FTC Hearings on Competition & Consumer Protection in the 21st Century

FTC Project No. P181201

Comments of the International Center for Law & Economics

Topic 9: Data Security

May 31, 2019

Authored by:

Geoffrey A. Manne (President & Founder, International Center for Law & Economics)

Justin (Gus) Hurwitz (Director of Law & Economics Programs, International Center for Law & Economics)

Julian Morris (Executive Director, International Center for Law & Economics)

Kristian Stout (Associate Director, International Center for Law & Economics)

Dirk Auer (Senior Fellow, International Center for Law & Economics)

ICLE | 2117 NE Oregon St. Suite 501 | Portland, OR 97232 | 503.770.0076
icle@laweconcenter.org | @laweconcenter | www.laweconcenter.org

Executive Summary

We thank the Commission for the opportunity to comment on "Competition and Consumer Protection in the 21st Century Hearings."

The International Center for Law and Economics (ICLE) is a nonprofit, nonpartisan research center whose work promotes the use of law & economics methodologies to inform public policy debates. We believe that intellectually rigorous, data-driven analysis will lead to efficient policy solutions that promote consumer welfare and global economic growth.

ICLE's scholars have written extensively on competition and consumer protection policy. Some of our writings are included as references in the comment below. Additional materials may be found at our website: www.laweconcenter.org.

In this comment, we primarily address the ninth topic raised by the Commission, concerning "the U.S. framework related to consumer data security, and the FTC's data security enforcement program."

Our comment addresses several pressing issues. It starts by outlining the flawed strategy which the FTC currently deploys to deal with data security issues. In a nutshell, the comment argues that the Commission's overreliance on enforcement by consent decrees has created a quasi-regulatory approach to data security, as opposed to the emergence of a common law on data security. In doing so, the FTC has adulterated some of the cornerstones of common law negligence, namely: the assessment of reasonable care on the part of the tortfeasor, the thorough analysis of causality, an economically grounded computation of harm, and the establishment that harm is likely absent some level of care.

Given these failings, we urge the FTC to consider implementing reforms that might bring its decisional practice closer to the common law tradition. These include giving more weight to economic analysis (notably by allowing the FTC's Bureau of Economics to play a greater role in data security proceedings), adopting modest measures that would increase the transparency of the FTC's data security decisions (thereby increasing legal predictability), bringing greater judicial review to data security proceedings, and incentivizing firms to better communicate their data security activities.

I. Introduction

The recent past has seen a number of landmark data breaches, the most high-profile of which was likely the Cambridge Analytica affair, whereby a private data analytics firm improperly gained access to the personal data of over a million Facebook users.[1] When news of the incident broke, it momentarily wiped billions of dollars from the social network's market cap.[2] It led to swift intervention by the FTC, which is likely to levy to a multi-billion dollar settlement,[3] and the firm is still coming to terms with the long term business ramifications of the data breach.[4] But Facebook was not alone. Another particularly high-profile breach was the attack on Marriott Starwood hotels.[5] That breach affected over 500 million customers and resulted in the unlawful access to over 5 million unencrypted passport numbers, as well as 18.5 million encrypted password numbers, 9.1 million encrypted payment card numbers, and other sensitive information.[6] On the upside, 2018 marked a sharp reduction in the number of data breaches, compared to 2017,[7] though more records were exposed than in 2017 (see figure below).

However, despite the potentially severe consequences of data security breaches, the question of what public policy is most appropriate to curtail and minimize the effects of breaches remains a heated

---

[1] Paige Leskin, *The 21 scariest data breaches of 2018*, BUSINESS INSIDER FRANCE, Dec. 30, 2018, https://www.businessinsider.fr/us/data-hacks-breaches-biggest-of-2018-2018-12; *see also* Lily Hay Newman, *The Worst Cybersecurity Breaches of 2018 So Far*, WIRED, Jul. 09, 2018, https://www.wired.com/story/2018-worst-hacks-so-far/; *see also* VERIZON, 2018 DATA BREACH INVESTIGATION REPORT (2018), https://enterprise.verizon.com/resources/reports/2018/DBIR_2018_Report_execsummary.pdf

[2] Rupert Neate, *Over $119bn wiped off Facebook's market cap after growth shock*, THE GUARDIAN, Jul. 26, 2018, https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock; *see also* Salvador Rodriguez, *Here are the scandals and other incidents that have sent Facebook's share price tanking in 2018*, CNBC, Nov. 20, 2018, https://www.cnbc.com/2018/11/20/facebooks-scandals-in-2018-effect-on-stock.html

[3] Jon Brodkin, *Facebook may face multi-billion dollar fine for Cambridge Analytica scandal*, ARSTECHNICA, Feb. 15, 2019, https://arstechnica.com/tech-policy/2019/02/facebook-may-face-multi-billion-dollar-fine-for-cambridge-analytica-scandal/; *see also* Kurt Wagner, *Facebook may be facing a "multibillion-dollar" fine from the FTC. Here's why,* VOX, Feb. 14, 2019, https://www.vox.com/2019/1/23/18193314/facebook-ftc-,fine-investigation-explained-privacy-agreement

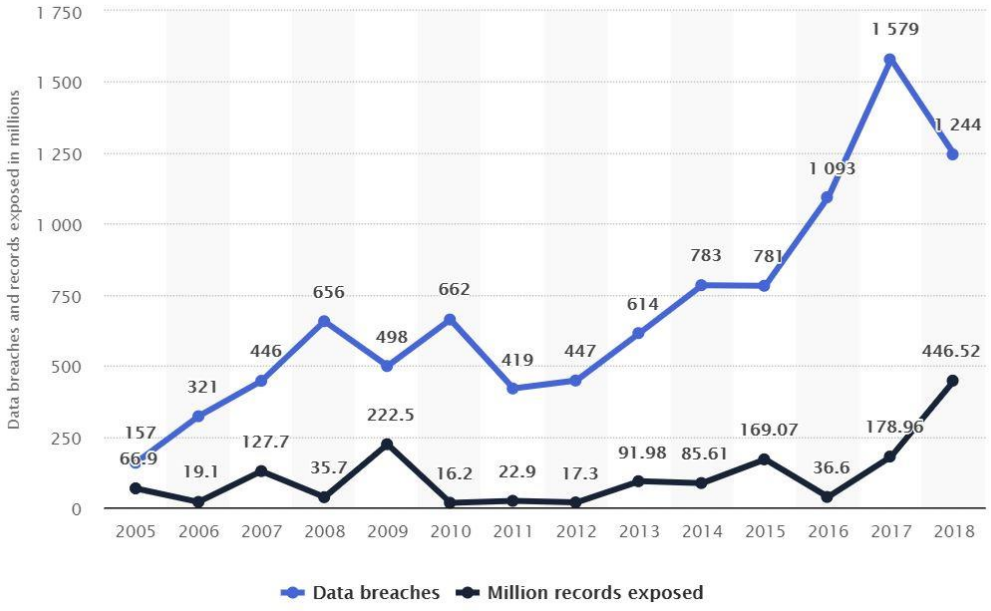
[4] Mike Isaac & Cecilia Kang, *Facebook Expects to Be Fined Up to $ 5 Billion by F.T.C. Over Privacy Issues*, N.Y. TIMES, April 24, 2019, *available at* https://www.nytimes.com/2019/04/24/technology/facebook-ftc-fine-privacy.html.

