UNREASONABLE: A STRICT LIABILITY SOLUTION TO THE FTC'S DATA SECURITY PROBLEM

James C. Cooper[*] *& Bruce H. Kobayashi*[**]

ABSTRACT

For over two decades, the FTC creatively employed its capacious statute to police against shoddy data practices. Although the FTC's actions were arguably needed at the time to fill a gap in enforcement, there are reasons to believe that its current approach has outlived its usefulness and is in serious need of updating. In particular, our analysis shows that the FTC's current approach to data security is unlikely to instill anything close to optimal incentives for data holders. These shortcomings cannot be fixed through changes to the FTC enforcement approach, as they are largely generated by a mismatch between the tools that Congress gave it over a century ago and what it needs to foster firms' incentives to mimic socially optimal levels of care for the data they hold. Not only does the current framework likely suffer from informational deficiencies attendant to its focus on "reasonable" security that render liability standards uncertain, it also lacks the ability to obtain the type of relief that will force firms to internalize the costs of their data security decisions. We examine the problem of data security enforcement through the lens of the economics of optimal precautions and identify several reasons why a strict liability regime administered by the FTC, under which firms pay for the expected harm from breaches they cause, is likely to be superior to the current framework that revolves around the concept of reasonableness. The benefits of strict liability flow from the likelihood that firms do not fully internalize the costs and benefits of their data security decisions and the relatively large informational burdens associated with measuring actual and optimal care under a negligence regime. We also show why in this informational environment, strict liability is better than negligence for developing a vibrant cyber insurance market, allowing for data security regulation to

* Associate Professor of Law and Director of the Program on Economics & Privacy, Antonin Scalia Law School.

** Paige V. and Henry N. Butler Professor of Law and Economics, Antonin Scalia Law School.

We would like to thank Tom Baker, Sasha Romanosky, Ted Rosenbaum, Andrew Stivers and participants at the Cyber Insurance and Cyber Resilience Workshop, University of Pennsylvania Law School for comments on earlier drafts. All errors are the authors.

be de facto outsourced to insurers who will contract with firms for optimal levels of care. Because these private contracts will harness private information on costs and benefits from precautions, they are likely to incentivize more efficient behavior.

TABLE OF CONTENTS

I. INTRODUCTION

Data breaches are ubiquitous. They are no longer surprising or newsworthy, and now are just part of the background noise of everyday life.[1] The list of well-known data breaches that have allowed hackers to acquire sensitive personal and financial information is large, including well-known national retail firms,[2] tech platforms,[3] banks,[4] health insurers,[5] and even federal and state agencies.[6] And this is just the tip of the iceberg—unpublicized breaches swamp those that are reported in the media.[7] Even with the announcement of

1. Julia Carpenter & Bourree Lam, *The Capital One Hack: Life in the Time of Breach Fatigue*, WALL ST. J. (Aug. 4, 2019, 3:49 PM), https://www.wsj.com/articles/the-capital-one-hack-life-in-the-time-of-breach-fatigue-11564824600.

2. *See, e.g.*, Paul Ziobro & Danny Yadron, *Target Now Says 70 Million People Hit in Data Breach*, WALL ST. J. (Jan. 10, 2014, 8:36 PM), https://www.wsj.com/articles/SB10001424052702303754404579312232546392464; Shelly Banjo, *Home Depot Hackers Exposed 53 Million Email Addresses*, WALL ST. J. (Nov. 4, 2014, 8:03 PM), https://www.wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309282; David Uberti, *Marriott Reveals Breach That Exposed Data of Up to 5.2 Million Customers*, WALL ST. J. (Mar. 31, 2020, 4:29 PM), https://www.wsj.com/articles/marriott-reveals-breach-that-exposed-data-of-up-to-5-2-million-customers-11585686590.

3. Robert McMillan & Deepa Seetharaman, *Facebook Finds Hack Was Done by Spammers, Not Foreign State*, WALL ST. J. (Oct. 17, 2018, 8:46 PM), https://www.wsj.com/articles/facebook-tentatively-concludes-recent-hack-was-perpetrated-by-spammers-1539821869; Greg Bensinger & Robert McMillan, *Uber Reveals Data Breach and Cover-up, Leading to Two Firings*, WALL ST. J. (Nov. 21, 2017, 11:38 PM), https://www.wsj.com/articles/uber-reveals-data-breach-and-cover-up-leading-to-two-firings-1511305453; Robert McMillan, *LinkedIn 2012 Data Breach May Have Hit Over 100 Million*, WALL ST. J. (May 19, 2016, 6:55 PM), https://www.wsj.com/articles/linkedin-2012-data-breach-may-have-hit-over-100-million-1463675653; Joshua Jamerson, *Myspace Breached by Hackers Before Memorial Day Weekend*, WALL ST. J. (May 31, 2016, 9:19 AM), https://www.wsj.com/articles/myspace-breached-by-hackers-before-memorial-day-weekend-1464700772; Robert McMillan & Ryan Knutson, *Yahoo Triples Estimate of Breached Accounts to 3 Billion,* WALL. ST. J. (Oct. 3, 2017, 9:23 PM), https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804.

4. Peter Rudegeair, AnnaMaria Andriotis & David Benoit, *Capital One Hack Hits the Reputation of a Tech-Savvy Bank*, WALL ST. J. (July 31, 2019, 5:30 AM), https://www.wsj.com/articles/capital-one-hack-hits-the-reputation-of-a-tech-savvy-bank-11564565402.

5. Anna Wilde Mathews & Danny Yadron, *Health Insurer Anthem Hit by Hackers*, WALL ST. J. (Feb. 4, 2015, 9:39 PM), https://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720.

6. John D. McKinnon & Laura Saunders, *Breach at IRS Exposes Tax Returns*, WALL ST. J. (May 26, 2015), https://www.wsj.com/articles/criminals-steal-taxpayer-data-via-irs-web-service-1432672691; Damian Paletta, *OPM Breach Was Enormous, FBI Director Says*, WALL ST. J. (July 8, 2015, 6:39 PM), https://www.wsj.com/articles/breach-was-enormous-fbi-director-says-1436395157. This list also includes our employer. *See* Cara Garretson, *George Mason University Suffers Security Breach*, NETWORK WORLD (Jan. 12, 2005, 12:00 AM), https://www.networkworld.com/article/2318057/george-mason-university-suffers-security-breach.html.

7. *See* Michael Hill & Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (July 16, 2021, 2:00 AM), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (designating Yahoo's 2013 breach, which the company publicly announced three years later, as the biggest breach).

record fines,[8] the seemingly endless parade of data breaches has generated criticisms of the current regulatory system. Much of this criticism has been directed towards the Federal Trade Commission (FTC),[9] which claims the title of "the nation's primary privacy and data security enforcer."[10] Indeed, the FTC's recent no-money settlement with Zoom involving allegedly poor data security practices prompted one Commissioner to bemoan what he sees as the FTC's "ineffective" approach to data security.[11]

Of course, simply observing that there are a large number of data breaches is not necessarily evidence that something is wrong with the current regulatory system. It is well known from the tort literature that when precautions are costly, accident-causing activity is beneficial, and ex-post remediation is cheap, the optimal number of accidents is not zero.[12] But when actors do not fully internalize the external costs of their activity, the result is too much activity and too many accidents. The quintessential example of the consequences of uninternalized spillover effects are firms that do not bear the full costs of industrial pollution they generate when producing socially valuable products like refined fuel or pesticides.[13] In such cases, the aim of enforcers is not to deter activity altogether—foregoing all the value generated by these products would impose too great a cost on society. Rather, efficient regulation forces the firm to internalize the full external costs of their activity, thereby fostering private incentives both to take optimal precautions against harm and to produce at socially optimal levels.[14]

---

8. For example, the consumer reporting agency Equifax agreed to settle charges with a variety of government agencies and the states for a $100 million civil penalty and at least $425 million dollars to help those affected by the data breach. *See Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, FED. TRADE COMM'N (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

9. *See, e.g.*, Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2237–46 (2015).

10. *See FTC Releases 2018 Privacy and Data Security Update*, FED. TRADE COMM'N (Mar. 15, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-releases-2018-privacy-data-security-update.

11. Dissenting Statement of Commissioner Rohit Chopra at 2, *Regarding Zoom Video Communications, Inc.*, Matter No. 1923167 (F.T.C. Nov. 6, 2020), https://www.ftc.gov/system/files/documents/public_statements/1582914/final_commissioner_chopra_dissenting_statement_on_zoom.pdf.

12. *See* STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW 178–79 (2004).

13. Omri Ben-Shahar, *Data Pollution*, 11 J. LEG. ANALYSIS 104 (2019) (using a data pollution metaphor to argue that social intervention should focus on the external harms from collection and misuse of personal data).

14. *Id. See generally* STEVEN SHAVELL, ECONOMIC ANALYSIS OF ACCIDENT LAW 7 (1987); WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW (1987).

The same principles apply to data security.[15] Because legitimate firms' collection and use of consumer data benefit consumers, an optimal enforcement policy would not seek to eliminate the risk of harm from data breaches.[16] Indeed, if it is sufficiently expensive to prevent data breaches, or sufficiently easy to mitigate the losses from a breach and make identity theft victims whole after a breach, the socially optimal level of breaches could be quite high. To use a hyperbolic example, one could completely eliminate the risk of financial account fraud by returning to an all-cash system. Clearly, the benefits of eliminating the staggering cost of credit card fraud would pale in comparison to the marginal cost of eliminating credit cards—which would include, for example, the large negative effects such a policy would have on online commerce. Rather, an optimal enforcement policy aimed at minimizing the systemic costs of data breaches would focus on inducing firms to take precautions against harmful breaches only as long as the marginal costs of additional security measures are less than the marginal benefits from those measures.[17] It is well-known that if firms take only cost-justified precautions, the sum of breach and security costs is at a minimum. This is important, because if firms pass along these costs to consumers, the full price of the firm's product will be at its minimum, leading consumers to purchase the "correct" amount of the product. Social welfare will be maximized.[18]

There is no reason to believe that the current enforcement regime approximates an optimal enforcement policy. In this Article we employ the lens of the economics of accidents to explain why the current FTC approach to data security is unlikely to lead firms to employ optimal data security.[19] Indeed, our analysis shows that the FTC's current approach to data security—with its focus on the concept of "reasonableness" (both in liability and remedy) and its almost complete inability to secure monetary relief—is unlikely to instill anything close to optimal incentives for data holders. Since the early 2000s, the FTC creatively employed its capacious statute to target shoddy data practices. It has challenged "unreasonable" security practices directly as "unfair" and indirectly as "deceptive" if the firm broke an express or implied promise

15. *See* Ben-Shahar, *supra* note 13, at 108–110.

16. *Id.* at 135–36.

17. *See* SHAVELL, *supra* note 12 at 21–26.

18. *Id.* at 22–23.

19. This article focuses on firms' incentives and not on law enforcement strategies aimed at those expending effort to cause breaches. For a discussion of these law enforcement strategies, see Ivan P. L. Png, Chen-Yu Wang & Qiu-Hong Wang, *The Deterrent and Displacement Effects of Information Security Enforcement: International Evidence*, 25 J MGMT. INFO. SYS. 125 (2008). Additionally, the Appendix below discusses optimal mitigation strategies but does not focus on the question of protective activity and expenditures by consumers. See Ye Hong & William Neilson, *Cybercrime and Punishment*, 49 J. LEGAL STUD. 431 (2020), for an examination of the deterrence effect of punishing firms that are victims of data breaches.

to take "reasonable" data security measures.[20] Although the FTC's actions were welcome at the time to fill a gap in enforcement as the Internet exploded, after two decades, there are reasons to believe that the FTC's current approach has outlived its usefulness and is in serious need of updating. Importantly, these shortcomings cannot be fixed through changes to the FTC enforcement approach; they are largely generated by a mismatch between the tools that Congress gave it over a century ago and what it needs today to foster efficient care for consumers' data.[21]

The first problem is informational. As noted above, the FTC developed an approach to data security revolving around the concept of "reasonable" security measures.[22] Whether the FTC uses unfairness or deception to challenge a data practice, it must define the standard of data protection required given the circumstances and articulate why the defendant's practices fell short. The FTC must perform the same task when enforcing its orders, which—at least until recently—have generally required liable firms to implement reasonable precautions or face civil penalties for order violations.[23] The ability of the FTC to identify both of these measures is likely to be fraught with error, leading to both over- or under-deterrence depending on the size and the bias of the error. The second problem is remedial. The primary harm from data breaches is the increase in the risk of both direct costs and financial harm resulting from identity theft and payment card fraud, and intangible harms resulting from the compromise of potentially embarrassing personal information. The FTC's ability to make careless firms pay for this harm, however, is essentially non-existent. In the October term of 2020, the Supreme

20. *See*, *e.g.*, Complaint at 3, Grago, F.T.C. Matter No. 1723003, Docket No. C-4678 (June 19, 2019), https://www.ftc.gov/system/files/documents/cases/172_3003_c4678_clixsense_complaint_7-2-19.pdf (alleging that poor data security practices both violated promises made to customers regarding data security and were unreasonable). The FTC has also challenged as deceptive the failure to live up to promises to take specific security measures. *See, e.g.*, Complaint at 11, Zoom Video Commc'ns, Inc., F.T.C. Matter No. 1923167, Docket No. C-4731 (Jan. 19, 2021), https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint_0.pdf (alleging failure to employ promised 256-bit end-to-end encryption).

21. *See generally* James C. Cooper & Bruce H. Kobayashi, *Equitable Monetary Relief Under the FTC Act: An Opportunity for a Marginal Improvement*, 83 ANTITRUST L.J. 645 (2021) (explaining the economic incentives created by the FTC's remedial powers); Ian M. Davis, *Resurrecting Magnuson-Moss Rulemaking: The FTC at a Data Security Crossroads*, 69 EMORY L.J. 781 (2020) (discussing the FTC's remedial powers associated with data security cases).

22. Failure to take "reasonable" security measures can be both an unfair and deceptive practice to the extent that the firm made material representations. *See infra* notes 39–41 and accompanying text.

23. As discussed in more detail, *infra*, while the FTC can predicate liability on failure to take reasonable security measures, the Eleventh Circuit decision in *LabMD* casts doubt on the extent to which the FTC can design orders requiring defendants to employ "reasonable" security measures. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1235–37 (11th Cir. 2018). As a result, post-*LabMD* order have become more specific. *See infra* notes 55–57 and accompanying text.

