, when considering a retribution-based justification, unfairness and luck-based arguments similarly undermine this justification as, in some cases, firms that experience data breaches did not act wrongly.

Because of the potential for inequality and unfairness, applying notification schemes designed to promote deterrence is problematic (as opposed to when it is merely an inescapable by-product of meeting other objectives). Therefore, if regulators are convinced of the importance of deterrence, design features should be added to control for luck by rendering its impact less harsh, more predictable, and easier to pool.

In a move to balance fairness and deterrence, breach notification statutes might define "personal information" and "breach" narrowly in order to limit the scope of the law.[407] In addition, the negative features that accompany deterrence could be softened by including language in the public notice (or allowing such language) which implicates the role of luck in this process.[408] Looking more broadly, it might be necessary to limit standing by only allowing plaintiffs to bring legal action when the firm who held their data acted negligently (thus rejecting calls to expand security-based torts to a strict liability regime). Similarly, the exceptions for notification should be interpreted broadly to allow firms that undertake reasonable security measures (such as applied encryption)[409] to escape the notification requirement.[410] Another possible exception would provide immunity from notification requirements if the firm adhered to a pre-determined

[403] *See* discussion *supra* Section II.B.1; Solove & Citron, *supra* note 97, at 781.

[404] Marian K. Riedy & Bartolomeij Hanus, *Yes, Your Personal Data is at Risk: Get Over It!*, 19 SMU SCI. & TECH. L. REV. 3, 34 (2016).

[405] Solove & Citron, *supra* note 97, at 781.

[406] *Id.* ("They thus do not deter the most blameworthy any more than the least blameworthy. Moreover, the cost of notification is not proportionate to the amount of harm that a breach might cause.").

[407] Alex Kramer, *Data Breach Bill's Scope, Harm Trigger Will Diminish Protections in Many States*, BLOOMBERG L.: TECH & TELECOM L. NEWS (Apr. 28, 2015, 11:00 PM), https://news.bloomberglaw.com/tech-and-telecom-law/data-breach-bills-scope-harm-trigger-will-diminish-protections-in-many-states [https://perma.cc/3ZJ9-LE58] (discussing the narrow proposed definition of "personal information" in the Data Security and Breach Notification Act of 2015); *see also* MASS. GEN. LAWS ANN. ch. 93H § 1 (West 2020).

[408] This language may affect the strength of the reputational sanction that a firm faces.

[409] *See* GDPR, *supra* note 2, at 52–53 (Article 34).

[410] It is important to note that exceptions to the notification requirement favor fairness to firms over the potential for consumers to mitigate harms that result from the breach.

certification process.[411] These latter suggestions aim to limit the key notion of unfairness we identified—unequal treatment of firms that applied reasonable security, but were nonetheless hacked.

Finally, we return to pooling via insurance, which might reduce fairness concerns. Pooling is challenging given the lack of predictability regarding the consequences of notification. The effects of data breaches may become more predictable if regulators and legislators agree on a regulatory freeze on these issues and if the possible damages for breaches are capped and clearly defined.

The fairness and efficiency of deterrence-focused design is further complicated when considering various issues related to activity levels. Here, given the potential failures of torts merely premised on "reasonability" standards to properly calibrate conduct, breach notification laws play a crucial role in ensuring optimal levels of activity. Thus, curbing notification due to the unfairness/luck related concerns mentioned will leave this activity level-based concern compromised. The fear of overactivity, however, could be recalibrated by direct regulation—namely, laws that mandate limited data usage and fine for insufficient security levels.[412]

The discussion of hacker activity levels highlighted the unfairness that results from sanctioning firms that are the targets of nation-state attacks. To remedy this outcome, exceptions should be carved out for such attacks. In other words, nation-state attacks might only mandate anonymous reporting to the public which is coupled with immunity from liability for the firm, or merely lead to government-initiated reports explaining the unique qualities of this attack. Alternatively, the harms that follow from reporting nation-state attacks might be pooled by government-based insurance. This might be required in any event, as it is unclear whether such attacks are covered by existing policies.[413]

2. Mitigation

Crafting a breach notification statute that prioritizes mitigation focuses almost solely on the victims of breaches. Given this focus, promoting mitigation should not be directly compromised or affected by the fairness/luck argument, which focuses on the unfairness to firms. Taken to an extreme, the possibility of unfairness could be largely avoided if mitigation is achieved without revealing the firm's identity, thus protecting firms from reputational harm. While anonymous reporting schemes generate challenges, the analysis above indicates their benefits in terms of fairness. When breach notifications that include the identity

[411] The GDPR includes an infrastructure for certification processes although these have failed to make a substantial impact for various reasons. *See* GDPR, *supra* note 2, at 8 (Article 43).