[5] Zack Whittaker, *Marriott now says 5 million unencrypted passport numbers were stolen in Starwood hotel data breach*, TECHCRUNCH, Jan. 2019, https://techcrunch.com/2019/01/04/marriott-five-million-passport-numbers-stolen-starwood/; David Volodzko, *Marriott Breach Exposes Far More Than Just Data*, FORBES, Dec. 4, 2018, https://www.forbes.com/sites/davidvolodzko/2018/12/04/marriott-breach-exposes-far-more-than-just-data/#cd296bf62978

[6] Kate O'Flaherty, *Marriot CEO reveals new details about mega breach*, FORBES, Mar. 11, 2019, https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/marriott-ceo-reveals-new-details-about-mega-breach/#57529c76155c; Zack Whittaker, *Marriott now says 5 million unencrypted passport numbers were stolen in Starwood hotel data breach*, TECHCRUNCH, Jan. 2019, https://techcrunch.com/2019/01/04/marriott-five-million-passport-numbers-stolen-starwood/

[7] Lucian Constantin, *Data breaches exposed 5 billion records in 2018*, CSO, Feb. 15, 2019, https://www.csoonline.com/article/3341317/data-breaches-exposed-5-billion-records-in-2018.html.

topic of debate, with authorities around the globe – especially in the US and the EU – often following diverging paths.[8]



[9]

Although seeking to reduce the frequency of these data breaches is, in and of itself, a laudable policy goal, it is equally important that the gains from these reductions outweigh the costs that are imposed upon firms and consumers. Indeed, using foreseeably available technology, the only world with zero online data breaches is one where people stop using the internet altogether. For this reason, we believe the FTC should follow a rigorous cost/benefit approach that would ultimately maximize consumer welfare. For the same reason, we believe that the FTC should encourage the emergence of bottom-up data security standards, which would provide a better balance between the various

[8] In Europe, the General Data Protection Regulation introduced a number of measures that deal with data security issues. It notably requires companies to report data breaches within 72 hours of their discovery: "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." *See* GDPR art. 33. Companies currently take, on average 49 days to report breaches. *See* Constantin, *supra* note 7.

[9] Victor Reklaitis, *How the number of data breaches is soaring-in one chart*, MARKETWATCH, May 25, 2018, https://www.marketwatch.com/story/how-the-number-of-data-breaches-is-soaring-in-one-chart-2018-02-26, Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions), STATISTA, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

costs and benefits at play than would top-down alternatives such as the imposition of strict ex ante obligations upon firms.

With this in mind, our comment assesses the FTC's current approach to data security. It argues that the Commission should deal with the threat of data breaches by developing a true common law of data security, rather than further cementing its historical approach based on thinly substantiated consent decrees and non-binding guidance documents. In other words, our comment argues that the FTC should discard its quasi-regulatory approach to data security matters in favor of a true common law alternative.

Unlike statutory law, which is based upon the text of statutes passed by legislatures, or regulations, which are promulgated and enforced by regulatory agencies, the common law is (broadly speaking) based on general principles and made up of specific rules developed over time in response to real-world disputes adjudicated in courts. This allows it to evolve in response to changing circumstances.[10] In the abstract, of course, the FTC's process is neither evolutionary in nature nor does it produce general rules, as would be the case for true common law.[11] Rather, it is a succession of wholly independent cases, without any precedent, narrow in scope, and binding only on the parties to each particular case. Like all regulation, it tends to be static; the FTC is, after all, an enforcement agency, charged with enforcing the strictures of specific and little-changing pieces of legislation and regulation. As we will discuss below, for better or worse, much of the FTC's data security adjudication adheres unerringly to the terms of the regulations it enforces with little in the way of gloss or evolution. As such, the FTC's process in data security cases tends to reject the ever-evolving "local knowledge" of individual actors and substitutes instead the inherently limited legislative and regulatory pronouncements of the past. By contrast, real common law emerges through a case-by-case, bottom-up process; as a result, it adapts to changing social and economic circumstances and is far less susceptible to the knowledge and rent-seeking problems that bedevil legislatures and administrative agencies. Constant litigation tends to weed out inefficient rules, enabling the common law to retain a generally efficient character unmatched by legislation, regulation, or even administrative enforcement.

Although there are a number of legislative reforms that would undoubtedly help, the FTC is today perfectly capable of conducting its data security investigations and enforcement actions in a way that would comport with traditional negligence analysis and thereby cure many of the defects in its current process.

---

[10] *See, e.g.,* Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 233 (Minn. 1998). The Minnesota Supreme Court defined the common law as: "the embodiment of broad and comprehensive unwritten principles, inspired by natural reason, an innate sense of justice, adopted by common consent for the regulation and government of the affairs of men. It is the growth of ages, and an examination of many of its principles, as enunciated and discussed in the books, discloses a constant improvement and development in keeping with advancing civilization and new conditions of society. Its guiding star has always been the rule of right and wrong, and in this country its principles demonstrate that there is in fact, as well as in theory, a remedy for all wrongs."

[11] *Id.* at 234.

To begin with, ***the FTC must introduce some concrete, publicly available standards*** (and well-defined safe harbors) from which firms can reliably determine whether their conduct comports with their duties with respect to data they possess and the likely risk of harm of a breach, given the relevant facts of their business activities. Included among these should be a clear statement regarding whether and how mere possession of data could lead to liability, the magnitude of increased risk that will constitute "likely" harm, and clear standards for measuring it. We are sympathetic to the criticism of published guidelines; that technology changes quickly and thus published, ex ante standards may be both under- and over-inclusive, especially over time. But given the virtually unconstrained scope of the FTC's discretion and its current processes, merely telling firms to behave "reasonably" using non-binding guidance documents, overinclusive complaints, and unspecific closing letters, seems woefully insufficient as a guide to firms' increasingly important duties under the law with respect to their customers' data.

Perhaps most critically, ***the FTC should both enunciate and follow clear standards of proof of causation in its data security enforcement decisions***. It is impossible to have perfect data security, and some number of breaches will always occur, even under the best of circumstances. Without true guidance as to when a particular breach was proximately "caused" by insufficient security, FTC enforcement will continue to appear arbitrary. This is even more important in cases where the FTC chooses to rely on its "likely to cause" authority: Without a well-established connection between any given set of data security practices and their ability to constitute a proximate cause of "likely" harm, Section 5 becomes an unbounded source of enforcement authority, virtually regardless of the measures that firms take to protect data.

The Commission could also introduce several self-imposed measures that would reduce the almost unbounded discretion which it currently enjoys in data security cases. Though this strategy might seem counterintuitive – the FTC would essentially make it harder for itself to prosecute some cases – it would ultimately support the FTC's core mission: protecting consumers and promoting competition. In other words, reducing its discretion might make it harder for the FTC to prosecute cases, but it would increase the probability that the right legal standards emerge from ensuing litigation. We suggest a series of possible steps in this direction. These range from increasing the role that economists play in the Commission's deliberations, to making its decisions more transparent and amenable to judicial review.