Court held that the FTC Act does not allow the FTC to obtain equitable monetary relief for first-time violations.[24] This leaves only the administrative path, which also limits the FTC to non-monetary injunctive relief.[25] The upshot is that in its current state, Section 5 of the FTC Act suffers from uncertain liability standards and an inability to force firms to internalize the costs of their data security decisions. Importantly, this state of affairs has implications beyond FTC enforcement. Although the FTC Act does not provide a private right of action, it is not an airtight compartment; private plaintiffs can rely on the FTC's reasonableness standard to make out claims related to data breaches under state law.[26]

We consider three possible approaches the FTC could take to ameliorate the current situation: (1) a laissez-faire approach, where the FTC polices express deception, but relies on market forces to be the primary source of incentives for firms to supply data protection; (2) a negligence rule, which is similar to the status quo, but would have firms pay for the harm they cause when they fail to take reasonable care; and (3) a strict liability rule, that would have firms pay for expected harm caused by a breach, regardless of the level of care taken. A standard result in the economics of accidents literature is that each of these approaches will lead firms to employ optimal security in a world of perfect information.[27] In practice, however, given the limits on information about both harm and cost of care, and the interdependent nature of security, the real-world application of these standards are likely to lead to divergent outcomes and differing rates of error.[28] We analyze the relative net benefits of each approach, and identify several reasons why a strict liability regime is likely to be superior to the current framework that revolves around the

24. AMG Cap. Mgmt., LLC v. Fed. Trade Comm'n, 141 S. Ct. 1341, 1347–52 (2021).

25. The FTC can obtain civil penalties for subsequent violations of administrative orders and can seek certain monetary remedies in federal court following a successfully litigated administrative case for conduct that a reasonable person would have known was "fraudulent or dishonest." *See* Cooper & Kobayashi, *supra* note 21, at 647.

26. *See, e.g.*, *In re* Equifax, Inc. Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1327–28 (N.D. Ga. 2019). Plaintiffs also use the § 5 standard to make out claims under California's Business and Professions Code § 17200. *See, e.g.*, Complaint at 30, Rahman v. Marriot Int'l, Inc., No. 8:20-cv-00654, 2021 WL 346421 (C.D. Cal. June 29, 2020).

27. *See* SHAVELL, *supra* note 12, at 9.

28. This result and the analysis in this article generally are related to the economic literature on the choice of regulatory instrument in the presence of uncertainty. While the choice of regulatory instruments (e.g., tradeable permits versus emissions taxes in environmental regulation, or the use of price versus quantity regulation of a natural monopolist) perform similarly with perfect information, the relative performance will be dependent upon case-specific factors under conditions of uncertainty. *See, e.g.*, Nathaniel O. Keohane, Richard L. Revesz & Robert N. Stavins, *The Choice of Regulatory Instruments in Environmental Policy*, 22 HARV. ENV'T L. REV. 313 (1998); Martin L. Weitzman, *Prices vs. Quantities*, 41 REV. ECON. STUD. 477 (1974). In the context of liability for data security, the relevant choice of regulatory instruments is between definition measurement of what constitutes "reasonable security" under a negligence /reasonable security approach, and the definition and measurement of ex-ante harm generated by a data breach under a strict liability approach.

concept of reasonableness. The benefits of strict liability flow primarily from the likelihood that absent some sort of liability regime, firms will not fully internalize the costs and benefits of their data security decisions, and the relatively large informational burdens associated with measuring actual and optimal care under a negligence regime that are likely to lead to enforcement errors.[29]

The time is ripe for this reform. Congress has been aflutter with various privacy and data security proposals in response to recent data breaches and privacy scandals,[30] and there is no sign that this appetite for reform will abate with the new administration.[31] Indeed, a recent FTC settlement with Zoom showcases the Democratic Commissioners' frustration with what they see as an impotent FTC.[32] Further, recent legal setbacks have raised serious questions about the FTC's remedial authority: in addition to the Supreme Court eliminating the FTC's ability to obtain equitable monetary relief in federal court in *LabMD*, the Eleventh Circuit casted serious doubt on the FTC's ability to enforce its administrative orders dealing with data security.[33] Both of these legal developments have renewed calls to give the FTC broader remedial authority, including the ability to obtain civil penalties. This ability could be used to implement a strict liability regime that requires firms to pay for the expected consumer harm from their breaches.[34]

---

29. The Antitrust Injury doctrine, set out in *Brunswick Corp. v. Pueblo Bowl-O-Mat, Inc.*, 429 U.S. 477 (1977), incorporates a similar approach that focuses on remedies and not the substantive law to control incentives in private antitrust suits. *See* John E. Lopatka & William H. Page, *Brunswick at 25: Antitrust Injury and the Evolution of Antitrust Law*, 17 ANTITRUST 20, 24 (2002); William H Page, *Antitrust Damages and Economic Efficiency: An Approach to Antitrust Injury*, 47 U. CHI. L. REV. 467 (1980).

30. *See, e.g.*, Data Protection Act of 2020, S. 3300, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/senate-bill/3300; Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/senate-bill/3456/text.

31. Jedidiah Bracy, *What Could a Biden Administration Mean for Privacy, Cybersecurity?*, INT'L ASS'N OF PRIV. PROS. (Nov. 9, 2020), https://iapp.org/news/a/what-could-a-biden-administration-mean-for-privacy-cybersecurity; Kristin L. Bryan et al., *Election 2020: Looking Forward to What a Biden Presidency May Mean for Data Privacy and Data Privacy Litigation*, NAT'L L. REV. (Nov. 12, 2020), https://www.natlawreview.com/article/election-2020-looking-forward-to-what-biden-presidency-may-mean-data-privacy-and.

32. Dissenting Statement of Commissioner Rohit Chopra, *supra* note 11.

33. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1235–37 (11th Cir. 2018).

34. It would be impossible for the FTC to operationalize a strict liability standard under its current § 5 authority because (1) it lacks civil penalty authority for first violations; and (2) is statutorily mandated to perform a cost-benefit analysis to find an act or practice unfair. *See* 15 U.S.C. § 45(n). At least one legislative proposal would impose strict liability. *See, e.g.*, Data Breach Prevention and Compensation Act of 2018, S. 2289, 115th Cong. (2018) (imposing strict liability and federal notification requirements on credit reporting agencies for data breaches). The bill provides civil penalties of $100 for each consumer whose name and at least one item of personally identifying information was compromised, plus an additional $50 for each additional item of personally identifying information compromised for each consumer. *Id.* § 4(b)(2)(A).

Finally, it is important to note that we are not the first to reach a similar conclusion. Over a decade ago, drawing an analogy between the reservoir of water in *Rylands v. Fletcher* and the reservoirs of data held by firms, Professor Danielle Citron argued that strict liability is preferable to negligence in dealing with data breaches.[35] Although we reach a similar conclusion, our analysis differs from hers in important ways, and makes several novel contributions. First, our proposal is not to expand liability under tort law doctrine, but rather for a federal agency, such as the FTC, to act as the national regulator of data security with broad preemptive effect.[36] Second, the results backing our proposal derive from the rigorous application of the workhorse optimal care model, in which a firm responds to various liability rules by minimizing the sum of precaution and liability costs. Applying a consistent economic framework allows us to highlight the key informational advantages of a strict liability approach centered on remedies that are based on the harm caused by the breach.[37] In particular, we show how strict liability is likely to be more robust to regulatory errors than a negligence-based standard. Finally, we show why strict liability is superior to negligence for developing a vibrant cyber insurance market in this informational environment, which will allow data security regulation to be *de facto* outsourced to insurers who will contract with firms for optimal levels of care. This facet of our analysis suggests that to the extent that the informational advantages of strict liability make

35. Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007). Like we do, she explains why negligence is unlikely to be up to the task because uncertain standards and enforcement can lead to over-deterrence. *Id.* at 263–64. Moreover, the failure of consumers to appreciate the residual risk associated with even optimal levels of security will create incentives for them to share too much data. *Id.* at 264–66. Further, she also suggests that strict liability may have an advantage by spreading data breach costs across all consumers. *Id.* at 285–87. In more recent work, Professor Solow-Niederman recognizes the shortcomings of privacy torts to reach the harm from data breaches, and advocates for a tort based on a breach of duty of confidentiality. Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J. 614 (2018). Recognizing that data breaches are most likely a unilateral care situation because consumers are unlikely to have the ability to avoid data breaches, she proposes a modified version of strict liability that would apply only to firms that failed to follow a "well-instantiated security guideline or . . . established security standard." *Id.* at 631–32. Because imposition liability would still be based on the firm failing to comply with a negligence-type established level of care, her approach is a negligence-based approach that eliminates some of the traditional defenses to liability (e.g., the actions of third-party hackers as a *superseding* cause). Moreover, her analysis does not address hard to define and uncertain level of care standards discussed below and in Citron, *supra* note 35.

36. Ben-Shahar also examines public law alternatives to private suits under tort law, including command and control data regulation, data taxes, as well as publicly enforced liability for breach. Ben-Shahar, *supra* note 13, at 133–48. His analysis incorporates the use of harm-based sanctions for breached firms, but he does not analyze the relative benefits of using a strict liability regime over a negligence-based regime. *See id.*

37. Professor Citron's analysis does not address the critical role of optimal harm-based remedies play in moderating incentives in a strict liability system, or the feasibility of using harm-based remedies in practice. *See* Citron, *supra* note 35.

underwriting data breach risks easier, it will allow for the development of private cyber insurance contracts that harness diffuse private information on costs and benefits from precautions held by insurers that cover many entities.

The remainder of this Article is organized as follows. Part II describes the FTC's current approach to data security. Part III applies a stylized version of the "optimal precautions" model to the data security context, and Part IV investigates whether the market alone can provide optimal levels of data security, answering the question in the negative. Part V presents the central claim of our Article and analyzes the relative costs and benefits of a negligence regime (which approximates the FTC's current approach), and a strict liability approach, finding the latter to be superior. This part also explores how a strict liability system is superior to one based on reasonableness to foster a robust cyber insurance market, which would facilitate an even more efficient use of information. Part VI discusses how a strict liability system would be operationalized in practice, and Part VII concludes.

II. FTC'S CURRENT APPROACH TO DATA SECURITY

Section 5 of the FTC Act gives the FTC broad authority to pursue firms engaged in "unfair and deceptive acts or practices."[38] As applied, the FTC's data security enforcement program has centered around the concept of reasonableness. As the FTC explained on the occasion of its fiftieth data security settlement:

> The touchstone of the [FTC]'s approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. . . . [T]he [FTC] has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.[39]

This standard comes directly from the FTC's unfairness authority under Section 5, which condemns conduct that creates "substantial injury to consumers" that is not outweighed by benefits to consumers or competition.[40] The

38. 15 U.S.C. § 45(a).

39. *See* FED. TRADE COMM'N, STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT (Jan. 31, 2014).

40. 15 U.S.C. § 45(n). Similarly, the Safeguards Rule under Graham-Leach-Bliley (GLB) requires covered firms to take data security precautions that is appropriate given the company's size, complexity, and scope of business, as well as the sensitivity of the data at issue. 16 C.F.R § 314.3 (2022).

FTC has used this approach to condemn practices that it alleges puts sensitive data at substantial risk that could have been avoided at minimal cost. For example, in its case against TJX, which concerned a data breach involving nearly several million payment card accounts, the FTC alleged that practices such as storing and transmitting payment card information in plain text, failing to use firewalls, not requiring strong passwords for administrative logins, or failing to employ standard measures to detect unauthorized network access or patching software were unfair.[41]

Importantly, the FTC does not require a breach to trigger the use of unfairness—shoddy security practices that raise the *risk* of harm will suffice. For example, *LabMD* involved the inadvertent placement of sensitive medical information on a peer-to-peer network without any evidence that third parties actually accessed the data.[42] More recently, the unfairness count in the FTC's settled complaint against Zoom alleged only that by circumventing certain security measures in Safari, Zoom introduced potential vulnerabilities; it did not allege any unauthorized access of consumer data or authorized viewing of Zoom meetings.[43]

The FTC also brings data security cases based on deception. Some of these cases involve breaches of specific promises, such as using certain types of encryption.[44] The FTC will also import the notion of reasonableness into deception when they allege that a company's general commitments to protecting data gives rise to an implied claim that it will take reasonable care of consumers' data.[45] For example, in the recent case involving Support King's "stalkerware" app SpyFone, the FTC alleged that Support King's promise to "take all reasonable precautions to safeguard customer information" was deceptive because the defendant in fact "did not take all reasonable precautions

41. Complaint, TJX Companies, Inc., F.T.C. Matter No. 0723055, Docket No. C-4227 (Aug. 1, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxcomplaint.pdf.

42. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1224–25 (11th Cir. 2018). The only third-party known to have accessed the data was Tiversa, a data security firm that eventually reported its finding to the FTC when LabMD would not pay Tiversa for data security services. *Id.* This tip led to the case against LabMD, and subsequent Congressional hearings and litigation involving possible impropriety. *Id.* at 1225 & n.7.

43. *See* Complaint, Zoom Video Commc'ns, Inc., *supra* note 20, at 8–10.

44. *See, e.g*., *id.* at 11–12; Complaint at 6, Credit Karma, Inc., F.T.C. Matter No. 132 3091, Docket No. C-4480 (Aug. 13, 2014), https://www.ftc.gov/system/files/documents/cases/1408creditkarmacmpt.pdf.

45. *See, e.g*., Complaint at 5, Credit Karma, Inc., *supra* note 44; Complaint at 6, Uber Techs., Inc., F.T.C. Matter No. 152 3054, Docket No. C-4662 (Oct. 25, 2018), https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_complaint.pdf.

to safeguard customer information and information stored in Respondent's database was not encrypted."[46]

What emerges from the FTC's history of data security enforcement is a negligence-like reasonable security standard, but one without clear guidance of what satisfies the standard.[47] All but three of the FTC's data security cases have settled, and only one of the litigated cases has required a judicial determination of whether a firm's data security practices were unreasonably lax.[48] Because the security practices challenged by the FTC have almost exclusively been far below a reasonableness standard,[49] the complaint allegations in settlement documents provide only information about what very poor security practices look like—that is, the cases provide a lot of information about what type of practices the FTC will consider unreasonable, but very little about what type of practices might *satisfy* a reasonableness standard. To fill this gap, the FTC has publicized some closing letters, and more recently has provided guidance concerning practices that are likely to meet a reasonableness standard in publications like Start with Security and Stick with Security.[50]

---

46. Complaint at 4, 6, Support King, LLC, F.T.C. Matter No. 1923003, Docket No. C-4756 (Dec. 20, 2021), https://www.ftc.gov/system/files/documents/cases/1923003c4756spyfonecomplaint_0.pdf.

47. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

48. The only litigated cases are *Fed. Trade Comm'n v. Wyndham*, 799 F.3d 236 (3d Cir. 2015); *LabMD, Inc. v. Fed. Trade Comm'n*, 894 F.3d 1221 (11th Cir. 2018); and *Fed. Trade Comm'n v. D-Link Sys. Inc.*, No. 3:17-cv-00039, 2017 WL 65168 (N.D. Cal. Jan. 5, 2017) (settled in 2019). In *LabMD*, the administrative law judge did not find the FTC had showed a likelihood of substantial consumer injury, so did not reach the reasonableness of LabMD's practices. Initial Decision at 82–87, LabMD, Inc., F.T.C. Matter No. 1023099, Docket. No. C-9357 (Nov. 13, 2015), https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf. The FTC, however, overturned this decision, and held that LabMD's practices were unreasonable. Opinion of the Commission, LabMD, Inc., F.T.C. Matter No. 1023099, Docket. No. C-9357 (July 29, 2016), https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf.