[412] For example, consider the FTC's enforcement action against Wyndham for their lax security practices. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

[413] Adam Satariano & Nicole Perlroth, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong*, N.Y. TIMES (Apr. 15, 2019), https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html [https://perma.cc/HNL6-VTNG].

of firms are distributed, some firms are harmed more than others.[414] Therefore, given the questionable effectiveness of mitigation and other potential shortcomings, "identifiable" mitigation should be limited to specific instances where it would be most effective.

Because mitigation prioritizes protecting data subjects from downstream harm,[415] mitigation-based design should have limited effects on firm activity levels (i.e. neither limiting nor enhancing activity). A possible caveat might be that mitigation-based design that entails expansive and expensive steps might burden firms and thus lead to lower activity levels (which, as noted, might be either good or bad, depending on whether the activity generates positive or negative externalities).

3. *Information Forcing*

As the activity level discussion focuses on incentivizing firms to take or refrain from taking action, it does not substantially impact the effectiveness or desirability of information forcing as a normative goal for breach notification. Similarly, at least at first glance, the fairness/luck discussion does not appear to distort the effectiveness of this justification or impact its design trajectories.

However, the luck-based discussion illuminates a crucial weakness in the effectiveness of information forcing. The information streaming from breach notifications does not necessarily identify a full picture of faulty security practices. If those forced to provide information are merely the unluckiest, then the dataset does not necessarily reflect real security failures, but random ones. This does not necessarily undermine the information forcing justification. But it emphasizes the need for a close study of additional online breaches.[416]

4. *Autonomy and Restorative Justice*

Autonomy concerns interact with notification outcomes in distinct ways. First, our discussions of unfairness and luck bring to light instances in which notification pertains to faultless breaches. In such instances, the individuals' "control" interest still mandates updating them as to their data's whereabouts.[417] However, "apologies" are not necessarily needed.[418] This would impact the language and terms required. As philosopher Linda Radzik explains, restorative justice is not an appropriate remedy in cases where the wrong is faultless (or the product of a mere accident).[419] This is because wrongs without faults do not force

[414] Sarah Hospelhorn, *Analyzing Company Reputation After a Data Breach*, VARONIS (Mar. 29, 2020), https://www.varonis.com/blog/company-reputation-after-a-data-breach/ [https://perma.cc/H29S-HM4F].

[415] *See supra* notes 109–113 and accompanying text (discussing how states' notification requirements mitigate downstream harm).

[416] *See supra* notes 163–164, 188 and accompanying text (discussing "near misses").

[417] *See supra* Section II.B.4.

[418] Linda Radzik, *Tort Process and Relational Repair*, *in* PHILOSOPHICAL FOUNDATIONS OF THE LAW OF TORTS 248 (John Oberdiek ed., 2014) (arguing that restorative justice is only appropriate when the injury was caused by "negligence, recklessness, or malice").

[419] *Id.* at 235.

the victim to reconsider their relationship to the wrongdoer.[420] By contrast, damaged relationships that are the focus of restorative justice typically only follow from wrongs that are the product of fault.[421]

Second, our analysis demonstrated the detriments of enhanced activity levels. Applying regulation that promotes and repairs autonomy by striving to "make amends" can also ideally (albeit, indirectly) reduce such levels.[422] As we speculated above, an apology might convince users that the breach was a one-time error that would not be repeated and that the firm now takes its data security duties seriously.[423] Therefore, they will remain loyal and refrain from shifting to a competitor (whose data practices might be just as bad). This, in turn, might limit switching between firms and therefore reduce the "activity level" of storing personal data overall, thus reducing the risks of breaches.

B. Crafting a Blueprint for a Model Breach Notification Scheme

Based on what we have learned thus far, let us now try and propose a regulatory scheme. The scheme strives to properly balance potential normative justifications and apply the lessons from our examination of underappreciated concepts which are related to tort theory. Structuring an optimal breach notification policy is a delicate task. Many of today's regulators fail to recognize this nuance and introduce laws which attempt to maximize on all fronts without fully appreciating the conflicting interests at stake[424] The GDPR is a classic example of a regulatory design that overlooks the need for balancing. In particular, the GDPR mandates disclosures to regulators (to gather data) and to data subjects (to mitigate their potential losses).[425] In addition, the GDPR pursues deterrence goals through a rigorous fine structure.[426] This approach risks undermining any normative goal by pursuing them all in tandem.

Yet the GDPR departs from the unconstrained maximizing paradigm in a couple of principal ways which are worth considering and potentially even adopting. For instance, the GDPR provides several nuanced exceptions to the disclosure requirement and incorporates a tiered system that differentiates between disclosures to data subjects and regulators.[427] This tiered approach implicitly recognizes the inherent tension between deterrence and mitigation.