Moreover, to the extent that the agency is already constrained by its own internal procedures, it should be more active in distilling and publicizing them.[12] Doing so would increase the accountability of the agency as well as providing better guidance to industry.

---

[12] There is some evidence to suggest that internal constraints are in fact in operation. In particular, the Commission reportedly closes approximately seventy percent of data security investigation that it formally opens. *See* Jeremy Snow, *FTC closes 70 percent of data security investigations*, FEDSCOOP, June 28, 2016, *available at* https://www.fedscoop.com/ftc-closes-more-investigations-than-it-brings-in-commissioner-says/

Should the Commission fail to heed these calls for reform, its enforcement philosophy will remain decidedly fatalistic, effectively making it impossible for firms to reliably ensure that their data security practices are sufficient to meet the standard of Section 5. This status quo is untenable insofar as it means that once a company collects sensitive data it may be presumptively in violation of the statute, with only the vagaries of prosecutorial discretion to separate legal and illegal conduct. Likewise, when breaches actually occur the FTC's position is improper: Inferring unreasonable security practices from the fact of unauthorized disclosure alone, without any demonstration of concrete harm or even rigorous assessment of the *likelihood* of harm, effectively converts Section 5 into a strict liability standard, in clear contravention of the statute.

II. The FTC's flawed "reasonableness" approach to data security

Although the FTC is well-staffed with highly skilled economists, its approach to data security is disappointingly light on economic analysis. The unfortunate result of this lacuna is an approach to these complex issues lacking in analytical rigor and the humility borne of analysis grounded in sound economics. In particular, the Commission's "reasonableness" approach to assessing whether data security practices are unfair under Section 5 of the FTC Act lacks all but the most superficial trappings of the well-established law and economics of torts, from which the concept is borrowed.

The mere label of reasonableness and the claimed cost-benefit analysis by which it is assessed are insufficient to meet the standards of rigor demanded by those concepts. Consider this example: In 2016 the Commission posted on its website an FTC staff encomium to "the process-based approach [to data security] that the FTC has followed since the late 1990s, the 60+ law enforcement actions the FTC has brought to date, and the agency's educational messages to companies."[13] The staff writes:

> From the outset, the FTC has recognized that there is no such thing as perfect security, and that security is a continuing process of detecting risks and adjusting one's security program and defenses. For that reason, the touchstone of the FTC's approach to data security has been reasonableness – that is, a company's data security measures must be reasonable in light of the volume and sensitivity of information the company holds, the size and complexity of the company's operations, the cost of the tools that are available to address vulnerabilities, and other factors. Moreover, the FTC's cases focus on whether the company has undertaken a reasonable process to secure data.[14]

In its *LabMD* opinion, the Commission describes this approach as "cost-benefit analysis."[15] But simply listing out (some) costs and benefits is not the same thing as *analyzing* them. Recognizing that tradeoffs exist is a good start, but it is not a sufficient end, and "reasonableness"—if it is to be anything other than the mercurial preferences of three FTC commissioners—must contain analytical content. Indeed, to be consistent with the common law meaning of the term, "reasonableness" implies the existence of clearly enunciated and applied *standards* that are of general application.

A few examples from the staff posting illustrate the point:

> In its action against Twitter, Inc., the FTC alleged that the company gave almost all of its employees administrative control over Twitter's system. According to the FTC's complaint, by providing administrative access to so many employees, Twitter *increased the risk*

---

[13] Andrea Arias, *The NIST cybersecurity framework and the FTC*, Fed. Trade Comm'n: Business Blog (Aug. 31, 2016 2:34 PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.

[14] *Id.*

[15] LabMD, Inc., Docket No. C-9357 at 11 (F.T.C. July 29, 2016) [hereinafter FTC LabMD Opinion], *overturned by* 894 F.3d 1221 (11th Cir. 2018).

> *that a compromise of any of its employees' credentials could result in a serious breach*. This principle comports with the [NIST] Framework's guidance about managing access permissions, incorporating the principles of least privilege and separation of duties.[16]

Twitter's conduct is described as having "increased the risk" of breach.[17] In this example even a *recitation* of the benefits is missing. But regardless, the extent of increased risk sufficient to support liability, the cost of refraining from the conduct, and any indication of how to quantify and weigh the costs and benefits is absent. Having disclaimed a belief in "perfect data security," the staff, wittingly or not, effectively identifies actionable conduct as virtually *any* conduct, because virtually any decision can "increase the risk" above a theoretical baseline of zero. Crucially, this extends not only to actual security decisions, but to decisions regarding the amount and type of regular business practices that involve any amount of collection, storage, or use of data.

In another example, the staff writes:

> Likewise, in Franklin's Budget Car Sales, Inc., the FTC alleged that the company didn't inspect outgoing Internet transmissions to identify unauthorized disclosures of personal information. Had these companies used tools to monitor activity on their networks, they could have reduced the risk of a data compromise or its breadth.[18]

Should "reasonable" data security mean that firms are required to do *anything* and *everything* that "could have reduced the risk" of breach? Again, that would mean that virtually any conduct could be sufficient, because there is almost always *something* that could further reduce risk—including limiting the scope or amount of normal business activity: while it surely would reduce the "risk" of breach if, for instance, a firm were significantly to limit the number of customers it serves, eschews the use of computers, and conduct all its business in a single, fortified location, it is unlikely that such behavior would be economically or socially desirable.

Of course, "reasonable" data security can't really require these extremes. But such unyielding uncertainty over its contours means that companies may be required to accept the reality that, no matter what they do *short* of the extremes, liability is possible. Worse, there is no way reliably to judge whether conduct (short of obvious fringe cases) is even *likely* to increase liability risk.

The *LabMD* case highlights the scope of the problem and the lack of economic analytical rigor endemic to the current "common law" data security standard. To be sure, other factors also contribute to the lack of certainty and sufficient rigor, (*i.e.*, matters of process at the agency), but at root sits a "standardless" standard, presented as an economic framework.[19]

---

[16] Arias, *supra* note 13 (emphasis added).

[17] *Id.*

[18] *Id.* (emphasis added).

[19] *See, e.g.,* Maureen K. Ohlhausen, Acting Chairman, Fed. Trade Comm'n, Opening keynote at the ABA consumer protection conference 2-3 (Feb. 2, 2017), https://www.ftc.gov/system/files/documents/public_statements/1069803/mko_aba_consumer_protection_conference.pdf.

In its enforcement complaint the Commission ultimately alleged two separate security incidents: the downloading of the 1718 file by Tiversa, and the mysterious exposure of a cache of "day sheets" allegedly originating from LabMD and discovered in Sacramento, CA. The FTC alleged that each incident was caused by LabMD's "failure to employ 'reasonable and appropriate' measures to prevent unauthorized access to personal data," and "caused, or is likely to cause, substantial harm to consumers . . . constitut[ing] an unfair practice under Section 5(a) of the Federal Trade Commission Act . . . ."[20]

The administrative law judge (ALJ) ruled against the Commission in his initial determination, holding, among other things, that the term "likely" means "having a high probability of occurring or being true,"[21] and that the FTC failed to demonstrate that LabMD's conduct had a high probability of injuring consumers. The ALJ put down a critical marker in the case, one that gave some definition to the FTC's data security standard by demarcating those instances in which the Commission may exercise its authority to prevent harms that are *actually* likely to occur from those that are purely speculative.