49. FTC data security cases have been referred to as "low hanging fruit," and include challenging practices like giving never changing default passwords for networks that store credit cards or transmitting sensitive information over unsecure networks in plain text. *See, e.g.*, *Wyndham*, 799 F.3d at 240–41; Complaint at 2, BJ's Wholesale Club, Inc., F.T.C. Matter No. 0423160, Docket No. C-4148 (Sept. 20, 2005), https://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305comp0423160.pdf; Complaint at 2, TJX Cos., Inc., F.T.C. Matter No. 0723055, Docket No. C-4227 (July 29, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxcomplaint.pdf.

50. *See, e.g.*, Letter from Maneesha Mithal, Assoc. Dir., Div. of Priv. and Identity Prot., Fed. Trade Comm'n, to Dana Rosenfeld, Kelley Drye (Nov. 12, 2014), https://www.ftc.gov/system/files/documents/closing_letters/verizon-communications-inc./141112verizon-closingletter.pdf; Letter from Maneesha Mithal, Assoc. Dir., Div. of Priv. and Identity Prot., Fed. Trade Comm'n, to Reed Freeman, Morrison & Foerster LLP (Mar. 12, 2010), https://www.ftc.gov/sites/default/files/documents/closing_letters/netflix-inc./100312netflixletter.pdf; Letter from Maneesha Mithal, Assoc. Dir., Div. of Priv. and Identity Prot., Fed. Trade Comm'n, to Lisa J. Sotto, Hunton & Williams LLP (Aug. 10, 2015), https://www.ftc.gov/system/files/documents/closing_letters/nid/150810morganstanleycltr.pdf.

Nonetheless, the FTC's data security "jurisprudence" does not provide the same type of information to potential injurers as common law negligence, where a myriad of judicial decisions map out the line between reasonable and unreasonable conduct.

If the current FTC approach to data security is akin to negligence, it comes with an important caveat that severely hinders its ability to effect optimal deterrence. In tort law, a plaintiff can recover damages when the defendant's unreasonable conduct proximately caused the harm.[51] It is the threat of having to pay for the harm caused by unreasonable conduct that forces internalization of the externality and provides incentives for defendants to take reasonable care. Although Section 5 unfairness and deception claims related to promises to take "reasonable care" mimic the negligence standard under tort law, the FTC cannot force this needed internalization because it is unable to secure monetary relief for the harm caused by unreasonable data security practices.

Almost all of the FTC's data security cases have been brought as administrative complaints.[52] If the defendant does not settle with the FTC, staff will litigate the case before an administrative law judge (ALJ), with the decision appealable to the full Commission and ultimately a federal appellate court.[53] In administrative litigation, the FTC can obtain injunctive relief, including orders that prohibit a defendant from continuing to engage in conduct that violates the FTC Act, as well as reporting requirements, and "fencing-in" relief that prohibits the defendant from engaging in conduct that does not violate Section 5, but nonetheless may help deter future violations.[54] In the context of data security, the FTC typically obtains a mandatory injunction, which until 2018, essentially required defendants to maintain reasonable security.[55] However, in *LabMD*, the Eleventh Circuit held that orders requiring a defendant "to meet an indeterminable standard of reasonableness" were vague, and thus unenforceable.[56] This has led the FTC to craft more specific process requirements in its data security orders.[57]

---

51. *See* RESTATEMENT (SECOND) OF TORTS § 281 (AM. L. INST. 1965).

52. *See supra* note 48.

53. 15 U.S.C. § 45(b).

54. *Id.*

55. For example, the order in LabMD was typical, requiring defendant to "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers." Final Order at 2, LabMD, Inc., F.T.C. Matter No. 1023099, Docket No. 9357 (July 28, 2016), https://www.ftc.gov/system/files/documents/cases/160729labmdorder.pdf.

56. LabMd, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1236 (11th Cir. 2018).

57. *See, e.g.*, Decision & Order, Grago, F.T.C. Matter No. 1723003, Docket No. C-4678 (June 19, 2019), https://www.ftc.gov/system/files/documents/cases/172_3003_clixsense_decision_and_order_7-2-19.pdf. For example, the FTC order requires the defendant to implement an "information security program . . . designed to protect the security, confidentiality, and

The FTC can collect substantial civil penalties (over $40,000 per violation) for violations of administrative orders.[58] Further, although the FTC Act allows the FTC to obtain a monetary judgment in federal court following an administrative proceeding, this power could almost certainly never be used in a data security case. Section 19 allows the FTC to obtain monetary relief in federal court against parties who have lost in administrative litigation, subject to the limitation that a reasonable person would have known that the conduct at issue was "dishonest or fraudulent."[59] Thus, for this avenue to be available to the FTC, it must litigate and win an administrative case, and more importantly, the security lapses must be so extreme that they could be characterized as something a reasonable person would have known was "dishonest" or "fraudulent."[60] These high hurdles have limited the FTC's use of Section 19 to twice in the past 30 years, and make it even more unlikely that it would be a feasible strategy in the data security context.[61]

Another obstacle to the FTC's ability to effectively deter unreasonable data practices is that the Supreme Court has held that Section 13(b) of FTC Act does not allow the FTC to obtain monetary relief in federal court.[62] Although there are various proposals in Congress to restore the FTC's power,[63] it is important to note that even before *AMG*, the FTC was only able to obtain remedies such as disgorgement or restitution, which typically are limited to some measure of revenue obtained from consumers for the product or service under scrutiny.[64] Importantly, these equitable remedies do not cover harm to consumers that did not contract directly with the firm (as typically would be the case for harm caused by a breach at a credit reporting agency or data broker) or consequential damages that arise when third parties misuse breached

integrity" of consumer's personal information, and mandates, focusing on processes like assessments, monitoring, and identifying responsible employees. *Id.* at 3.

58. 15 U.S.C. § 45(b). The maximum civil penalty amount has increased from $43,792 to $46,517 for violations of §§ 5(l), 5(m)(1)(A), and 5(m)(1)(B) of the FTC Act, 7A(g)(l) of the Clayton Act and § 525(b) of the Energy Policy and Conservation Act. See Adjustments to Civil Penalty Amounts, 87 Fed. Reg. 1070 (2022).

59. 15 U.S.C. § 57b(a)(2). In such an action, the FTC can obtain "rescission or reformation of contracts, the refund of money or return of property, the payment of damages." *Id.* § 57b(b).

60. The FTC could settle a § 19 case for monetary relief if it had a credible threat to bring and win an administrative case and the conduct at issue was dishonest or fraudulent.

61. *See* Fed. Trade Comm'n v. Figgie Int'l, Inc., 994 F.2d 595 (9th Cir. 1993); Stipulation of Settlement & Final Order, Fed. Trade Comm'n v. Telebrands Corp., Case 2:07-cv-03525-JAG-MCA (D.N.J. Dec. 31, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2009/01/090114finalorder.pdf.

62. AMG Cap. Mgmt., LLC v. Fed. Trade Comm'n, 141 S. Ct. 1341, 1347–52 (2021).

63. *See, e.g.*, Consumer Protection and Recovery Act, H.R. 2668, 117th Congress (2021-2022) (authorizes the Federal Trade Commission (FTC) to seek monetary relief in federal court from businesses that engage in unlawful commercial practices such as false advertising, consumer fraud, and anticompetitive conduct).

64. *See, e.g.*, Fed. Trade Comm'n v. Com. Planet, Inc., 815 F.3d 593 (9th Cir. 2016). *See generally* Cooper & Kobayashi, *supra* note 21, at 645–48, 652–58.

consumer data, such as fraudulent credit card charges or ID theft.[65] That is, the harm from the typical data breach is not likely to be remedied by disgorgement or restitution because the harm flows from third-parties stealing and misusing consumer data, not from the breached firm tricking consumers into buying something. As can readily be seen, the FTC's remedial powers are sorely lacking the ability to deter unreasonable data practices. The FTC's injunctive relief requiring certain data security practices is unlikely to mimic efficient care, and moreover applies only to the firm under order. Further, while injunctive relief the FTC can obtain probably places non-trivial burdens on some firms—especially if it requires major changes in business model—these burdens are unlikely to correlate in any meaningful way with consumer harm, which is a necessary condition to force firms to internalize the expected harm their data security practices cause. Finally, monetary remedies are available only when the defendant was engaged in "dishonest or fraudulent" conduct, which is unlikely in most data breach cases surrounding negligence. In sum, the FTC's current remedial authority are unlikely to provide any meaningful incentives for firms to invest efficiently in data security.[66]

III. THE BASIC MODEL

An economic approach to optimal enforcement regimes seeks to minimize the total social costs associated with data breach. These costs include both the harm from exposure of personal data and the cost of increased data security investments designed to reduce the likelihood of a breach, or to mitigate the level of consumer harm in the event of breach. While data breaches generate increased costs for consumers through new and existing account fraud, medical identity theft, and the exposure of sensitive information, they also induce increased investments in data security. For example, compliance

65. For example, the only viable monetary theory in the FTC's complaint accompanying the $575 million global settlement between Equifax and the FTC, CFPB, and the states was deception related to the security provided to consumers and small businesses who purchased Equifax services (such as credit scores or credit monitoring). Complaint for Permanent Injunctive & Other Relief at 15–17, 19–21, Fed. Trade Comm'n v. Equifax Inc., No. 1:19-mi-99999-UNA (N.D. Ga. July 22, 2019), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf. Had the FTC been the only agency involved in the settlement, equitable monetary relief under 13(b) would have only allowed the FTC to seek restitution for consumers and business who were deceived into purchasing these services, a miniscule sum in comparison to the core harm that came from the breach of hundreds of millions of records. It is possible that the FTC could have also pursued civil penalties for a "knowing" violation of the safeguards rule. *See id.* at 14 (alleging that Equifax had "awareness and actual knowledge" of its data security failures, which allegedly violated the Safeguards Rule). The FTC Act provides for actions in federal district court for civil penalties for a rule violation if the defendant has "actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive is prohibited by such rule." 15 U.S.C. § 45(m)(1)(A).

66. *See* Cooper & Kobayashi, *supra* note 21 at 647.

with NIST data security standards would require firms to encrypt their data, conduct assessments, and to hire third-party assessors and a chief information officer.[67] In its "Start with Security" business guide, moreover, the FTC recommends that businesses take steps that include guarding networks against various types of attacks, limiting the extent to which firms collect and store sensitive information, using strong cryptology to store and transmit confidential information, segmenting networks, monitoring network traffic, and verifying that service providers use reasonable security.[68]

Although these measures clearly make data more secure and reduce the harm from any breach that occurs, they can also generate significant costs. These costs are not limited to just direct expenditures on data security, but also to the informational costs associated with attempting to anticipate threats ex-ante. Further, to the extent that additional security and the reduced collection of sensitive data diminishes customer experience (for example, having to logon with two-factor authentication or having to change passwords frequently), increased data security can reduce product demand. Thus, from a social standpoint, the goal should not be to achieve perfect or even maximal security, but rather to foster incentives for firms to minimize *the sum* of breach and security costs. What is more, an important byproduct of minimizing total social costs is that firms will produce at the lowest possible cost, thus maximizing the consumer and producer surplus created when they sell their products. In Figure 1, we use a stylized version of the workhorse optimal precautions model from the law and economics literature to illustrate this problem. Security expenditures, s, are measured on the horizontal axis, and reduce the probability of a breach—which we define as $\phi(s)$—causing consumer harm, h. At the same time, security costs, $c(s)$, increase as s increases. The total expected social cost associated with any level of security, $TSC(s)$, is the sum of $c(s)$ and $\phi(s)\,h$.[69]

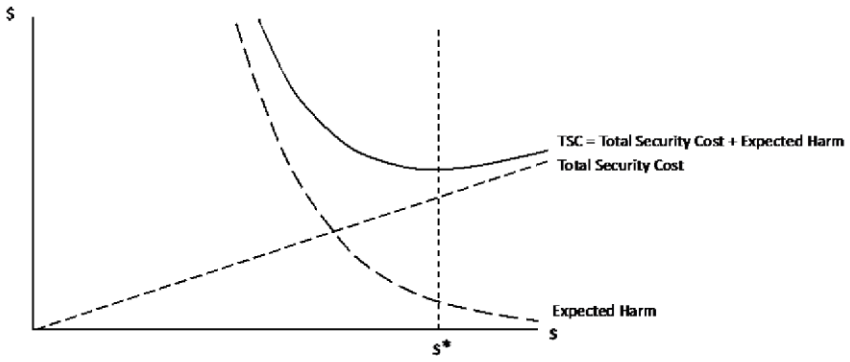
67. NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

68. FED. TRADE COMM'N, START WITH SECURITY, A GUIDE FOR BUSINESS: LESSONS LEARNED FROM FTC CASES (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

69. The model in the Appendix also allows for firms to take actions that serve to mitigate the harm when a breach occurs. Ex-post mitigation expenditures, m, decrease the per record harm $h(m)$, but come at a cost of $e(m)$, and optimal mitigation occurs when the marginal benefit of such expenditures equals the marginal cost of such expenditures. The marginal benefit of an increase in mitigation expenditures m is the reduction in harm conditional upon a breach $-h'(m)$. The marginal cost of such expenditures is $e'(m)$. Thus, the optimal level of mitigation expenditures m^* occurs where $-h'(m) = e'(m)$. In contrast to security expenditures, which are incurred ex-ante regardless of whether or not a breach occurs, mitigation expenditures have the advantage of only being incurred with probability $\phi(s)$ when a breach occurs. Further, because ex-ante prevention (s) and ex-post mitigation (m) expenditures are substitutes, increases in mitigation will reduce the optimal level of security expenditures by reducing the harm associated with a breach. Note that although security expenditures are a function of expected mitigation expenditures, mitigation expenditures are conditional on a given level of security expenditures

Total social cost is at its minimum at s^*, which as we show in the Appendix, coincides with the level of security where marginal benefit from additional security (in terms of reduced probability of a breach) is equal to its marginal cost.[70] Note that from a social perspective, we do not want harm driven to zero if security is costly. Optimal security does not occur when all breaches are deterred, but instead occurs at s^* when there are no more cost-effective—in the sense that marginal benefit is less than marginal cost—security measures to be taken.

FIGURE 1
OPTIMAL DATA SECURITY



Until this point, we have focused only on incentives to invest in data security for a *given level* of data collection. But even if a firm takes optimal care of the data it collects, it can still reduce expected data breach harms by limiting how much data it collects in the first place. Even if Home Depot and a local hardware store collect the same data from customers and employ the same security procedures, a breach at Home Depot affects a greater number of customers and is more costly to society than a breach at a local hardware store. As with decisions regarding care, decisions regarding collection involve weighing the marginal costs and benefits of additional data collection. Broadly, firms end up collecting data through two channels. First, data collection can be the artifact of a product market transaction (e.g., payment card and other sensitive information transmitted to a merchant with the purchase of a smart phone). Second, data is often itself the purpose of the transaction, as is the case when online platforms provide content and services for free and employ the information about their users to generate advertising revenue. In

because mitigation is triggered only when a breach has already occurred. It can be shown that $\frac{\partial S^*}{\partial m} = \frac{-\phi' d H^*_{m*}}{c'' + \phi'' d[h+e]} < 0$, where H^*_{m*} is the change in minimized net harm with respect to changes in the optimal level of mitigation expenditures.