We structure our blueprint recommendations while seeking to accommodate the four potential justifications that we have sketched so far. Given its simplicity, overall importance, and lack of substantial competing interests, we start

[420] *See id.*

[421] *See id.*

[422] *See infra* Question 3 in Section IV.B.

[423] *See supra* Section II.B.4.

[424] *See infra* notes 425–426 and accompanying text.

[425] *See* GDPR, *supra* note 2, at 52 (Articles 33 and 34).

[426] *See generally id.*

[427] *See GDPR Exemptions: Who Is Exempt from GDPR Requirements?*, HIPAA J. (May 11, 2018), https://www.hipaajournal.com/gdpr-exemptions-who-is-exempt-from-gdpr/ [https://perma.cc/UAT5-78JY].

with information forcing. An optimal data breach notification statute would implement and distinguish between short-term and long-term information forcing goals. Information forcing with immediate goals (such as notifying potential targets) should be administered under separate laws (as is the current practice) with special laws for industries that potentially involve greater harm, such as telecommunications and critical infrastructure.[428]

By contrast, information forcing that works in service of long-run objectives—such as formulating and improving security standards—should be incorporated in potentially every data breach notification statute. In order to facilitate this goal, the criteria for both personal information and "breach" for notification should be broadly defined (even broader than generally stated in most regulatory frameworks), yet firms may receive immunity for additional reporting requirements and they will be limited in scope, in instances we will detail. Again, this multi-tiered approach mirrors the design of the GDPR's Article 33.[429]

Restorative justice is currently an overlooked justification, yet we believe it should play a larger role in any ideal breach notification statute. Promoting restorative justice might move to strengthen trust between consumers and firms, promoting fairness and efficiency.[430] As a result, restorative justice should be promoted through breach notification, though empirical studies should examine its actual impact.

Because restorative justice is often largely symbolic,[431] however, it is not crucial to assure it is pursued in every instance of breach, particularly in cases where it may lead to unfair outcomes. According to this strategy, full notification including a reference to the firm's identity and wrongdoing should be limited to cases where fault and wrongdoing is more egregious. This point somewhat resembles the GDPR's Article 34 that only requires notifying the data subject in cases where there are potentially serious consequences (yet this requirement does not depend on finding fault with the information collector).[432]

Mitigation is seen by many regulators as a measure which responds to real consumer need.[433] Its utility, however, is unclear and potentially varies among sectors and over time. One potential drawback of mitigation is that the constant influx of notifications is duplicative, especially in cases where a consumer has already been notified of that specific risk, or where the breach is insignificant. In these cases, a notice that does not reveal the firm's identity may be optimal. In addition, when notifications are focused on mitigation, they must be carried out in a short time span and as soon as possible.[434]

[428] Eldar Haber & Tal Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis*, 44 FLA. ST. U.L. REV. 515, 530–35, 537, 539 (2017).

[429] *See* GDPR, *supra* note 2, at 52 (Article 33). The GDPR sets forth a two-tiered notification scheme with lenient requirements in Article 33, as opposed to the stricter ones in Article 34.

[430] *See supra* notes 212–214 and accompanying text.

[431] Erik Luna, *The Theory and Jurisprudence of Restorative Justice*, 2003 UTAH L. REV. 205, 233 (2003).

[432] *See* GDPR, *supra* note 2, at 52 (Article 34).

[433] *See supra* notes 90–97 and accompanying text.

[434] *See supra* notes 115–120 and accompanying text.

On the other hand, individual preferences might vary. Those interested in full information on breaches should be provided with it if they signal their preference in advance. As a result, some centrally planned innovations might be necessary. These would require a central regulatory agency to track repeat breaches and register the public's preferences. Doing so would enable blocking redundant notifications containing duplicative information and would ensure delivery of full information to those that indicate this preference.

Deterrence presents the most difficult challenge. When aggressively pursued, deterrence undermines fairness and impedes both mitigation and restorative justice.[435] When deterrence is only weakly pursued, it might not provide sufficient incentive for firms to invest in adequate security.[436] The key to resolving this tension is the ability to differentiate between data segments and pool risks successfully.

As discussed earlier, the sting of luck-related concerns could be mitigated by a layer of anonymous notices which would be acceptable in borderline cases. This scheme should be expanded to include breaches resulting from nation-state attacks and when the information was restored after a ransomware attack in which the victim did not pay the ransom. In all such cases, notifications should be made to the central authority as well.