In its vote to overturn the ALJ, the Commission found among other things:

1. That "a practice may be [likely to cause substantial injury] if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low;"

2. That the FTC established that LabMD's conduct in fact, "caused or was likely to cause" injury as required by Section 5(n) of the FTC Act;

3. That substantiality, "does not require precise quantification. What is important is obtaining an overall understanding of the level of risk and harm to which consumers are exposed;" and

4. That "the analysis the Commission has consistently employed in its data security actions, which is encapsulated in the concept of 'reasonable' data security" encompasses the "cost-benefit analysis" required by the Act's unfairness test.[22]

In actuality, however, the Commission's purported "reasonableness" standard—which, as its name suggests, purports to evaluate data security practices under a negligence-like framework—actually amounts in effect to a rule of strict liability for any company that collects personally identifiable data.

---

[20] Brief of Complainant at 5, LabMD, Inc., 160 F.T.C. No. 9357, 2015 WL 7575033 (Nov. 13, 2015) [hereinafter FTC Complainant Brief].

[21] Initial Decision at 42, LabMD Inc., 160 F.T.C. No. 9357, 2015 WL 7575033 (Nov. 13, 2015) [hereinafter ALJ LabMD Initial Decision] (The day sheets were ultimately excluded from evidence because the FTC couldn't prove whether the documents had ever been digital records, nor could it prove how the day sheets made their way out of LabMD and to Sacramento).

[22] FTC LabMD Opinion, *supra* note 15, at 10-11.

In its decision to overturn the Commission's ruling, the Eleventh Circuit does not address most of the problems we identify in this comment,[23] which means that many problems therefore remain uncorrected (as yet) by the courts. But it does nicely reinforce a core underpinning of our analysis (the common law negligence basis of the requisite analysis under the Commission's Section 5 unfairness authority) and thus the apparent applicability of our broader arguments:

> The Commission must find the standards of unfairness it enforces in "clear and well-established" policies that are expressed in the Constitution, statutes, or the common law. The Commission's decision in this case does not explicitly cite the source of the standard of unfairness it used in holding that LabMD's failure to implement and maintain a reasonably designed data-security program constituted an unfair act or practice. It is apparent to us, though, that the source is the common law of negligence.[24]

A subtle but very important contour of the Eleventh Circuit's decision is its reliance on the "public policy" prong of the Unfairness Statement as a framing device for its view of *LabMD*.[25] According to the Unfairness Statement, it is not strictly necessary that the Commission base its decision upon "public policy" grounds, and indeed, owing to the highly subjective nature of declaring what is and is not "public policy," it can be dangerous if the Commission broadly resurrects its "public policy"-driven approach to consumer protection. Yet, the Eleventh Circuit's intuition is not wholly inappropriate in *LabMD*. The Commission has for years pursued a so-called "common law of data security," initially rooted in its deception authority, but more commonly brought under its unfairness authority today. There are roughly two possibilities for how to look at this "common law": either as an exercise of general unfairness power related to consumer injury or unethical behavior,[26] or else as arising out of an established public policy.[27]

Yet, the language of the Commission, as we detail further *infra*, as well as its behavior in developing a "common law" of data security suggests strongly that the Commission is developing something like a negligence analysis in its data security practice. Thus, to the limited extent that the court employed the public policy prong of the *Sperry & Hutchinson* factors, it appears appropriate to hold the Commission to the obligation to adopt "clear and well established" principles of negligence law.

The Eleventh Circuit in *LabMD*, however, ultimately declined to explore the contours of how a proper negligence-like analysis would apply to the Commission's Section 5 unfairness authority.[28]

---

[23] *See, generally,* LabMD, Inc. v FTC, 894 F.3d 1221 (11th Cir. 2018) [hereinafter "11th Circuit Opinion"].

[24] 11th Circuit Opinion, 894 F.3d at 1231.

[25] *See, generally*, *Id.*

[26] *See Letter from the FTC to the House Consumer Subcommittee*, appended to In re Int'l Harvester Co., 104 F.T.C. 949, 1073 (1984) ["Unfairness Policy Statement" or "UPS"], available at http://www.ftc.gov/ftc-policy-statement-on-unfairness.

[27] *Id.*

[28] The court described the Commission's actions as relying upon negligence law, but, in order to reach its holding, simply assumed that its negligence-like analysis was broadly correct, *Id.* at 17-18, and limited its analysis to the appropriateness of the Commission's particular remedy sought in light of the harms alleged. *Id.* at 18.

Yet, in oral arguments (as noted below), the court suggested that multiple deficiencies exist in the Commission's Section 5 data security enforcement when viewed through a negligence lens.[29]

In the following sections, our comment explores these (and other) defects in the Commission's LabMD decision and its approach to data security enforcement under Section 5 more generally.

A. The FTC's unreasonable "reasonableness" approach to data security

Consumer welfare is the lodestar of Section 5. Like the consumer-welfare-oriented antitrust laws, Section 5 does not proscribe specific acts but is a general standard, designed to penalize and deter "unfair" conduct that harms consumers on net—*without* sweeping in pro-consumer conduct that does not cause demonstrable harm (or that is "reasonably avoidable" by consumers themselves).[30]

In form, Section 5(n) and the Unfairness Statement from which it is derived incorporate a negligence-like standard,[31] rather than a strict-liability rule. Section 5(n) states that:

> The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice

---

[29] *See, e.g., infra*, note 23 and accompanying text.

[30] *See* FTC LabMD Opinion, *supra* note 15, at 26 (quoting Unfairness Policy Statement, *supra* note 26 at 1073 ("A 'benefit' can be in the form of lower costs and . . . lower prices for consumers, and the Commission 'will not find that a practice unfairly injures consumers unless it is injurious in its net effects.'").