70. We illustrate this condition in the Appendix.

either case, allocative efficiency requires that the marginal value of consumer data collected equals the marginal cost of acquiring it, securing it, *and* the expected harm from a breach given the firm's level of security.

To illustrate this problem, Figure 2 depicts the firm's derived demand for data (labelled *VMP(d)*), which is the marginal value of additional data collected.[71] As noted above, data can provide direct value to a firm through use in targeted advertising or increased quality of the product due to customization, or simply because it is a necessary input to facilitate a product market transaction.[72] The Figure also illustrates the marginal social costs of data collection, storage and use. From a social perspective, these costs not only include the direct marginal costs of acquiring and maintaining the information (labeled $\omega'(d)$ in Figure 2), but also the expected breach costs per additional unit of data collected ($H(s^*) = \phi(s^*)^*h$).[73] Thus, from a social perspective, the allocatively efficient level of data collection is d^*, which is less than the data collected if firms focused only on their private costs (d').[74]

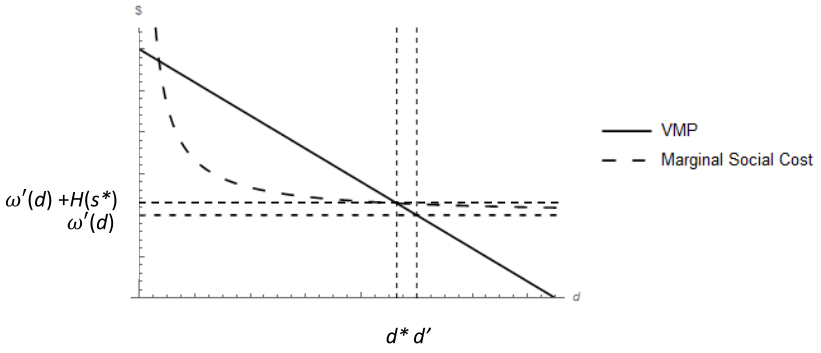
71. For a firm in a competitive output market, the derived demand for data will equal to the Value of the Marginal Product (VMP) of data. For single pricing firms facing a downward sloping supply curve in the output market, the derived demand for an input will equal the Marginal Revenue Product of the input. We use this scenario to derive results in the Appendix.

72. The amount of data collected will not be a function of firm output unless consumers always purchase a given quantity. For example, a consumer who purchases one gallon or thirty gallons of gasoline, or one item or a cart full of items at the grocery store, will provide the same information to the seller and the credit card network.

73. The standard model of optimal precautions treats accident avoidance costs as occurring per-unit of activity (e.g., mile driven) or output (e.g., cars off an assembly line). *See, e.g.*, SHAVELL, *supra* note 12, at 194–95, 195 n.29. We think in the data security context it makes more sense to treat security costs, $c(s^*)$, as fixed for a given scale. For example, once a firm chooses expenditures on encryption levels and employee training, they apply to all of the data processed. This assumption is equivalent to assuming that the marginal precaution cost per unit of data collected is zero and does not affect any of our conclusions.

74. With $s = s^*$, per data unit expected breach costs $H(s^*) = \phi(s^*)\, h(s^*)$ and the marginal social cost of data collection equals $\omega'(d) + \phi(s^*)\, h$. In the Appendix, we consider a more general model that allows the firm to engage in post-breach mitigation expenditures to reduce harm.

FIGURE 2
OPTIMAL DATA COLLECTION



The analysis above assumes that the harms generated by a data breach are specific to the firm. However, many security harms exhibit interdependence, and the interdependent versus independent nature of firms' security choices can have an impact on the incentives to take care.[75] Examples of such interdependencies include instances where there are multiple entry points that need to be secured. For example, in the IOT context, an insecure camera connected to a secure wireless router and other secure devices on the network can provide the weak link that compromises the security of the entire network. Similarly, one merchant can become the victim of a credential stuffing attack when lax security at another site leads to the breach of login credentials. A third example is a setting where multiple sites hold the same data, so that a breach of one site is equivalent to a breach of multiple sites.[76]

Under these conditions, we show (in the Appendix) that interdependence reduces the optimal security level to $s^{**} < s^{*}$.[77] The possibility that the common harm is caused by a breach at some other site acts as a "contagion tax" that reduces the incremental value of marginal expenditures aimed at a protecting any individual site.[78] In general, a data security breach likely includes both data held in common with other firms, as well as data held only by the breached firm. This implies that the socially optimal amount of data security is likely to lie somewhere between s^{**} and s^{*}.

75. *See* Howard Kunreuther & Geoffrey Heal, *Interdependent Security*, 26 J. RISK & UNCERTAINTY 231 (2003).

76. An example of largely overlapping data would be the credit reporting data held by the three credit reporting agencies.

77. *See* Appendix, equation (12) and subsequent text.

78. *Id.*

IV. CAN THE MARKET SOLVE THE PROBLEM?

In this Part, we examine whether market forces are likely to create incentives for data holders to mimic the socially efficient level of care. We find that the informational assumptions required for the market to lead to optimal care and activity levels are not likely to materialize because consumers often have difficulties tracing causation and verifying firms' data security claims. This conclusion leads to our discussion in Part V of negligence-based and strict liability rules.

In a world without liability for data breaches, the firm faces no *legal* compulsion to internalize the harm its data security practices caused. This, however, does not imply that firms face no consequences resulting from breaches or that they will choose to have lax data security. In particular, if consumers appreciate the potential harm associated with a firm's practices and force firms fully internalize the cost of these harms, firms will have optimal incentives to take care even if there is no legal compulsion to do so.

To see why, consider a setting in which consumers costlessly can determine a firm's level of security and the expected harm associated with that level of security (i.e., consumers know the value of $H(s)$). Assume further, for simplicity, that the firm exists in a competitive industry (so that prices are always equal to marginal cost in equilibrium) and that the only marginal costs are those associated with data security and expected data breach harms. Suppose a firm adopts a less than optimal level of data security $s^o < s^*$. With full information, consumers will recognize that when they share their personal data with this firm, they will suffer the per unit expected harm associated with less than optimal care $H(s^o) > H(s^*)$. *Ceteris paribus*, consumers will perceive a higher *real* price equal to the nominal price P plus the higher security costs $H(s^o)$. In contrast, a firm with the same nominal price P that adopts an optimal security level will have a lower real price $P + H(s^*) < P + H(s^0)$.[79] Put another way, the extra security expenditures (from s^o to s^*) make the firm better off, as the marginal benefits to the firm from lower expected consumer harm (in terms of increased demand for its product) exceed the marginal costs of these additional security expenditures.[80] In this manner, perfect information among consumers can force firms to internalize fully expected breach costs, leading to the optimal security and data collection levels illustrated in Figures 1 and 2.

---

79. This is equivalent to consumers reducing the value placed on the firm's product by $H(s^o) - H(s^*)$. Equivalently, if firms pay a price equal to expected harm to consumers for data, taking less than optimal security will result in higher data acquisition costs $(H(s^*)) < (H(s^o))$, again making the firm uncompetitive.

80. Notice that optimal security decisions also lead to optimal levels of output. Any other value of s other than s^* will lead to lower profits because either revenue will be too low ($s^o < s^* \rightarrow (H(s^o)) < (H(s^*)$, causing the effective price to be above profit maximizing levels), or per unit costs will be too high ($s^o > s^* \rightarrow c(s^o) > c(s^*)$). This follows directly from the definition of d^* and s^*.

Note that this logic holds even if the profit-maximizing nominal price for the firm's product is zero (e.g., a search engine or a social media platform). In this scenario, just as in the positive-price market discussed above, where consumers have perfect information, the *effective price* to consumers is the potential harm consumers may incur from sharing data, $H(s)$. A platform could skimp on security by choosing a level less than s^*, but it will no longer be maximizing profits: just as in the case with a fully transparent nominal price discussed above, the loss in revenue associated with the effective price increase from the cost-minimizing competitive level ($H(s^*)$) to ($H(s^o)$) will be greater than the security cost savings associated with moving from $c(s^*)$ to $c(s^o)$.[81]

There are, however, reasons to believe that consumers may lack sufficient information to hold firms accountable for their lax data security practices in the marketplace. For example, a consumer providing their credit card information to an online vendor is unlikely to know much about the company's data security practices, or if they did, how these practices impact the likelihood of suffering some type of identity theft.[82] What's more, in a world awash with personal data, when a consumer suffers a fraudulent charge on their credit card, they will never know with certainty whether the thief obtained the account information from a recent high-profile breach or from something more mundane, such as a skimmer used at a local gas station.[83] Relatedly, in some cases, the consumer may not be a customer of the firm holding the data. For example, ad networks, credit reporting agencies, and data brokers all collect consumer data, but in many cases do not sell their services to consumers. Accordingly, their customers—businesses who use these data—will not alter their demand for data based on data security practices. In these contexts, price fails to mediate security and output choices like it would for firms that are consumer-facing.

Further, under current tort law principles, consumers may not be able to recover the full harms caused by a breach. For example, consumers may not be able to show standing to sue in federal court if harms have yet to materialize, and harmed consumers may find it difficult to prove specific causation

81. For example, suppose that low security costs $5 and leads to $10 in expected harm, while high security costs $7 and leads to $6 in expected harm. If the platform chose low security, it would result in a cost savings of $2, but a reduction in consumer demand of $4 compared to high security. Thus, the platform's profits per unit of data would be $2 lower for choosing low security. Joe Farrell makes a similar point with respect to firm's choice of privacy policies. *See* Joseph Farrell, *Can Privacy Be Just Another Good?*, 10 J. TELECOMMS. & HIGH TECH. L. 251, 253–56 (2012).

82. Firms also have weak incentives to reveal information about attributes that make their product more attractive than those offered by rival firms.

83. On the other hand, some non-financial harms (e.g., a breach involving health information) are likely to be traceable because the data are usually stored by one firm that has had an identifiable breach, and the harm occurs only when one becomes aware that the data are exposed.

in cases where their personal information was exposed in multiple breaches.[84] Another potential bar to recovery is the economic loss rule, which prevents consumers from suing for economic losses caused by the negligent performance of a contract.[85] Thus, a consumer who is the victim of a data breach would be left only with contractual remedies, which are very unlikely to cover consequential damages caused by unauthorized third-party access to data stored by the firm.[86] Finally, harmed consumers may find it difficult to prove specific causation in cases where their personal information was put at risk in multiple breaches.

When markets do not force firms to internalize the expected costs of data breaches fully, legal intervention has the potential to better align private and social incentives to provide security. As we demonstrate below, the alignment of private and social incentives for investments in security could be achieved by an ideal negligence system. In such a system, the optimal level of security for each firm is clearly defined and perfectly enforced and is coupled with deterring sanctions of sufficient size to force firms to comply with the legal standard. However, the current form of FTC intervention—a negligence standard with an ambiguously-defined standard of care and an inability to make firms pay for consumer harm in most circumstances—is far from ideal and is thus unlikely to align private and social incentives. As we show below, the level of security that results from the FTC's current approach is unclear: moderate levels of uncertainty over the level of security needed to satisfy Section 5 can lead to overinvestment, while high levels of uncertainty over the legal standard, coupled with decisions that tend to map out only a lower bound for data security practices, could lead to under investment. Moreover, even if the standard is relatively clear, heterogeneity across firms with respect to the costs and benefits of data security may lead to both over- and under-deterrence unless the standard is tailored to each firm's unique circumstances.[87] Further complicating matters is the fact that the FTC is limited to

84. *See* Daniel J. Solove & Danielle Keats Citron, *Risk & Anxiety: A Theory of Data Breach Harms*, 96 TEXAS L. REV. 737, 739–44 (2018).

85. *See* RESTATEMENT (THIRD) OF TORTS §3 (AM. L. INST. 2020).

86. *See* Catherine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DEPAUL L. REV. 339, 362–65 (2017).

87. *See, e.g.*, Steven Shavell, *Corrective Taxation Versus Liability as a Solution to the Problem of Harmful Externalities*, 54 J.L. & ECON. 249, 256 n.16 (2011). In situations where harm and precaution costs are not likely to vary across firms, and regulators may have superior incentives to collect information about risks, ex-ante regulation may be more efficient. *See* Steven Shavell, *Liability for Harm Versus Regulation of Safety*, 13 J. LEGAL STUD. 357, 360 (1984) ("In certain contexts information about risk will not be an obvious by-product of engaging in risky activities but rather will require effort to develop or special expertise to evaluate."); *see also* Brian Galle, *In Praise of Ex Ante Regulation*, 68 VAND. L. REV. 1715, 1731, 1756 (2015) (arguing that the deadweight loss due to over- and under-deterrence caused by ex-ante regulation can be ameliorated if agencies can create more discrete regulatory categories); Bruce H. Kobayashi & Joshua D. Wright, *Antitrust and Ex-Ante Sector Regulation*, *in* THE GLOBAL ANTITRUST INSTITUTE REPORT ON THE DIGITAL ECONOMY 865 (2020) (noting the use of both

equitable remedies, which as a practical matter means that non-compliance penalties will not track consumer harm. The upshot is a liability regime that is unlikely to provide anything even approximating optimal incentives.

V. REASONABLE SECURITY VERSUS STRICT LIABILITY

In this Part, we lay out the economic case for our central claim—that holding firms strictly liable for data breaches would represent an improvement over the FTC's current negligence-like regime. As shown above, in cases where firms do not internalize the full social cost of the harms from data breaches, there is a misalignment of the private and social incentives to provide data security. This misalignment provides a rationale for legal intervention to improve incentives for firms to make optimal security and output choices.

The analysis below considers two ex-post liability regimes.[88] The first is a negligence regime that imposes liability on breached firms with levels of security that are lower than a threshold level of security. This approach is similar to the FTC's current use of unfairness to challenge "unreasonable" data security practices (or deception to challenge broken promises to take "reasonable" security). For example, the FTC could set a standard for data security and levy penalties on companies for non-compliance that caused, or increased the risk of, harm. This approach would require the FTC to set the standard and assess the firm's level of care relative to a standard of care after it observes some triggering event that is likely to cause consumer harm. A second *ex-post* enforcement approach would have the FTC observe an event that causes consumer harm (e.g., a breach), assess the magnitude of the harm, and penalize the breached firm an amount equal to the harm. Akin to a strict liability rule, this approach requires firms to pay a fine equal to the consumer harm caused by a breach regardless of the level of care taken.

We show that the root of the problem with the current negligence-like regime administered by the FTC is informational: firms are in a better position than the FTC to weigh the marginal costs and benefits of taking additional data security precautions. A strict liability approach, in which the FTC penalizes firms an amount equal to actual or expected consumer harm associated with a breach, would harness firms' private information to make these tradeoffs. This standard would require the FTC either to identify actual harm

approaches under the antitrust laws). *But see* Ben-Shahar, *supra* note 13, at 133–38 (analyzing the problems with the use of ex-ante regulation in the context of data security).