Furthermore, pooling might be essential for overcoming the unfairness of luck-related concerns. Successful pooling might be possible over time with better information sharing rules and other measures detailed above. Yet the risks in some sectors will pool better than others. The banking and health sectors are relatively concentrated and populated by repeat players and therefore would most likely pool well.[437] In other sectors, however, the noted option of anonymous reporting which does not reveal the firms' name should be considered more generously.

Finally, and to assure that the weakening of regulations that aim to enhance deterrence does not lead to unacceptable risky activity levels, regulators must strengthen ancillary rights which ensure that proper activity levels are maintained, like the data minimization requirements presented in the GDPR, and enforcing reasonable security levels, as the FTC is striving to do. California's newly enacted CCPA is one initial step in this direction.

The following presents a summary of these recommendations in the format of the design questions discussed throughout this analysis, with additional ancillary rules required to achieve a proper balance and calibrate the key justifications:

[435] *See supra* Section II.B.1 (discussing deterrence effects on mitigation); *supra* notes 208–209 (discussing deterrence effects on restorative justice).

[436] *See supra* note 56 and accompanying text.

[437] It therefore should be no surprise that in the EU, banking contexts feature specific breach notification schemes. See Directive 2015/2366, of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC, 2015 O.J. (L 337) 35, 105 (discussing "incident reporting").

Question #1: What forms of information should be included in the definition of "personal information" that breach notifications refer to?

As broad as possible—and should reflect the meaning of "personal information" in other contexts.

Question #2: What constitutes a breach, triggering the notification process?

A tiered process must be established. The lowest tier, which requires notifications to the central authority, should be as broad as possible—so to even include "near misses." To ensure full disclosure, immunity should be considered for faultless breaches. A second tier would include more severe breaches which might cause damage to individuals and thus justify available mitigation measures (for instance, if it pertains to usernames and passwords). Yet it would not include loss or inaccessibility to data.

Question #3: Who must receive the notification? What would the notification include?

An optimal response would distinguish between the tiers noted above. All breaches should be reported to a central entity. Only breaches in the second tier would be reported to individuals, yet here too there would be several distinctions regarding the identification of the breaching firm, as detailed below. Second-tier breaches should also be reported to state A.G.s and credit agencies.

Identity of breached firm: could be omitted when the breach is insignificant or when:

The hack is a reoccurring event (as recorded in a central register).

The hack involves a mere system lock-out resulting from an unpaid ransomware attack.

The hack resulted from a suspected nation-state attack.

Identity should be revealed: all other second-tier breaches, hacks in the health and financial sectors (given efficient pooling), and when an individual requests actual reporting in advance.

Content: in egregious cases (to be defined): must include admitting of wrongdoing, apology, and attempt to make amends. Generally, the language of the notifications should focus on mitigation. Firms should be permitted to include language which reflects on the role of luck in the breach, and, if relevant, the security measures they reasonably applied.

Question #4: How promptly must a firm comply with their disclosure obligations?

For second-tier breaches requiring mitigation: as soon as possible. For deterrence/data sharing: 30–45 days.

Question #5: What exceptions should be introduced to these requirements?

Consider applying exceptions from notifications to individuals if the breach was only revealed more than three years after the breach occurred (after good faith monitoring had transpired). Continue providing encryption-based exceptions. Consider an exception for personal (as opposed to governmental) disclosure if firms exercised high security standards and were nonetheless hacked by nation-states.

Overall Policy: Consider moratorium to the legal structure to enable risk assessment and pooling.

For Future Examination and Re-Assessment: impact of making amends; varying impact on different firm sizes; examine the effectiveness of mitigation and risk pooling.

Ancillary rights:

1. Rights regarding limiting usage of personal information are essential.
2. Laws generating an obligation for reasonable data security are important.
3. Cyber insurance and pooling should be promoted, while considering government-backed (or event initiated) insurance for nation-state attacks.
4. Other measures to collect breach-related information must be applied.
5. Standing in breach notification cases should serve as a reasonable barrier (in the interest of limiting deterrence and apologies).

V. Conclusion

According to Wired magazine, Professor Deirdre Mulligan led the charge that integrated breach notification into California state laws.[438] Since then, breach notification laws have become popular data security tools across the world. Rigorous theoretical thinking has been a staple of breach notification and a motivating force behind this unique regulatory scheme from its inception. It is only fitting, therefore, that as this scheme comes of age, it returns to the academic drawing board for rethinking and refitting. This Article provides the initial blueprint for doing so.

* * *

[438] Kim Zetter, *California Looks to Expand Data Breach Notification Law*, WIRED (Mar. 6, 2009, 6:07 PM), https://www.wired.com/2009/03/ca-looks-to-exp/ [https://perma.cc/JNR8-V65E].