[31] *See* 11th Circuit Opinion, 894 F.3d at 1231. But, in point of fact, Section 5 most likely contemplates *more* than mere negligence—i.e., recklessness. As LabMD's initial merits brief argues: "While the FTC correctly recognized that something more than satisfaction of Section 5(n) is required, the Opinion erred in using "unreasonableness" as that something more. Instead, culpability under Section 5 requires a showing that the practice at issue was not merely negligent (i.e., "unreasonable"), but instead involved more egregious conduct, such as deception or recklessness—namely, that the practice was "unfair." "The plain meaning of 'unfair' is 'marked by injustice, partiality, or deception.'" LeBlanc v. Unifund CCR Partners, 601 F.3d 1185, 1200 (11th Cir. 2010) (quoting Merriam-Webster Online Dictionary (2010)); *see* FTC v. Wyndham Worldwide, Inc., 799 F.3d 236, 245 (3d Cir. 2015) (suggesting that, to the extent "these are requirements of an unfairness claim," such requirements were met based on defendant's allegedly deceptive statements); TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 496-97 (1st Cir. 2009) (analyzing unfairness under Massachusetts consumer protection statute, which incorporates "FTC criteria"; concluding that the statute covers only "egregious conduct"; and finding defendant's alleged "inexcusable and protracted reckless conduct" met the "egregious conduct" test). Here, the FTC made no finding that LabMD's failure to employ the Additional Security Measures was deceptive or reckless or otherwise involved conduct sufficiently culpable to be declared "unfair." The absence of any finding that LabMD's conduct fell within the definition of the term "unfair" rendered the FTC's Section 5 analysis fatally incomplete." Brief of Petitioner at 28, LabMD Inc. v. FTC, (11th Cir. Sep. 29, 2016) (No. 16-16270) [hereinafter "*LabMD 11th Cir. Petitioner Brief*"].Although we agree with the thrust of this argument, in this article we contend that the "something more" contemplated by Section 5 can be incorporated into the FTC's "reasonableness" approach (assuming it were ever properly deployed). In particular (and as discussed below), "likely to cause substantial injury," properly understood (e.g., as interpreted by the ALJ in LabMD) clearly entails a level of risk beyond that implied by mere negligence. Moreover, logic and, arguably, the constitutional requirement of fair notice demand that the duty of care to which companies are properly held for data security purposes be defined by standards known or presumptively known to companies (e.g., widely accepted industry standards).

> causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[32]

Congress plainly intended to constrain potentially hasty assumptions that imposing nearly *any* costs on consumers is "unfair."[33] Unfairness thus entails a balancing of risk, benefits, and harms, and a weighing of avoidance costs consistent with a negligence regime (or at least, with respect to the last of these, strict liability with contributory negligence).[34] Easily seen and arguably encompassed within this language are concepts from the common law of negligence such as causation, foreseeability, and duty of care. As one court has described it in the data security context, Section 5(n) contemplates "a cost-benefit analysis . . . [that] considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."[35]

The Commission has previously described this as a "reasonableness" approach that specifically eschews strict liability:

> The touchstone of the Commission'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 Commission . . . 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.[36]

Giving purchase to a reasonableness approach under the Commission's own guidance would seem to require establishing (i) a clear baseline of appropriate conduct, (ii) a company's deviation from that baseline, (iii) proof that its deviation caused, or was significantly likely to cause, harm, (iv) significant harm, (v) proof that the benefits of (e.g., the cost savings from) its deviation didn't outweigh the expected costs, and (vi) a demonstration that consumers' costs of avoiding harm would have been greater than the cost of the harm.[37]

---

[32] 15 U.S.C. § 45(n) (2012).

[33] No market interaction is ever without costs: paying any price, waiting in line, or putting up with advertising are all "costs" to a consumer.

[34] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 291 (AM. LAW INST. 1965) ("Where an act is one which a reasonable man would recognize as involving a risk of harm to another, the risk is unreasonable and the act is negligent if the risk is of such magnitude as to outweigh what the law regards as the utility of the act or of the particular manner in which it is done.").

[35] FTC v. Wyndham Worldwide, Inc., 799 F.3d 236, 255 (3d Cir. 2015).

[36] Commission Statement Marking the FTC's 50th Data Security Settlement at 1 (Jan. 31, 2014), *available at* http://bit.ly/2hubiwv (emphasis added).

[37] *Id.*; *see also* 15 U.S.C. § 45(n) (2012).

Indeed, as noted above, the Commission has itself previously declared that when relying on public policy to identify consumer harm, its Section 5 authority must be derived from "formal sources such as statutes, judicial decisions, or the Constitution as interpreted by the courts, rather than being ascertained from the general sense of the national values."[38] Parsing the complaint and Order, the Eleventh Circuit believed (as do we) that this meant that the common law of negligence was the natural source of law (and, by implication, constraint) to apply in the *LabMD* case.[39]

But the Commission's development of the case is somewhat at odds with this approach. During oral arguments before the Eleventh Circuit, the court questioned the FTC about what "reasonableness" entails and how litigants are expected to understand their obligations:

> **Judge Tjoflat**: And business, industries, have got to figure out what the Commission means by reasonably . . . They'll never know what the Commission means, something happens and the Commission will say it's unreasonable.*
>
> **FTC Attorney**: Well, let me say, this is not a close case at all. This is a case where we have . . . ment
>
> **Judge Tjoflat**: I'm not talking about this close case. Just the plain unreasonableness test. An industry can think it's reasonable, and something happens, and the Commission will say it's unreasonable—in hindsight you should have done such and such . . .
>
> **FTC Attorney**: That happens to businesses in tort law all the time. It could be people say I didn't realize this is unreasonable, well, you know, the things that you need to do to establish that you're acting reasonably are the kind of things that are laid out in the available guidances . . .
>
> **Judge Tjoflat**: There is a difference between tort law in the common law application and in a government rule as to what is reasonable and not reasonable. I think that's the essence—the public policy implications—it seems to me, of what you're saying, is an unlimited license to figure out what is reasonable and unreasonable in the economy. And the Commissioners will sit around and decide what is reasonable and I don't believe that's a good public policy objective.
>
> **FTC Attorney**: Well, I believe that's exactly what Congress intended.[40]

Thus, it appears that, in the view of the Commission, it need not engage with the distinct elements of a case, nor offer an analysis of past cases, adequate to give sufficient notice to investigative targets beyond their need to act "reasonably."

---

[38] Unfairness Policy Statement, *supra* note 26.

[39] 11th Circuit Opinion, 894 F.3d at 1231.

[40] Oral Argument at 35-36, LabMD Inc. v. FTC, (11th Cir. Sep. 29, 2016) (No. 16-16270) [hereinafter *"LabMD 11th Circuit Oral Argument"*], *available at* https://www.ca11.uscourts.gov/system/files_force/oral_argument_recordings/16-16270.mp3?download=1 (transcript on file with the authors).

Yet, by eliding the distinct elements of a Section 5 unfairness analysis in the data security context, the FTC's "reasonableness" approach ends up ignoring Congress' requirement — whether based on "public policy" or otherwise — that the Commission demonstrate duty, causality and substantiality, and perform a cost-benefit analysis of risk and avoidance costs. While the FTC nods to the existence of these elements, its inductive, short-cut approach of attempting to define reasonableness by reference to the collection of practices previously condemned by its enforcement actions need not—and, in practice, does not—actually entail doing so. Instead, we "don't know . . . whether . . . practices that have not yet been addressed by the FTC are 'reasonable' or not,"[41] and we don't know how the Commission would actually weigh them in an actual rigorous analysis.

In its *LabMD* opinion, for instance, the Commission claims that it weighed the relevant facts. But if it did, it failed to share its analysis beyond a few anecdotes and vague, general comparisons. Moreover, it failed in any way to adduce how specific facts affected its analysis, demonstrate causation, or evaluate the relative costs and benefits of challenged practices and its own remedies. The Commission asserted, for example, that the exposed data was sensitive,[42] but it said nothing about (i) whether any of it (*e.g.*, medical test codes) could actually reveal sensitive information; (ii) what proportion of LabMD's sensitive data was exposed; (iii) the complexity or size of the business; (iv) the indirect costs of compliance, such as the opportunity costs of implementation of the FTC's required remedies; and (v) the deterrent effect of its enforcement action (among other things).