88. In theory, a negligence regime could operate through either ex-ante regulation where the trigger is the discovery of a level of security that falls below the standard irrespective of whether harm has occurred, rather than an ex-post enforcement regime where the firm is liable only when there is triggering event that causes, or is likely to cause, consumer injury. For reasons discussed above, this Article focuses on ex-post enforcement with a triggering event being an observed breach.

traceable to defendant's breach, or to estimate the ex-ante expected harm from the breach. Importantly, the informational requirements for estimating the expected harm from an actual event are likely far lower than those needed to estimate actual and optimal care for idiosyncratic firms. Further, we show that firms' data security decisions are less sensitive to errors in estimating damages than errors in estimating standards of care. Another benefit of a strict liability approach is that by forcing firms to internalize harm associated with data security practices, it will lead to optimal activity levels as well because expected consumer harm will be built into the price of their good or service.[89] Thus, forcing firms to internalize the harm they cause—rather than forcing them to comply with an estimated standard—is likely to lead to outcomes that align more closely with the social ideal.

A. *Ideal Negligence*

In an ideal negligence regime, the threshold level of security for liability is s^*, as derived in Part III.[90] A negligence regime leads firms to comply with the liability standard by creating a discontinuity in expected liability payments at the standard of care needed to be found non-negligent, here assumed to be s^*. Figure 3 illustrates the incentives of the firm when the fine imposed on negligent firms equals harm. The firm is liable for expected harm $H(s)$ and incurs security costs ($c(s)$) at security levels $s < s^*$. Once the firm reaches s^*, however, it is no longer liable for the harm it causes, and pays only its cost of security ($c(s)$). Clearly, the optimal strategy for the firm is to avoid liability by setting its security expenditures level $s = s^*$, resulting in total costs equal to $c(s^*)$.

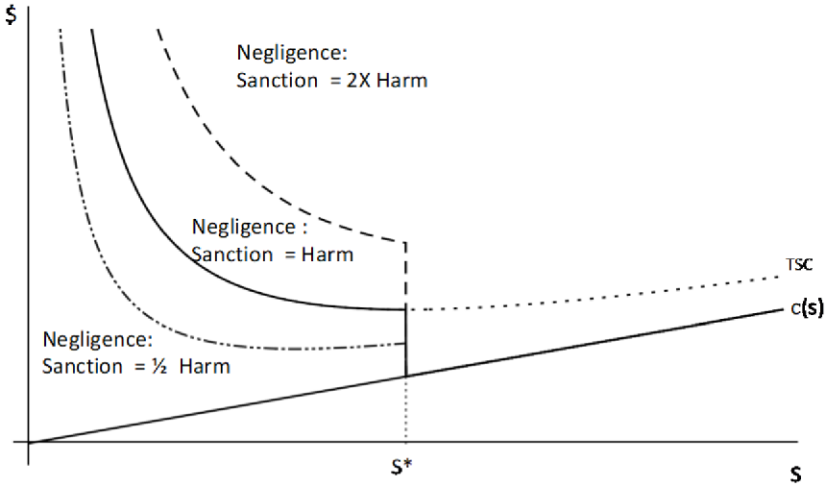
89. In the context of free advertising-supported services, firms could adjust quantity levels by, for example, collecting less data, or less sensitive data.

90. In *United States v. Carroll Towing Co.*, 159 F.2d 169 (2d. Cir. 1947), Judge Hand suggests the following formulation for liability in the context of damages caused by a barge breaking away from its moorings:

> [T]he owner's duty, as in other similar situations, to provide against resulting injuries is a function of three variables: (1) The probability that she will break away; (2) the gravity of the resulting injury, if she does; (3) the burden of adequate precautions. Possibly it serves to bring this notion into relief to state it in algebraic terms: if the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether B less than PL.

Id. at 173. Economists use a modified marginal version of the Hand Formula where there is negligence if the marginal burden of an untaken precaution is less than the reduction in expected loss, or $\Delta B < \Delta pL$. *See, e.g.*, WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW 85–87 (1987). In terms of the model presented in the Appendix, $\Delta B = c'(s)$, $\Delta p = \phi'(s)$ and $L = d\,[h(m) + e(m)]$. *See also* Mark F. Grady, *Untaken Precautions*, 18 J. LEGAL STUD. 139 (1989) (discussing the economic interpretation of the Hand Formula).

FIGURE 3
NEGLIGENCE STANDARD WITH FULL INFORMATION



A major advantage of an ideal negligence system is that the incentives generated are not sensitive to the magnitude of the remedy imposed on firms that fail to have reasonable security. To the contrary, there is a wide range of penalties that will provide firms with incentives to invest optimally in security as long as the liability standard is correctly specified.[91] For example, as shown in Figure 3, sanctions equal to twice and half harm incentivize the firm to take optimal care because they preserve the discontinuity at s^*.[92] Thus, an agency implementing an ideal negligence regime does not have to expend resources estimating harm accurately because the goal is not to set a price equal to external harm, but rather to deter non-compliance with the optimal standard with sanctions of sufficient size.

It is important to note, however, that even ideal negligence regimes fail to produce the correct incentives for firms to acquire and use data.[93] If a firm makes optimal security investments, it will not have to pay for the harm that results at s^* ($H(s^*)$). Thus, the firm's cost of acquiring and using data will not include the expected harm from data breach. If consumers do not appreciate this residual harm, the ideal negligence system will not correct for this type of misperception, and as explained in Part III, firms will have incentives to collect and use socially excessive amounts of data.

91. *See* Robert Cooter, *Prices and Sanctions*, 84 COLUM. L. REV. 1523, 1529 (1984).

92. At some point, however, if expected penalties fall too much it becomes rational for the firm to choose the level of security that minimizes security costs plus the expected fine. *Id.* at 1530–31; *see also* Louis Kaplow, *The Value of Accuracy in Adjudication: An Economic Analysis*, 23 J. LEGAL STUD. 307 (1994).

93. *See* Steven Shavell, *Strict Liability Versus Negligence*, 9 J. LEGAL STUD. 1 (1980).

B. Negligence with Costly Information

Until now, we have assumed that a regulatory agency is able to costlessly set the standard of care at s^* and costlessly assess firms' levels of care. Because implementing an ideal negligence approach requires the accurate estimation of both s^* and the level of care taken by the defendant, s_i, informational limitations are likely to cause regulators to be imprecise in their assessment of liability. For example, firms vary greatly with respect to the factors that affect the optimal level of data security. A large hospital that collects reams of highly sensitive consumer data is likely to have both lower costs to implementing security and higher levels of potential harms. By contrast, a minor website that collects relatively small amounts of mostly login information poses a much lower level of harm and likely would have a more difficult time than a large content provider implementing state of the art security. Because optimal security investments differ greatly between these firms, the legally required level of compliance (s^*) should vary as well.[94]

However, making such fine distinctions between firms requires a great deal of information and analysis. Further complicating matters is that data security is not one-dimensional: firms can employ various means to protect data that are both complements and substitutes. For example, in the payment card context, fraud detection algorithms and network authentication are substitutes for point-of-sale authentication methods, such as signatures and PINs.[95] The practical complexity of determining the optimal level of security and the actual level of security a firm takes means that an agency's assessment of liability is likely to be error-prone.

Errors that are biased in one direction—systematically setting the standard too high or too low—will cause firms to invest either too much or too little security, respectively. In addition to clear, yet erroneous standards, informational problems can lead to stochastic enforcement decisions. That is, because the enforcement standard is a probability distribution rather than a fixed point, investing in security below s^* will not always result in liability, and investing in security at or above s^* can sometimes result in liability. When liability is stochastic, firms take security measures based on *expected* liability.[96] Importantly, even if the agency is unbiased—that is, correct on average—in its assessment of the actual levels of security firms adopt and optimal levels of security (s_i, and s^*, respectively), firms will still lack

94. *Id.* at 22–23.

95. *See* James C. Cooper & Todd J. Zywicki, *A Chip Off the Old Block or a New Direction for Payment Card Security? The Law and Economics of the U.S. Transition to EMV*, 2018 MICH. ST. L. REV. 869, 906 (2018).

96. More formally, when considering security expenditures, the firm will now minimize $C(s_i) + [1\text{-}F(s_i)]H(s_i)$ where $F(s_i)$ is the likelihood of escaping liability when investing in security level s_i. With errors in assessing compliance with the standard, a wide range of security levels (depending on the variance of $F(s_i)$) carry some positive probability of liability, with $F(s)$ close to 0 for low security levels and $F(s)$ close to 1 for high security levels.

incentives to take optimal care. This result occurs because even though the errors are symmetric, the impact of these errors on expected liability costs are not.[97]

Figures 4A and 4B illustrate this result. Note that with stochastic liability, the discontinuity at s^* generated by an ideal negligence regime disappears and is replaced by a line connecting the tails of the distribution of the agency's estimate of s^*. This is due to the fact that now there is no single level of security that will always absolve the firm of liability for harm from data breaches. In Figure 4A, firms minimizing the sum of expected accident and avoidance costs in the face of uncertainty now choose $s^U > s^*$. This overdeterrence result will hold as long as the variance in the regulator's assessment of liability is not too large, or precaution costs do not rise too quickly.[98] If the variance is large, or when costs rise quickly, firms rationally underinvest in security, as the benefits in terms of reducing the likelihood of erroneous liability are too small in relation to the cost savings from reducing security investments. This underdeterrence result is shown in Figure 4B, where the variance is doubled.

97. Consider two situations. First, suppose a firm takes $s_i \geq s^*$, but the authority nonetheless finds it to be non-compliant. Here, the cost of the error to the firm is the penalty for non-compliance, which is assumed to be the harm caused at s_i ($H(s_i)$). Alternatively, suppose a firm takes $s_i < s^*$, but the authority erroneously finds it to have met the reasonableness standard. In this instance, the benefit from the error is the only cost difference between s_i and s^* ($c(s_i)$-$c(s^*)$), which will be less than consumer harm at s_i. Thus, because from a firm's perspective, the costs of being erroneously found liable is greater than the benefits of erroneously escaping liability, firms rationally will over-invest in data security. This result will hold as long as security costs do not rise too quickly, or enforcement errors are not too large.

98. *See generally* Richard Craswell & John E. Calfee, *Deterrence and Uncertain Legal Standards*, 2 J.L. ECON & ORG. 279 (1986) (deriving bounds for increased variance being associated with over- or under-deterrence).

FIGURE 4A
NEGLIGENCE AND UNCERTAINTY (OVERDETERRENCE)

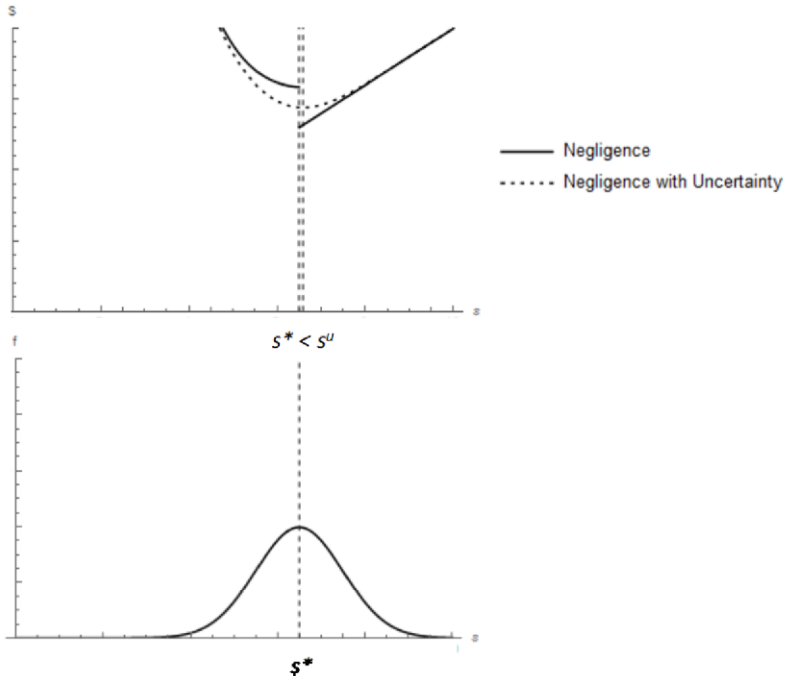


FIGURE 4B
NEGLIGENCE + TREBLE DAMAGES AND MORE UNCERTAINTY
(UNDERDETERRENCE)

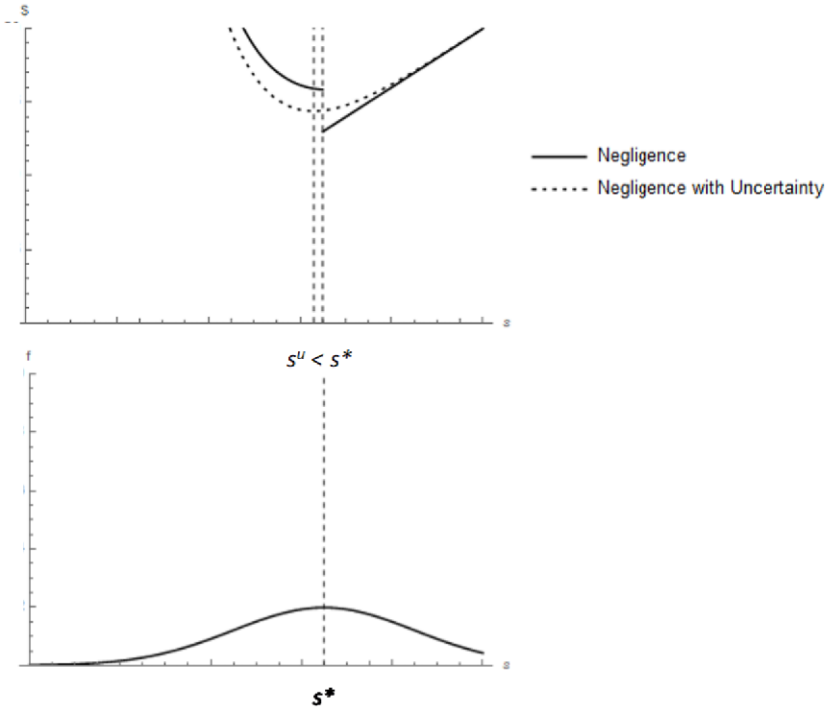
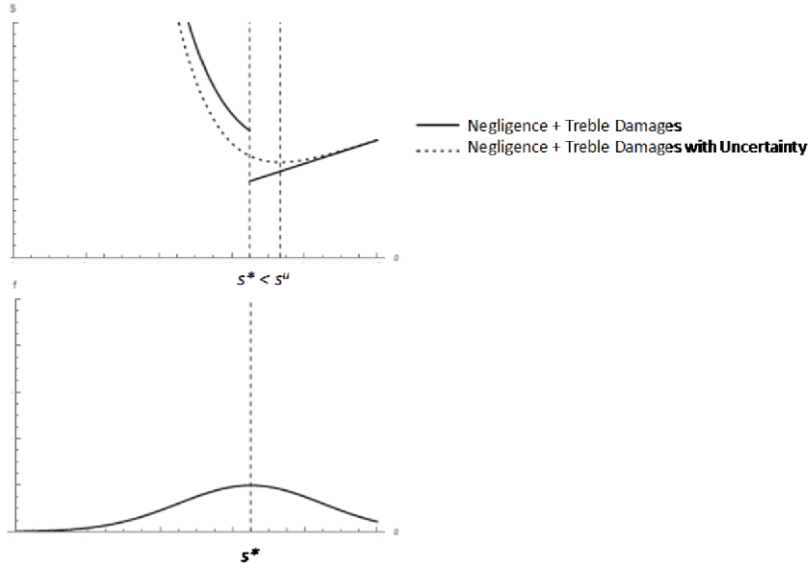


Figure 4C shows the effect of sanctions or remedies that exceed harm coupled with uncertain (yet unbiased) liability standards. While harm-based penalties under-deter in this setting, treble damages will induce the firm to spend more than s^*. Thus, the presence of uncertain legal standards or enforcement eliminates one of the primary benefits of the ideal negligence system: the lack of sensitivity of incentive to the magnitude of the remedy.[99] This is due to the fact that there is no longer a sharp discontinuity in private costs at the optimal level of care, s^*; private costs are now a continuous function of care because higher care reduces the likelihood of being held liable over the entire distribution of possible levels of care that a regulatory body may find to be optimal.

99. If the agency is biased in the sense that liability is still stochastic, but the distribution of liability standards is not centered around s^*, a firm's incentives will further depart from social incentives. For example, if the agency systematically finds firms investing in $s^L < s^*$ security in compliance with the standard, firms' will shift their expectations to center around s^L, rather than s^*, which, *ceteris paribus*, will decrease their incentives to invest in security. The opposite conclusion would hold if the agency were biased in favor of finding liability.

FIGURE 4C
NEGLIGENCE + TREBLE DAMAGES AND MORE UNCERTAINTY
(OVERDETERRENCE)



Unless the agency always accurately assesses both the optimal and the actual levels of security for a given firm, firms will face a stochastic liability standard. The results summarized in Table 1 show that this theory does not provide a crisp prediction of whether a firm faced with stochastic liability will over- or under-invest in security; it depends on the accuracy of the agency's liability decisions on average, as well as the variance of those decisions and the marginal costs of precaution. Moreover, the magnitude of the sanction or remedy imposed conditional on a breach occurring will alter the firm's incentives to invest in security. Thus, a non-ideal negligence-type system requires the enforcement agency to invest in the accuracy of both its liability determination and the size of its sanction.

TABLE 1
FIRM SECURITY INCENTIVES WITH STOCHASTIC LIABILITY

		Variance & Marginal Security Costs	
		Low	High
Average Agency Estimate Of Liability Standard	s^*	Over-deterrence	Under-deterrence
	s^L	?	Under-deterrence
	s^H	Over-deterrence	?

C. *Strict Liability*

In this Section we lay out the advantages of strict liability to an imperfect negligence regime that is likely to arise when information is costly. First, we show that like ideal negligence, ideal strict liability leads to optimal security levels, but unlike negligence, it also incentivizes optimal levels of data collection. We then show that in the face of costly information, the incentives produced by strict liability are more robust to errors in enforcement than those produced by negligence because regulators only need to estimate damages.

1. Ideal Strict Liability

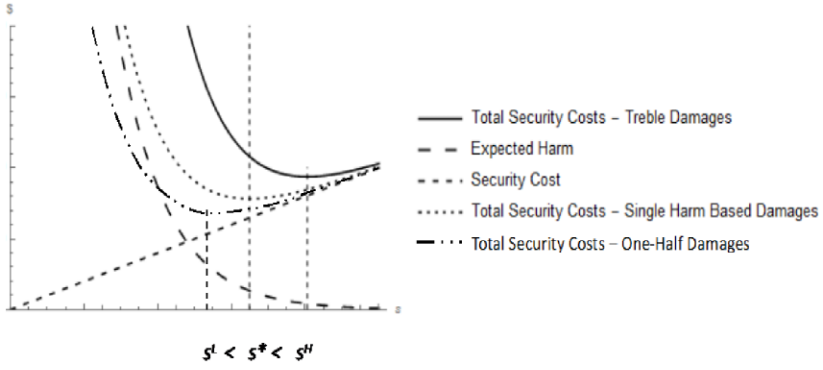
Unlike a negligence rule, a strict liability rule does not dictate a level of security. Instead, it works by requiring a firm to pay for all the external harm it causes regardless of the level of care taken. If a firm is forced to internalize the harm, the firm's profit maximization problem becomes identical to the one that faces the social planner depicted in Figure 1 in Part III. Through this mechanism, the firm will have incentives to take socially optimal security precautions, s^*, which will lead to socially optimal data collection decisions, d^*. This result contrasts with ideal negligence discussed in above in Part V.A. because the firm is forced to internalize the harm that occurs even when optimal security measures are taken.

2. Strict Liability with Costly Information

For the same reasons that the determination of the negligence standard can be subject to error, regulators also may estimate harm with error. When penalties are stochastic, firms will base their actions on the expected

penalty.[100] An important difference between negligence and strict liability standards is the effect of unbiased error. As discussed above, in the case of negligence, unbiased errors in determining compliance with the legal standard s^* distort a firm's incentives. An important advantage to strict liability is that even if the agency estimates harm with error, as long as it is correct on average, firms will still have incentives to invest optimally in security. This is because firms base their security investments on ex-ante expected damage payments, which will yield optimal incentives when expected damage payments are equal to harm.[101] This result is the dotted line in Figure 5, which traces the total social cost curve with accurate damages.

FIGURE 5
STRICT LIABILITY



As in the case of negligence, however, if an agency systematically over- or under- estimates injury, a firm will invest in too much or too little security compared to the social optimum, respectively.[102] The case where an expected fine equal to three times harm is shown in Figure 5. The dashed line is a firm's expected costs if expected penalties are equal to harm. When firms expect penalties to be three times actual harm, their expected harm plus security costs

100. The expected magnitude of the fine conditional on a breach is $E(Fine) = d * \int f g(f) df$, where d is the number of records, f is the estimate of the harm based fine, $g(f)$ is the distribution of estimates, and df is the differential term.

101. As noted above, with stochastic damages, firms minimize expected total security and breach costs. If the ex-post estimate of $E(Fine)$ equals is unbiased, then the harm per record can be written as $[h(m)] + \varepsilon$, where ε is a random error term with mean 0 and variance σ^2. Under these conditions, the expected fine will equal: $E(Fine) = d * [h(m) + \int \varepsilon f(\varepsilon) d\varepsilon]$. The last term is the mean of the error term ε, which is zero by definition. Thus, the magnitude of the expected fine equals $d * [h(m)]$, leading firms to choose $s^*$and d^*. *See generally* Kaplow, *supra* note 92; Louis Kaplow & Steven Shavell, *Accuracy in the Assessment of Damages*, 39 J.L. & ECON. 191 (1996).

102. This is because the distribution of the agency estimates (g(*f*)) will not be centered on actual harm per record $[h(m) + e(m)]$, but instead around over- or under-estimates of actual harm.

rise to the solid line, and they over invest in security $s^H > s^*$. Conversely, Figure 5 shows expected firm costs when penalties are half actual harm, which leads them to under invest in security $s^L < s^*$.

There is an important difference between systematic errors with regard to the level of care in a negligence regime and in damages in a strict liability regime. As shown above, because the negligence rule sets up a discontinuity around the standard of care required by the authority, there are strong incentives to calibrate actual care to what the regulatory authority requires. Take the extreme example of a biased standard of care with no error: $\tilde{S}$ which is twice as much as s^*. As seen in the previous Section, as long as $\tilde{S}$ is not too large and costs do not rise too quickly, it is optimal for a firm to always take $\tilde{S}$ because it will reduce expected damage payments to zero. That is, in the relevant range, overinvestment in security moves one-to-one with the erroneous liability standard. On the other hand, if damages are overestimated by 100% with certainty, a rational firm will not increase its level of care by 100%.[103] This is because privately optimal care under strict liability is continuous; although an increase in expected damages above actual harm results in incentives to take additional care above s^*, this decision is tempered by the fact that extra care is costly and only marginally reduces expected damages.

D. *The Advantage of Strict Liability*

The analysis above demonstrates some of the advantages of a regulatory structure based on strict liability over one based on negligence. First, the agency does not have to specify optimal levels of precaution or activity level.[104] The agency would not have to estimate optimal or actual levels of security investments, which are likely to be idiosyncratic and multidimensional.[105] Instead, for strict liability to function, the agency must estimate only expected consumer harm resulting from a breach, which is likely to be less prone to the type of errors that distort firms' incentives. Firms, in turn, would be allowed to decide for themselves how much to spend on data security and mitigation, and to decide how much data to collect, use, and retain based on their expectations of the harm that their data collecting activities are likely to cause. Importantly, these decisions will be based on firms' private knowledge of the costs of prevention and the benefits of increasing their level of spending on data security. If the firms' private knowledge is superior to the knowledge

103. For example, in the model in the Appendix that supports all of the results presented in the Article, $\frac{\partial s^*}{\partial H} = \frac{1}{\lambda H} < 1$.

104. Mark A. Geistfield, *Protecting Confidential Information Entrusted to Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability*, 66 DEPAUL L. REV. 385 (2017); Citron, *supra* note 35; Shavell, *supra* note 93.

105. *See generally* Mark F. Grady, *Multiple Tortfeasors and the Economy of Prevention*, 19 J. LEGAL STUD. 653 (1990); Mark F. Grady, *Res Ipsa Loquitur and Compliance Error*, 142 U. PA. L. REV. 887 (1994).

of the agency—which is almost certainly the case—the choices are likely to better reflect the costs and benefits of such activity as long the remedies force firms to fully internalize the costs generated by a breach.

Second, strict liability is more robust than negligence to the type of enforcement errors that are likely to accompany any standard in employed in the real world. As long as the agency's harm estimates are correct on average, firm and social incentives to invest in security are more likely to be aligned than under a stochastic negligence rule.[106] Further, biased estimates of harm have less impact on firm care and data collection incentives than do biased estimates of optimal care.

Third, because firms internalize all of the harm they cause, a strict liability rule is likely to provide both consumers and firms with the improved incentives with respect to data sharing. Under a negligence-based approach to data security, consumers bear the residual risk of data breaches that occur even when firms take optimal care. Under a strict liability approach, firms bear this risk. If firms have superior information about this residual risk relative to consumers, and this risk is passed along to consumers in the form of higher prices or fewer requests for data, levels of data sharing will be more efficient.

Fourth, there are also benefits that would accrue directly to the FTC. Strict liability will reduce the level of per-case resources. For example, staff would no longer need to investigate a defendant's data security methods or work with internal or external experts to assess the reasonableness of these methods. Because each case only would require estimating harm, the FTC staff could increase the number of data security cases it handles with the same level of resources. A strict liability approach will also have the collateral benefit of allowing the FTC to avoid the difficulties in complying with the Eleventh Circuit's *LabMD* decision.[107] In *LabMD*, the FTC had alleged that a medical testing firm failed to take reasonable security measures when an employee had exposed a file containing sensitive medical information to a peer-to-peer network.[108] Because the FTC presented no evidence of actual harm, and because the data in question had not been seen by anyone other than FTC staff and the forensics firm that discovered the data, the ALJ found that FTC had not satisfied the "likelihood of substantial consumer injury" element of unfairness.[109] The FTC reversed the ALJ's ruling, finding that the increased risk of harm from exposure of the data to the peer-to-peer network presented a sufficiently high likelihood of substantial injury.[110] The heart of the FTC's

106. The estimate of ex-ante expected damages should reflect factors known to the firm at the time it makes its decision to collect, use, and protect data. *See generally* Kaplow & Shavell, *supra* note 101.

107. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221 (11th Cir. 2018).

108. *Id.* at 1224–25.

109. Initial Decision, LabMD, Inc., *supra* note 48, at 88.

110. Opinion of the Commission, LabMD, Inc., *supra* note 48, at 25.

order required LabMD to develop a data security program "that is reasonably designed" to protect the personal information it collects and to design and implement "reasonable safeguards to control the risks" to the personal information it holds.[111] On appeal, the Eleventh Circuit sidestepped the injury issue, and instead held that the FTC's order was unenforceable due to vagueness because it "commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness."[112] In response, the FTC has been forced to mandate more specific requirements in its data security orders.[113] A strict liability regime would relieve the FTC of the burden of crafting and monitoring orders with bespoke and specific security requirements—which are taxing on staff resources—in order to comply with *LabMD*.

Finally, by vesting a single national enforcer with the authority to levy deterring payments to remedy harmful breaches, a strict liability approach will solve the tort system's inability to provide adequate deterrence. Although major (and minor) data breaches often spawn private class actions, these cases often run into roadblocks due to an inability to make sufficient showings of harm, either at the standing stage or as an element of cause of action.[114] When plaintiffs lack evidence that the breach in question actually led to harm (e.g., evidence of new or existing account fraud),[115] courts have generally rejected the plaintiffs' claims as too speculative, because an increased risk of harm without more fails to satisfy the requirement in federal court that injuries must be "'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'"[116] Substituting a strict liability regime administered by the FTC for private tort actions would have two clear benefits. First, because the FTC does not have to satisfy standing requirements, it can force firms to internalize the expected harm they cause, even if it is unrealized. Second, a

111. Final Order, LabMD, Inc., *supra* note 55, at 2.

112. *LabMD, Inc.*, 894 F.3d at 1236.

113. More specific requirements in its data security orders can be seen in the FTC's case against LightYear Dealer Technologies, LLC (also known as DealerBuilt). As Chairman Simons noted in announcing this case: "The settlement with DealerBuilt imposes more specific security requirements and requires company executives to take more responsibility for order compliance, while also strengthening the third party assessor's accountability and providing the FTC with additional tools for oversight." *Auto Dealer Software Provider Settles FTC Data Security Allegations*, FED. TRADE COMM'N (June 12, 2019), https://www.ftc.gov/news-events/press-releases/2019/06/auto-dealer-software-provider-settles-ftc-data-security.

114. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harm*, 96 TEX. L. REV. 737, 748–54 (2018).

115. Some courts have found harm sufficient for standing purposes when there is evidence that the data are in the hands of hackers who have malicious intent and there is some evidence of extant fraud. *See* Remijas v. Neiman Marcus Grp., 794 F.3d 688, 689–90 (7th Cir. 2015) (evidence of some fraudulent charges for some customers); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (evidence of fraudulent attempt to open a bank account with data from breach).

116. Spokeo, Inc. v. Robins, 578 U.S. 330 (2016) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)); *see* Solove & Citron, *supra* note 114, at 748–54 (collecting cases).

court-administered negligence regime for those private cases with sufficiently concrete harm for standing is likely to suffer from the same informational problems as the FTC's current approach. Thus, moving toward an FTC-administered strict liability regime would generate more efficient incentives for firms.

E. *Strict Liability as a Facilitator for Cyber Insurance*

An important collateral benefit of moving from a regulatory regime based on negligence to one based on strict liability is that a strict liability regime improves the ability for cyber insurers to function as *de facto* regulators. It has long been recognized that liability insurers provide valuable services beyond indemnification.[117] Insurance companies, through risk management programs, provide standard setting and safety monitoring roles designed to manage and reduce the risk to those they insure. Although this proposition may at first blush seem counterintuitive—after all, insurance companies are in the business of providing protection against risk—the ability to coax their insured to take cost effective steps to reduce risk will allow an insurance company to charge lower premiums and hence to be more competitive. For example, Shavell shows that if an insurer can observe and contract on an insured's level of care, liability insurance will lead to first-best outcomes because the insurer will translate efficient risk-reducing actions into premium reductions that are larger than the marginal cost of precaution.[118] Insurance companies have several tools at their disposal to create incentives for their clients to take efficient risk-reducing measures, including refusing to insure, underwriting based on risk through "feature ratings" or "experience ratings," and providing their own best practices concerning risk reduction or loss mitigation that come from industry-wide knowledge and internal research.[119] In this manner, liability insurance that links premiums to care can ameliorate moral hazard, even with full insurance.