Perhaps more significantly, the FTC conducted an inappropriately *post hoc* assessment that considered only those remedial measures it claimed would address the specific breach at issue. But this approach ignores the overall compliance burden on a company to avoid excessive risk without knowing, *ex ante*, which specific harm(s) might occur. Actual compliance costs are far more substantial, and require a firm to evaluate which of the universe of possible harms it should avoid, and which standards the FTC has and would enforce. This is a far more substantial, costlier undertaking than the FTC admits.

Implicitly, the Commission assumes that the specific cause of unintended disclosure of PII was the only (or the most significant, perhaps) cause against which the company should have protected itself. It also violates a basic principle of statistical inference by inferring a high prior probability (or even a certainty) of insufficient security from a single, post hoc occurrence. In reality, however, while the conditional probability that a company's security practices were unreasonable given the occurrence of a breach may be *higher* than average, assessing by how much (or indeed if at all) requires the clear establishment of a baseline and a rigorous evaluation of the contribution of the company's practices to any deviation from it. The FTC's approach fails to accomplish this, and, as discussed in more detail below, imposes a de facto strict liability regime on companies that experience a breach, despite

---

[41] Omer Tene, *The Blind Men, the Elephant and the FTC's Data Security Standards*, PRIVACY PERSPECTIVES BLOG (Oct. 20, 2014), *available at* http://bit.ly/2hJwlwI (emphasis in original).

[42] FTC LabMD Opinion, *supra* note 15, at 16.

its claim that "the mere fact that a breach occurred does not mean that a company has violated the law."[43]

1. A Duty Without Definition

Section 5(n) plainly requires a demonstrable connection between conduct and injury.[44] While the anticompetitive harm requirement that now defines Sherman Act jurisprudence was a judicial construct,[45] Section 5(n) itself demands proof that an "act or practice causes or is likely to cause substantial injury" before it may be declared unfair.[46] But the FTC's reasonableness approach, as noted, is not directed by the statute, which nowhere defines actionable conduct as "unreasonable"; rather, the statute requires the agency to engage in considerably more in order to identify unreasonable conduct. But even assuming "reasonableness" is meant as shorthand for the full range of elements required by Section 5(n), the FTC's approach to reasonableness is insufficient.

The FTC aims to engage in a case-by-case approach to unreasonableness, eschewing prescriptive guidelines in an effort to avoid unnecessarily static definitions. While agencies do have authority to issue regulations through case-by-case adjudication,[47] that ability is not without limit. And despite the FTC's reliance upon the Supreme Court's *Chenery* case for the principle that it is entitled to "develop behavioral standards by adjudication" on a case-by-case basis,[48] *Chenery* does not provide unbounded support.

To begin with, *Chenery* holds that agencies may not rely on vague bases for their rules or enforcement actions and expect courts to "chisel" out the details:

> If the administrative action is to be tested by the basis upon which it purports to rest, that basis must be set forth with such clarity as to be understandable. It will not do for a court to be compelled to guess at the theory underlying the agency's action; nor can a court be expected to chisel that which must be precise from what the agency has left vague and indecisive. In other words, 'We must know what a decision means before the duty becomes ours to say whether it is right or wrong.'[49]

In the data security context, the FTC's particular method of case-by-case adjudication—reliance upon a purported "common law" of ill-detailed consent orders—entails exactly the sort of vagueness that the *Chenery* court rejected as a valid basis for agency action. The FTC issues complaints based on the "reason to believe" that an unfair act has taken place. Targets of these complaints settle for myriad

---

[43] FTC LabMD Opinion, *supra* note 15, at 10.

[44] 15 U.S.C. § 45(n) (2012).

[45] *See, e.g.,* Cont'l T.V., Inc. v. GTE Sylvania, Inc., 433 U.S. 36 (1977).

[46] 15 U.S.C. § 45(n) (2012).

[47] Sec. & Exch. Comm'n v. Chenery Corp., 332 U.S. 194, 203 (1947).

[48] Brief for Respondent at 49.

[49] *Chenery Corp.*, 332 U.S. at 196–97 (emphasis added).

reasons and no outside authority need review the sufficiency of the complaint. And the consent orders themselves are, as we have noted, largely devoid of legal and even factual specificity. As a result, the FTC's authority to initiate an enforcement action based on any particular conduct is effectively based on an ill-defined series of previous hunches—hardly a sufficient basis for defining a clear legal standard.

But the FTC's reliance upon *Chenery* is even more misguided than this. In *Chenery*, the respondent, a company engaged in a corporate reorganization, was governed by statutory provisions that explicitly required it to apply to the Securities and Exchange Commission (SEC) for permission to amend its filings in order to permit the conversion of its board members' preferred stock into common stock in the new corporation.[50] In upholding the SEC's authority to block the proposed amendment, the Court opined that:

> The absence of a general rule or regulation governing management trading during reorganization did not affect the Commission's duties in relation to the particular proposal before it. The Commission . . . could [act] only in the form of an order, entered after a due consideration of the particular facts in light of the relevant and proper standards. That was true regardless of whether those standards previously had been spelled out in a general rule or regulation. Indeed, if the Commission rightly felt that the proposed amendment was inconsistent with those standards, an order giving effect to the amendment merely because there was no general rule or regulation covering the matter would be unjustified.[51]

The Court thus based its holding on the fact that the SEC was, without question, responsible for approving these sorts of transactions, and the parties understood that they had to apply to the SEC for approval. Accordingly, the Court held that the SEC could not help but act and would have to rely upon either a prior rulemaking or a case-by-case assessment based on previously established standards. There is no such certainty with respect to FTC enforcement of Section 5. Instead, the FTC seeks targets for investigation and exercises prosecutorial discretion without full disclosure of the basis upon which it does so. Targets have no particular foreknowledge of what the FTC expects of them in the data security context. Thus, when the FTC undertakes enforcement actions without clearly defined standards and under constraints that ensure that it will not undertake enforcement against the vast majority of unfair acts—and without any guidance regarding why it decided *not* to undertake these actions—it does not set out a reasonable regulatory standard. Rather, from the target's point of view, any action appears more predatory and effectively arbitrary than it is regulatory.

This is not to say that reasonableness must be defined with perfect specificity in order to meet the requirements of *Chenery*; reasonableness is necessarily a somewhat fuzzy concept. But courts have

---

[50] *Id.* at 201.