What is more, if the insurance company has better information than the firm about the link between care and harm, liability insurance can improve outcomes—and there are reasons to believe that this may be the case in a wide variety of circumstances. For example, liability insurers will have access to information gleaned from experiences across an industry and thus can serve as "specialized outsiders," providing advice to firms on how to reduce the likelihood and severity of accidents.[120] Indeed, some have argued that the

117. *See, e.g.*, Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197 (2012); Tom Baker & Rick Swedloff, *Regulation by Liability Insurance: From Auto to Lawyers Professional Liability*, 60 UCLA L. REV. 1412 (2013).

118. Steven Shavell, *On Liability and Insurance*, 13 BELL J. ECON. 120 (1982).

119. *See* Ben-Shahar & Logue, *supra* note 117, at 206–18.

120. *See* Victor P. Goldberg, *The Devil Made Me Do It: The Corporate Purchase of Insurance*, 5 REV. L. & ECON. 541, 543 (2009); *see also* Haitao Yin, Howard Kunreuther &

risk-reducing ancillary services provided by insurance, rather than the risk bearing itself, is the primary explanation as to why risk neutral parties who can afford to self-insure might nonetheless purchase liability insurance.[121]

Cyber insurance is a relatively recent product, but is among the fastest growing lines of insurance, with estimated annual growth rates of 27% across all industries.[122] Further, there are now over 500 insurance carriers in the United States offering some form of cyber insurance, with average coverage between $10 million and $25 million.[123] A recent survey of cyber insurance policies finds that insurers are underwriting losses related to government penalties and private claims arising out of data breaches, which suggests that insurers are employing many of the risk-reducing tools used in general liability insurance policies to cyber insurance policies.[124] They find, for instance, that insurers collected information through detailed questionnaires designed to assess a firm's risk profile.[125] Information collected included the sensitivity and volume of data a firm handles, a firm's compliance with government and industry data security standards, and a firm's data breach history.[126]

Although the methods of pricing risk vary and are based on limited information about the relationship between certain practices and risks, most cyber insurers appear to set prices based on estimated risk profiles. For example, cyber insurers will look to a firm's history of data breach incidents or to its propensity to engage in a "high hazard" business, where lots of business is conducted online and involves sensitive consumer data, in deciding whether to charge a higher insurance premium.[127] A majority of sampled policies based premium adjustments on a firm's answers to a security questionnaire that inquired about the quality of a firm's "privacy controls," "network

---

Matthew W. White, *Risk-Based Pricing and Risk-Reducing Effort: Does the Private Insurance Market Reduce Environmental Accidents?*, 54 J.L. & ECON. 325 (2011) (providing evidence that the existence of private liability insurance for underground storage tanks reduced environmental damage).

121. Goldberg notes that the Hartford Boiler Insurance and Inspection Company began as only an inspection company, but evolved to provide insurances as a way to share the risk associated with a boiler accident after an inspection. Goldberg, *supra* note 120, at 543; *see also* Tom Baker, *Back to the Future of Cyber Insurance*, 3 PROF. LIAB. UNDERWRITING SOC'Y J. 1 (2019) (discussing multiple ways beyond risk transfer that cyber insurers manage uncertainty in selling cyber insurance); Ben-Shahar & Logue, *supra* note 117 (discussing the role of insurance companies in managing risk and the role of mandatory cyber insurance for firms that collect, store and use data).

122. Sasha Romanosky, Lillian Ablon, Andreas Kuehn & Therese Jones, *Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?*, 5 J. CYBERSECURITY 1, 2 (2019); *see also* Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, 43 LAW & SOC. INQUIRY 417 (2017).

123. Romanosky et al., *supra* note 122, at 2.

124. *Id.* at 6–7.

125. *Id.* at 8–12.

126. *Id.* at 9–11.

127. *Id.* at 14–15. High sales volumes or assets will also tend to lead to higher premiums.

security controls," "content liability controls," "laptop and mobile device security policy," and "incident response plan."[128] Importantly, these are all factors under a firm's control, which means that they have incentives to take private actions that reduce risk as long as the marginal precaution cost is less than the premium reduction. Although it is unclear the extent to which prices currently reflect actual risk, as insurers gain knowledge about the relationship between certain practices and the marginal reduction in risk, one would expect underwriting accuracy—and hence the ability to use premiums to create incentives for firms to take efficient precautions—to grow.[129] Some policies also use exclusions to temper moral hazard, for example, by covering claims arising out of "deceptive or unfair trade practices" involving "theft, loss, or unauthorized disclosure" of personal information, but excluding incidents in which the insured "colluded in the theft, loss, or unauthorized disclosure."[130]

In addition to using pricing and exclusions to affect a company's cyber security practices, cyber insurers also provide a variety of risk-management tools to their clients. As one study of cyber insurance practice explained, "insurance institutions are doing something more than transferring risks—they are actively managing the underlying risk of data breach."[131] For example, cyber insurers typically provide a security assessment of an insured's systems, audit written handbooks and training material for legal compliance, train employees on best practices, and assess the risks posed by third-party vendors.[132] Cyber insurers also provide a robust suite of post-breach tools that help clients respond, investigate, and mitigate the harm resulting from a breach, such as providing access to expert legal teams.[133] As one study concludes, "the insurance company, through the risk management services it offers with cyber insurance, largely drives the company's incident response when a data loss occurs."[134] It appears that some cyber insurance companies anticipate that their services will mitigate losses in the event of a breach. One policy, for example, developed premiums based in part on an FTC estimate of consumers' costs from identity theft and adjusted premiums downward by

128. *Id.* at 16 tbl.13. Romanosky et al., find some more sophisticated approaches, including rating a firm's overall security posture along six dimensions (data classification, security infrastructure, governance, risk and compliance, payment card controls, media controls, and computer systems interruption loss). *Id.* at 17.

129. *Id.* at 16.

130. *Id.* at 7. Excluding coverage of "inside jobs" is common in policies covering theft, and is a recognition that firms are in a better position than insurance companies to police their employees. *See, e.g.*, Atwater Creamery Co. v. W. Nat'l Mut. Ins. Co., 366 N.W.2d 271, 275–76 (Minn. 1985).

131. Talesh, *supra* note 122, at 428.

132. *Id.* at 429–31. The outcome of these risk assessments can impact insurance premiums. *See id.* at 429.

133. *Id.* at 432.

134. *Id.*

almost eighty percent due to the client's anticipated use of the recommended "case management restoration services."[135]

The role of liability insurance plays in shaping firm behavior depends on the underlying liability regime. For example, in a world where data handlers face no liability for breaches, first-party insurance would be the primary form of coverage: consumers would either self-insure or purchase some type of policy to protect them from identity theft. Firms facing no liability for data breaches would not choose to purchase cyber insurance. Although it may mitigate consumer moral hazard with respect to providing personal data to firms, first-party insurance would have no impact on data handlers' incentives to take care.

Alternatively, in either a negligence or a strict liability regime, claims would be handled by third-party liability insurance policies owned by data handlers. Although both negligence and strict liability will facilitate the ability of liability insurers to regulate data security precautions via contract, there are reasons to believe that strict liability will lead to superior outcomes. To see this, it is important to note that the underlying liability regime is what triggers an obligation for the insurance company to pay. This is the mechanism that allows insurance to translate the incentives created by a liability regime into prices that impact care decisions.[136] Accordingly, it follows that regulation by contract between insurers and data handlers will mimic whatever errors are present in the underlying liability-determining process.

Under the current FTC framework, liability is triggered when the FTC determines that data security measures are unreasonable, so liability insurers use the tools at their disposal to move insureds to comply with the FTC standard. As discussed in Part IV, if levels of care are measured with error, or if the standard of reasonable care is stochastic—even if optimal on average—then the privately optimal level of care is unlikely to be optimal. Thus, the privately optimal contract between a liability insurer and its data handler client will be calibrated to this suboptimal standard of care, rather than optimal care. On the other hand, under the strict liability regime described in Part III, liability is triggered whenever the firm has a breach that impacts consumers, rather than when it fails to meet an imprecise standard articulated by the FTC. As long as damages are measured accurately on average, the contracts between liability insurers and data handlers will be calibrated to optimal care.

Further, the advantages from strict liability that flow from harnessing a firm's private information about the marginal costs and benefits from taking precautions are likely to be amplified when coupled with liability insurance. As discussed above, one of the primary values of liability insurance derives from an insurer's broad knowledge of industry best practices. In some contexts, unreasonableness determinations by the FTC may be useful in

135. Romanosky et al., *supra* note 122, at 12 n.36.
136. *See* Ben-Shahar & Logue, *supra* note 117, at 234.

providing information to data handlers on where due care standards lie.[137] However, even assuming that FTC liability determinations are accurate representations of optimal care, cyber insurers are likely to be able to duplicate this information propagation function via private contract at a lower cost and with accuracy tailored to each firm. [138]

VI. WHAT IS TO BE DONE?

In this Part, we lay out some of the details that would be involved in setting up a strict liability regime administered by the FTC. First, we discuss how harm would be calculated, and then, we identify necessary legislative changes to the FTC Act. Finally, we address potential concerns that may result in political opposition to our approach.

A. *Calculating Penalties*

A strict liability standard would require the FTC to levy a monetary penalty on firms when their breaches harm consumers. The goal of the monetary relief imposed by the FTC should be to ensure that firms fully internalize the external harms that their data security practice impose on third parties. Ideally, a strict liability approach would be based on actual harm. In the data security context, however, harm is difficult to measure given the problems associated with tracing an instance of an identity fraud to a specific breach. This is especially true given the non-trivial baseline level of identity fraud risk that exists due to the overall prevalence of data breach. Thus, strict liability should be triggered by a data breach that increases the risk of identity fraud. Accordingly, a necessary predicate for a functioning strict liability standard using harm-based penalties is some form of a breach notification requirement that would reliably alert the FTC of breaches in a timely manner. Failure to comply with such a requirement could be deterred either by increasing sanctions to reflect the additional harm caused by noncompliance, or by adding a multiplier to reflect attempts to evade liability.[139]

---

137. *See* Marie-Cécile Fagart & Claude Fluet, *Liability Insurance Under the Negligence Rule*, 40 RAND J. ECON. 486, 487 (2009) (describing the useful role of negligence determinations when insurers cannot contract ex-ante on care levels); *see also* Surajeet Chakravarty, David Kelsey & Joshua C. Teitelbaum, Tort Liability and Unawareness 3 (Apr. 1, 2019) (unpublished manuscript), https://ssrn.com/abstract=3179753 ("Under negligence, however, the litigation provides the world with more information. In particular, the court's stipulation of a new due care standard serves as a knowledge transmission mechanism, providing the world with information about the updated probability of harm.").

138. *See, e.g.*, Citron*, supra* note 35, at 266–67 (noting that as cyber insurance markets evolve, "database operators that continue collecting sensitive information will be better position to assess the cost of residual risk").

139. Sasha Romanosky, Rahul Telang & Alessandro Acquisti, *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGMT. 256 (2011).

Assuming the FTC can detect harmful breaches, penalties should be set equal to expected harm that includes the direct consumer losses from fraudulent charges or identity theft (to the extent traceable). Further, when there is no evidence of direct harm, the FTC can estimate increased risk of harm from breaches of Personally Identifiable Information (PII) using public and private data from the breached firm.[140] This estimate should be current, unbiased, and vary based on the type of data and the length of time since the breach. For example, recent data suggest that around 6.5% of the population suffered some form of identity theft in 2017, but of those consumers who received at least one breach notification, 18.5% suffered some form of identity fraud.[141] These data do not establish the marginal impact of breach on the incidence of identity fraud, but they do imply that on average, when a consumer's data are exposed to at least one reported breach in a year, their odds of identity fraud increase by a factor of 3.25.[142] This increase in risk could be married with an estimate of monetary losses when financial data is at stake. Where the price of sensitive PII has no readily available market price (e.g., sensitive health information), the FTC would need to conduct its own study, or rely on existing empirical estimates of willingness to pay for privacy protection to arrive at statutory damages. Further, penalties would reflect the mitigated level of harm as well as the ex-post costs that consumer incurs to mitigate harm.[143]

The FTC should limit actions to breaches that impact consumers, and any monetary relief imposed by the FTC should reflect remedies imposed by

140. PII are data that can be used to identify a person. Examples include a person's name, social security and driver's license numbers, physical and e-mail addresses, and birthdates. The FTC has a broad definition of PII, and "now regard[s] data as personally identifiable when it can be *reasonably linked* to a particular person, computer, or device." Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Keynote Address at the Technology Policy Institute Aspen Forum: Protecting Consumer Privacy in the Digital Age: Reaffirming the Role of Consumer Control 3–4 (Aug. 22, 2016), https://www.ftc.gov/system/files/documents/public_statements/980623/ramirez_-_protecting_consumer_privacy_in_digital_age_aspen_8-22-16.pdf.

141. *See* Al Pascual, Address at the Fed. Trade Comm'n's Competition and Consumer Protection in the 21st Century 41–45 (Dec. 11, 2018), https://www.ftc.gov/system/files/documents/public_events/1418261/ftc_hearings_session_9_transcript_day_1_12-11-18.pdf.

142. Using the odds formulation of Bayes' Rule $\frac{P(I|B)}{P(NI|B)} = \frac{P(B|I)}{P(B|NI)} * \frac{P(I)}{P(NI)}$, where $P(I)$ is the probability of injury from a breach, $P(NI)$ is the probability of no injury from a breach, and $P(B)$ is the probability of breach. Substituting in values for $P(I)$, $P(NI)$, $P(I|B)$, and $P(NI|B)$ from AL PASCUAL, KYLE MARCHINI & SARAH MILLER, JAVELIN STRATEGY, 2018 IDENTITY FRAUD: FRAUD ENTERS A NEW ERA OF COMPLEXITY (2018), and solving for $\frac{P(B|I)}{P(B|NI)}$, results in 3.24. For further discussion of the correlation between exposure to a breach and odds of experiencing fraud, see Pascual, *supra* note 141.