[51] *Id.*

developed remarkably consistent criteria for establishing it. Thus, under typical negligence standards, an actor must have—and breach—a duty of care before its conduct will be deemed unreasonable.[52] This requires that the actor's duty be defined with enough specificity to make it clear when her conduct breaches it. In most jurisdictions, "care" is defined by reference to standard industry practices, specific legislative requirements, contractual obligations, or a prior judicial determination of what prudence dictates.[53] Moreover, in most jurisdictions, the appropriate standard of care reflects some degree of foreseeability of harm; there is no duty to protect against unforeseeable risks.[54]

The FTC has established no concrete benchmark of due care for data security, nor has it properly established any such benchmark in any specific case. To be sure, the Commission has cited to some possible sources,[55] but it has failed to distinguish among such sources, to explain how much weight to give any of them, or to distill these references into an operable standard. Not only was this true at the time of LabMD's alleged conduct, but it remained the case six to seven years *later* when the case was adjudicated—and still holds true today.[56]

Crucially, because "perfect" data security is impossible, not all data security practices that "increase" a risk of breach are unfair.[57] *Some* amount of harm (to say nothing of *some* number of breaches) is fully consistent with the exercise of due care—of "reasonable" data security practices. For the statute to be meaningful, data security practices must be shown to fall outside of customary practice—i.e., to increase the risk of unauthorized exposure (and the resulting harm) above some "customary" level—before they are deemed unreasonable.

The FTC's decision in *LabMD* asserted that this standard is sufficiently well defined, that LabMD's failure to engage in certain, specific actions enabled the data breach to occur, and thus that LabMD must have deviated from an appropriate level of care.[58] But it is not the case that LabMD had *no* data security program. Rather, "LabMD employed a comprehensive security program that included a compliance program, training, firewalls, network monitoring, password controls, access controls, antivirus, and security-related inspections."[59] While the Commission disputed some of these practices, for every practice the FTC claims LabMD did *not* engage in, there were other practices in which

---

[52] *See* STUART M. SPEISER ET AL., 2A AMERICAN LAW OF TORTS § 9:3 (2016).

[53] RESTATEMENT (SECOND) OF TORTS § 285 (1965).

[54] *Id.* at § 302. *See also* David Owen, *Duty Rules*, 54 VAND. L. REV. 767, 778 (2001) ("In general, actors are morally accountable only for risks of harm they do or reasonably should contemplate at the time of acting, for the propriety of an actor's choices may be fairly judged only upon the facts and reasons that were or should have been within the actor's possession at the time the choice was made.").

[55] *See, e.g.,* FTC LabMD Opinion, *supra* note 15, at 12 (referring to HIPAA as "a useful benchmark for reasonable behavior").

[56] As the 11th Circuit has pointed out. CITE to 11th Circuit Opinion, 894 F.3d at 1231.

[57] *See* COMMISSION STATEMENT, *supra* note 36, at 1.

[58] FTC LabMD Opinion, *supra* note 15, at 17-25.

[59] LabMD 11th Cir. Petitioner Brief, *supra* note 31, at 2 (citations to the record omitted).

it inarguably *did* engage.[60] And the FTC did not establish that, taken together and even absent the specific practices discussed by the FTC, these practices were outside of the normal range of customary data security protections.

Importantly, where, as in *LabMD*, the FTC focuses on the sufficiency of precautions relating to the *specific* harm that occurred, it fails to establish the requirements for an overall data protection scheme, which is the relevant consideration. The general security obligations under which any company operates prior to a specific incident are not necessarily tied to that incident. *Ex ante*, in implementing its security practices, LabMD would not necessarily have focused particularly on the P2P risk, which was, at the time, arguably not generally well understood nor viewed as very likely to occur. Before Tiversa's incursion, LabMD surely faced different security risks, and undertook a range of measures to protect against them. Given this, the existence of P2P software on one computer, in one department, and against LabMD's policy, was arguably not inherently unreasonable in light of the protections LabMD *did* adopt. Yet the Commission invalidated all of LabMD's data protection measures because of the single breach that *did* occur.

The truth is that the FTC simply did not establish that LabMD's practices were insufficient to meet its duty of care.[61] At best, the Commission argued that LabMD failed to engage in *some* conduct that *could* be part of the duty of care. But even if LabMD failed to engage in every practice derived from FTC consent decrees (most of which post-date the relevant time period in the case), or some of the practices described in one or more of the industry standard documents to which the FTC refers,[62] the Commission did not demonstrate that LabMD's practices, *as a whole*, were insufficient to meet a reasonable standard of care.

---

[60] *Id.*

[61] The Eleventh Circuit agreed that the FTC had failed to connect the allegations in the complaint, as well as the remedy sought, to LabMD's actual conduct:

> The proposed cease and desist order, which is identical in all relevant respects to the order the FTC ultimately issued, identifies no specific unfair acts or practices from which LabMD must abstain and instead requires LabMD to implement and maintain a data-security program "reasonably designed" to the Commission's satisfaction.
>
> ***
>
> In the case at hand, the cease and desist order contains no prohibitions. It does not instruct LabMD to stop committing a specific act or practice. Rather, it commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness. This command is unenforceable.

11th Circuit Opinion, 894 F.3d at 1230, 1236.

[62] FTC LabMD Opinion, *supra* note 15, at 12 n. 23.

The failure to establish a baseline duty of care also means that companies may lack constitutionally required fair notice of the extent of the data security practices that might be deemed unreasonable by the FTC.[63]

The Eleventh Circuit, in fact, zeroed in on the fair notice issues at oral argument:

> **Judge Tjoflat**: Well, but the problem — the reason for rulemaking is there's no notice for any of these things in the past . . . that's why you use rulemaking . . . You're going to set prophylactic rules in the future. Nobody knows they've been violating anything. We're going to create something and you will violate . . . .
>
> **FTC Attorney**: Right. Well, I . . . agree that . . . that's one reason why . . . an agency might use prophylactic rulemaking, of course. The Supreme Court made very clear in *Bell Aerospace* and in the *Chenery* case that the agency is entitled to proceed on a case-by-case adjudication, particularly in situations like this where it's difficult to formulate *ex ante* rules. And the rule that the Commission has set forth here . . . is that companies have a duty to act reasonably under the circumstances . . . .
>
> **Judge Tjoflat**: That's about as nebulous as you can get, unless you get industry standards.[64]

This absence of fair notice resulting from the FTC's chosen procedures is crucially important as it is a cornerstone of constitutional due process:

> The fair notice doctrine requires that entities should be able to reasonably understand whether or not their behavior complies with the law. If an entity acting in good faith cannot identify with "ascertainable certainty" the standards to which an agency expects the entity to conform, the agency has not provided fair notice.[65]

The FTC's approach, by contrast, effectively operates in reverse, by inferring unreasonableness from the existence of harm, without clearly delineating a standard first. If the common law of torts had developed according to FTC practice, duty of care would be defined, in effect, as conduct that does not allow (or has not, in clearly analogous contexts, allowed) injury to occur. Not only does such an

---

[63] Gerard Stegmaier &Wendell Bartnick, *Psychics, russian roulette, and data security: The FTC's hidden data-security requirements*, 20 GEO. MASON L. REV. 673, 675-77 (2013).

[64] LabMD 11th Circuit Oral Argument, *supra* note 40, at 23-24.