143. Mitigation expenditures would include time and resources costs involved in minimizing the odds of identity fraud post breach, for example, by purchasing credit monitoring or credit freezes or ordering new credit or debit cards. It is irrelevant whether the firm reimburses consumers for this cost or pays for it directly (e.g., by purchasing credit monitoring services for all affected consumers). *See generally* Donald Wittman, *Optimal Pricing of Sequential Inputs: Last Clear Chance, Mitigation of Damages, and Related Doctrines in the Law*, 10 J. LEGAL STUD. 65 (1981).

others, including redress or mitigation expenditures already paid by the breached firm to consumers.[144] Further, the FTC should avoid taking action when a clear contractual relationship between consumers and the firm allocates risks from a data breach. Grafting an ex-post FTC remedy to existing contractual obligations could dampen incentives to allocate risk efficiently ex-ante and increase the cost of contracting.[145]

We also think that the FTC should limit actions to remedy harm caused by custodians of consumer data, and not reach the sale of products that consumers use to transmit data, such as routers, or other connected devices. In these cases, the problems of causation and information asymmetry, while not absent, are not as stark as in the case of data custodians. Accordingly, it is better to allow the market and the contract between the consumer and the firm to govern the level of data security promised, with the FTC's ability to police misrepresentations about security as a backstop.[146]

B. *Necessary Legislative Fixes*

A fully operationalized version of our strict liability approach would require Congress to provide the FTC with additional authority. As discussed in Part II, the FTC is currently unable to secure remedies that approximate consumer harm from a breach.[147] Because its current tools are not up to the task, the FTC must obtain additional legislative authority to levy damages on firms

144. This is because a firm should pay for steps consumers take to mitigate harm, and thus should get credit for these expenditures if taken prior to an FTC action. Our proposal envisions the FTC administered regime preempting state and private actions. However, if this were not the case, a breached firm should also receive credit for civil damages and penalties imposed by private litigants and other governmental actors. As noted above, under state law, tort liability for data security lapses may be limited or even precluded. *See* Sharkey, *supra* note 86, at 342. In theory, the FTC remedy should also take into account market imposed reputational losses imposed on breached firms. *See generally* Jonathan M Karpoff & John R. Lott, *The Reputational Penalty Firms Bear from Committing Criminal Fraud*, 36 J. L. & ECON. 757 (1993) (analyzing optimal criminal penalties in the presence of market imposed reputational penalties). *See also* Joshua Mitts and Eric Talley, *Informed Trading and Cybersecurity Breaches*, 9 HARV. BUS. L. REV 1 (2019) (documenting the negative abnormal stock price effects suffered by breached firms and firms with inadequate levels of cybersecurity).

145. To the extent that promises of certain levels of data security are deemed to create a contract, the proper remedy would be under the contract, not an FTC action. However, courts have almost uniformly rejected the notion that privacy policies constitute contracts between firms and consumers. *See, e.g.*, *In r*e Jet Blue Airways Corp. Priv. Litig., 379 F. Supp. 2d 299, 324–28 (E.D.N.Y. 2005); Dyer v. Northwest Airlines Corps., 334 F. Supp. 2d 1196, 1199–200 (D.N.D. 2004).

146. For example, the Northern District of California rejected a claim based on an insecure device that was likely to cause harm in *D-Link*. Fed. Trade Comm'n v. D-Link Sys. Inc., No. 17-cv-00039, 2017 WL 65168 at *5–6 (N.D. Cal. Jan. 5, 2017). Although the court dismissed the FTC's unfairness claim as too tenuous, it rejected plaintiff's motion to dismiss the FTC's claim that it's data security promises were deceptive under § 5. *Id.* at *2–3, *6.

147. The FTC also enforces a variety of rules, many of which allow for civil penalties. 15 U.S.C. § 45(m)(1)(A). The focus of this Article, however, is on the use of the FTC's UDAP authority under § 5.

that are tethered to consumer harms related to data breaches. The good news is that the time is ripe for reform, as Congress considers how to restore the FTC's remedial powers in the wake of *AMG*.

One path could be to provide the FTC with the specific authority to fine breaching firms an amount equal to an estimate of consumer harm, or to provide a general civil penalty authority, with a requirement that the penalty is based on consumer harm.[148] Further, any legislation should include rulemaking authority to allow the FTC to require breach notification, establish parameters for financial harms, and set statutory penalties for non-financial harms. Finally, any legislation should preempt state and common law causes of action to allow the FTC to become the sole data security enforcer. Not only would competing state and private actions sounding in negligence dilute the benefits of a national strict liability standard, but as discussed below, it would likely be a political concession necessary to help allay business concerns.

In addition to new authority, depending on the thresholds for breach reporting, the FTC would likely require additional resources to handle the volume of cases. For example, one estimate finds that in 2018 there were 1,079 data breaches involving non-governmental entities.[149] If even ten percent of these breaches were reportable to the FTC under a strict liability standard, this represents a marked increase in the number of data security cases that staff currently handles annually. But, because the resources per case would be dramatically reduced, an increased caseload would not require a proportional increase in resources.

C. *Possible Concerns*

Any strict liability regime is likely to engender political opposition from businesses, especially because there is probably no level of care that would insulate a firm from suffering a breach and thus from paying damages. However, there are reasons to believe that these concerns could be assuaged.

First, by eliminating the need to calibrate their actions to an uncertain FTC standard, strict liability would provide firms with increased regulatory certainty, which will reduce compliance costs. Further, cyber insurance will allow residual risk to be efficiently transferred and converted into a fixed cost.

Second, including a preemption provision would insulate firms from private and state suits, which is likely to result in lower levels of liability and litigation costs overall. The Fair Credit Reporting Act (FCRA), which sets

148. The FTC Act currently provides that civil penalties for knowing violations of order provisions and rules be based on "the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require." 15 U.S.C. § 45(m)(1)(C).

149. Of the 1,079 data breaches, 571 involved businesses, 363 involved the healthcare sector, and 135 involved the financial sector. Joseph Johnson, *Number of Data Breaches in the United States from 2013 to 2019, by Industry*, STATISTA (Mar. 9, 2021), https://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business.

out robust federal requirements and severely curtails private actions under FCRA and state law, could provide a model.[150] For example, enacting legislation could vest all federal enforcement authority with the FTC, preempt states from enforcing their own data security laws, and limit private negligence actions to those involving malice or willful intent to injure.[151] Even leaving the explicit preemption aside, a reform that eliminates the reasonableness inquiry would remove the ability of class action plaintiffs to use a negligence per se theory based on an alleged breach of the FTC's Section 5 standard.[152]

A third way to alleviate business concerns is to ensure that any legislation or rulemaking exclude certain breaches caused by highly sophisticated attacks, such as those by state actors. It could also set a *de minimis* threshold for payment based on the size and sensitivity of data breached. This would have a collateral benefit of creating incentives for some firms to forego the collection of large volumes of sensitive data.[153] What is more, initially, legislation could also limit the use of strict liability regimes to specific settings, e.g., to settings where market mechanisms for cost internalization are weak, or where current remedies are inadequate to align private and social incentives. For example, data brokers and credit reporting agencies have large stores of sensitive consumer information, but these entities are typically not consumer-facing, and thus may be especially unlikely to have sufficient private incentives to take care with consumer data.[154]

Another possible argument against strict liability is that it may lead to consumer moral hazard: if consumers are fully insured against harm from breaches, they will lack incentives to take cost-effective precautions (such as utilizing different passwords or creating strong passwords), or they may share too much data with firms. However, the likely inability of consumers to

150. *See, e.g.*, 15 U.S.C. § 1681t(b)(1) (preempting the application of state laws with respect to certain duties required by FCRA).

151. *See* 15 U.S.C. § 1681h(e) (limiting state actions for negligence, invasion of privacy, or defamation related to consumer reports to cases in which the defendant acted with "malice" or "willful intent to injure").

152. *See, e.g.*, *In re* Equifax, Inc. Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1327–28 (N.D. Ga. 2019). Plaintiffs also use the § 5 standard to make out claims under California's Business and Professions Code § 17200. *See, e.g.*, Complaint at 30, Rahman v. Marriot Int'l, Inc., Case No. 8:20-cv-00654, 2021 WL 346421 (C.D. Cal. June 29, 2020).

153. However, when applied, a strict liability framework generally should avoid safe harbors, as they merely replace ex-post determination of reasonableness after a triggering event with ex-ante determination of compliance with a standard. In this way, the determination and use of safe harbor thresholds can destroy informational benefits from strict liability.

154. *See, e.g.*, Data Breach Prevention and Compensation Act of 2018, S. 2289, 115th Cong. (2018) (imposing strict liability and federal notification requirements on credit reporting agencies for data breaches). The bill provides civil penalties of $100 for each consumer whose name and at least one item of personally identifying information was compromised, plus an additional $50 for each additional item of personally identifying information compromised for each consumer. *Id.* § 4(b)(2)(A).

appreciate the marginal impact of certain precautions on expected harm or the residual risk associated with sharing data conditional on certain precautions suggests that strict liability is unlikely to have a significant impact on consumer behavior. Indeed, to the extent that firms pass expected liability costs to consumers, consumers will engage in more efficient levels of data sharing. Finally, if firms pay damages to the Treasury rather than to consumers, consumers will feel the costs of data breach, providing them with incentives to take efficient precautions, mitigate harms ex-post, or to insure against harmful breaches.

VII. CONCLUSION

An optimal enforcement program for data security should require firms to internalize the external harm of their data security practices. Two facets of the FTC's current approach to data security enforcement program render it unsuitable to provide firms with correct incentives to invest in data security. First, its reasonableness requirements are opaque and estimated with error due to poor information, leaving firms uncertain about whether they are in compliance with Section 5. Second, the FTC is unable to obtain remedies that are systematically related to the harms that consumers are likely to suffer from data breaches.

Accordingly, we recommend that as Congress considers legislation to address privacy and data security concerns, it should seriously consider reforms that would give the FTC sufficient powers to operationalize a strict liability approach to data security cases with civil penalty authority. This approach has several advantages over the FTC's current data security program. First, it would harness firms' (and cyber insurers') superior private information about the specific costs and benefits of protecting consumer data, leading to more efficient levels of security. Second, the ability to levy civil penalties would allow the FTC to force firms to fully internalize the expected harms generated by their data security decisions. Finally, this approach not only would increase the efficacy of FTC enforcement, but it also would provide firms with legal certainty and readily insurable residual risk. Removing reasonableness from the FTC's approach to data security is the only reasonable path.

APPENDIX

In this Appendix, we set out the specific model of security expenditures used in the body of the Article.

Definitions:

s_i = security level of firm *i*.

$\phi(s_i)$ = probability of a breach at firm I, $\phi'(s) < 0$, $\phi''(s) > 0$.

$c(s_i)$ = total cost of security.

m_i = per data record mitigation level by firm *i*.

$h(m_i)$ = per data record mitigated harm conditional on a breach.

$e(m_i)$ = total mitigation cost per data record.

d_i = data collected by firm *i*.

$w(d)$ = total cost of data collection, use, and storage.

A1: Independent Harms

As a benchmark, consider a single site that houses unique data of size *d*, and that a data breach of that site would cause expected harm equal to $H(d, s, m)$. In the partial equilibrium model used, the problem for the social planner is to maximize the value of the data net of the costs of a potential breach and the cost of security expenditures. In particular, the social problem is to choose the level of data retained *d* and security and mitigation expenditures (*s* and *m*) in order to maximize:

$$W(s,m,d) = TP(d) - H(d,s,m) - \omega(d,s) - c(d,s) \quad (1)$$

The first order conditions are given by:

$$VMP(d) - \frac{\partial[H(d,s,m)]}{\partial d} - \frac{\partial \omega(d,s)}{\partial d} - \frac{\partial c(d,s)}{\partial d} = 0 \quad (2d)$$

$$-\frac{\partial[H(d,s,m)]}{\partial s} - \frac{\partial \omega(d,s)}{\partial s} - \frac{\partial c(d,s)}{\partial s} = 0 \quad (2s)$$

$$-\frac{\partial[H(d,s,m)]}{\partial m} = 0 \quad (2m)$$

The Figures in the body of the Article depict this outcome for the following specific functional forms and parameters. In particular, we assume that the expected harm from a breach equals:

$$H(d,s,m) = \phi(s) * d[h(m) + e(m)] \quad (3)$$

where $h(m)$ is the mitigated per unit harm generated from exposure of a unit of data *d*, $e(m)$ is the cost of firm's mitigation expenditures of *m* per exposed record, and $\phi(s)$ is the probability a breach occurs given a level of security expenditures *s*. In particular, we assume that this probability equals:

$$\phi(s) = \lambda e^{-\lambda s}, \phi'(s) = -\lambda^2 e^{-\lambda s} \quad (4)$$

The cost of data security, mitigation expenditures, and the acquisition cost of data are given by:

$$c(s) = k * s \quad (5)$$

$$e(m) = z * m \quad (6)$$

$$\omega(d) = w * d \quad (7)$$

Finally, we assume that the value of the marginal product of data is linear and diminishing ($g < 0$), and given by:

$$VMP(d) = b + gd \quad (8)$$

Under assumptions (3)–(7) the first order conditions become:

$$b + g * d - w - \phi(s) * h = 0 \quad (2d')$$

$$-\phi'(s) * h * d - k = 0 \quad (2s')$$

$$-h'(m) - z = 0 \quad (2m')$$

Simultaneously solving (2d'), (2s') and (2m') yields the values (s^*, m^*, d^*) that maximize equation (1). The graphs in the body of the Article assume the following parameter values:

$k = 2$

$w = 2$

$h = 50$

$b = 6$

$g = -.4$

A2: Common Harm

To see how the optimal security expenditures change in the presence of interdependent security, consider a setting where all N symmetric firms in an industry collect, use, and store the same data. Let $\phi_i(s_i) = \phi(s)$ denote the probability that a breach occurs at site i given symmetric security expenditures $s_i = s$. Let B denote the number of sites that are breached.

Suppose that a breach of one or more sites results in common harm $H^c = d[h(m) + e(m)]$. That is, a breach of one site is sufficient to cause the common harm, and breaches of additional sites do not cause marginal harm. Given that the same harm occurs when there is one or more breaches ($B > 0$), the probability of a breach event that generates the common harm is $P(B > 0)$. With a common equilibrium level of security s for all symmetric firms, the probability of no breach equals:

$$Prob(B = 0) = \frac{N!}{N!0!}\phi(s)^0(1 - \phi(s))^N \quad (9)$$

The probability harm is generated is the probability of one or more breach, or:

$$1 - Prob(B = 0) = 1 - (1 - \phi(s))^N \quad (10)$$

The expected harm will equal:

$$H(d, s, m) = \left[1 - \left(1 - \phi(s)\right)^N\right] d[h(m) + e(m)] - Nc(s) \quad (11)$$

First order condition for s is:

$$\frac{\partial H(d,s,m)}{\partial s} = -N[1 - \phi(s)]^{N-1}\phi'(s)d[h(m) + e(m)] - Nc'(s) = 0,$$

or equivalently:

$$-[1 - \phi(s)]^{N-1}\phi'(s)d[h(m) + e(m)] = c'(s) \quad (12)$$

Note that when the term $[1 - \phi(s)]^{N-1} = 1$, the first order condition is equivalent to the first order condition in the non-interdependent case set out above. Compared to the optimal level of security in that case *s**, and given that $[1 - \phi(x)]^{N-1} \leq 1$, it follows that *s*** < *s**. The term $[1 - \phi(x)]^{N-1}$ represents a "contagion tax" that reduces the incremental value of marginal expenditures aimed at a protecting an individual site. Intuitively, the potential that the common harm is caused by a breach at some other site j = 2, … , N reduces the value of preventing a breach at site = 1. Figure A1 illustrates the effect of security interdependence on the marginal incentives to invest in security.

Figure A1– Interdependent Security