[65] Stegmaier & Bartnick, *supra* note 63, at 677. Note that the fair notice doctrine has not been incorporated into any Supreme Court cases to date. Thus, this formulation comes from the D.C. Circuit's jurisprudence, and represents a relatively stronger version of the doctrine. *Id.* at 680. By contrast, some other circuits require little more than actual notice. While the Fifth Circuit "may be consistent with the D.C. Circuit," the Seventh Circuit requires that regulations are not "incomprehensibly vague." *Id.* at 15 n. 45; Tex. E. Prods. Pipeline Co. v. OSHRC, 827 F.2d 46, 50 (7th Cir. 1987). And "[t]he Second, Ninth, and Tenth Circuits have used a test that asks whether 'a reasonably prudent person, familiar with the conditions the regulations are meant to address and the objectives the regulations are meant to achieve, has fair warning of what the regulations require.'" *Id.*

approach fail to provide actors with a reliable means to determine the specific conduct to which they must adhere, it fails even to provide a discernible and operable *standard* of care.

Far from establishing what conduct constitutes "reasonable" data security *ex ante*, the FTC's approach is tantamount to imposing a strict liability regime in which "reasonableness" is largely unknowable at the time conduct is undertaken and is reliably determined only in reference to whether or not an injury-causing breach occurs *ex post*. This is in marked contrast to the negligence-like regime that Congress implemented in Section 5(n).

2. *The Difficulty of Establishing A Duty Of Care To Prevent The Acts Of Third Parties—And The FTC's Failure To Do So.*

An important peculiarity of data security cases is that many of them entail intervening conduct by third parties—in other words, information is disclosed to unauthorized outside viewers as a result of an incursion (breach) by third parties, rather than removal or exposure by employees of the company itself. There is, in fact, some question whether the FTC Act contemplates conduct that merely facilitates (or fails to prevent) harm caused by third parties, rather than conduct that causes harm to consumers directly.[66] But even if the FTC does have authority to police third-party breaches (and thus the appropriate security measures to reduce their risk),[67] the fit between such conduct and Section 5 remains uneasy.

The FTC has traditionally used its unfairness power to police coercive sales and marketing tactics, unsubstantiated advertising, and other misrepresentations to consumers. In such cases, there is a more direct line between conduct and harm.[68] In data security cases, however, the alleged unfairness is a function of a company's failure to take precautions sufficient to *prevent* a third party's intervening, harmful action (i.e., hacking).

In cases of negligence, third parties can certainly create liability when the defendant has some special relationship with the third-party—such as a parent to a child, or an employer to an employee—and thus is reasonably on notice about the behavior of *that* particular party. The law also imposes liability in certain circumstances despite the intervening behavior of totally unpredictable and uncontrollable third parties—e.g., in some strict product liability cases.

But in part because intervening conduct does frequently negate or mitigate liability, establishing duty (and, of course, causation) where a company's conduct is not the proximate cause of injury entails a different and more complex analysis than in a "direct harm" case. Yet the FTC typically pays scant

---

[66] *See generally* Michael D. Scott, *The FTC, the unfairness doctrine, and data security breach litigation: has the Commission gone too far?*, 60 ADMIN. L. REV. 127 (2008).

[67] *See, e.g.*, FTC v. Wyndham Worldwide, Inc., 799 F.3d 236, 248-49 (3d Cir. 2015).

[68] *See generally* Richard Craswell, *Identification of unfair acts and practices by the Federal Trade Commission*, 1981 WISC. L. REV 107 (1981).

attention to the nature of third-party conduct, despite its assertion that "reasonable and appropriate security is a continuous process of assessing and addressing [precisely such external] risks."[69]

In *LabMD*, for example, the breach at issue was effected by a third-party, Tiversa, employing an unusual and unusually invasive business model based upon breaching firms' networks in order to coerce them to buy its security services. Despite Tiversa's problematic behavior, the FTC did not (at least in its public presentations of its analysis) assess the particularities of Tiversa's conduct, the likelihood that a company would fall prey to it, and the likelihood of other, more-typical risks that could have arisen but been prevented by protecting against Tiversa's conduct. Assessing whether LabMD's conduct was appropriate in light of Tiversa's conduct requires, among other things, assessing how likely was Tiversa's (or similar, malicious, third-party) conduct before it occurred and the extent to which LabMD's (necessarily imperfect) protections against *other* conduct reasonably protected against Tiversa's, as well. The fact that Tiversa succeeded in obtaining PII from LabMD does not, of course, mean that LabMD's overall data security regime—nor even its P2P-specific elements—was "unfair."

While the FTC's decision does discuss more general risks of P2P file-sharing services, it fails to distinguish between the risk of inadvertent disclosure through "normal" P2P conduct and Tiversa's intentional intrusion. The decision asserts that "there was a high likelihood of harm because the sensitive personal information contained in the 1718 file was exposed to millions of online P2P users, many of whom *could* have easily found the file."[70] But even if typical P2P users "could" have found the file, this says little about the likelihood that they would do so, or, having "found" it, that they would bother to look at it. As the FTC *LabMD* opinion notes, the 1718 file was only one of 950 files on a single employee's computer being shared over LimeWire (a P2P file-sharing program), the vast majority of which were music or videos.[71] Certainly, just because Tiversa identified and accessed the file says next to nothing about the likelihood that a typical P2P user would.[72]

To be sure, the FTC was correct to discuss this risk (and other risks) that did *not* give rise to the specific alleged injury at issue in the case. And it is likewise appropriate to question security practices that could give rise to breach even if they did not (yet) do so. But the FTC cannot establish that the

---

[69] FTC LabMD Opinion, *supra* note 15, at 11.

[70] FTC LabMD Opinion, *supra* note 15, at 21 (emphasis added).

[71] *Id.* at 4.

[72] Importantly, while Tiversa used proprietary software to scour P2P networks for precisely such inadvertently shared files, typical P2P users (the "millions of online P2P users" referred to by the Commission) use(d) programs like LimeWire to search for specific files or file types (e.g., mp3s of specific songs or specific artists), rarely if ever viewing a folder's full contents. LimeWire itself (and other programs like it) segregated content by type, so that users would have to look specifically at "documents" (as opposed to "music" or "videos," e.g.) in order to see them (and even then a user would see only a file's name, not its contents). Given the prevalence of malware and viruses being shared via P2P networks, typical users were generally reluctant to access any strange files. And, although it is true that a user would not need to search for the exact filename in order to be able to see it, the file at issue in this case, named "insuranceaging_6.05.071.pdf," would not likely have aroused anyone's interest if they happened upon it—least of all typical P2P users searching for music and videos.

protections that LabMD employed to ameliorate inadvertent exposure of PII left documents unreasonably protected on the basis that non-hackers "could" have accessed them. LabMD had a policy against installation of P2P programs, and it periodically checked employees' computers, among other things. Given the actual *ex ante* risk of inadvertent P2P exposure, this may well have been sufficient. Indeed, at minimum the evidence in the case suggests that LabMD's security practices were sufficient to confine P2P file-sharing to a single computer from which very little sensitive information was taken, and from which *no* information was taken by "typical" P2P users. But we simply don't know whether LabMD's practices were sufficient to meet its reasonable duty of care because the FTC never assessed this.[73]

B. The FTC's effective disregard of causation

Section 5(n) unambiguously requires that there is some causal connection between the allegedly unfair conduct and injury.[74] While the presence of the "likely to cause" language complicates this (as we discuss at length below), causation remains a required element of a Section 5 unfairness case. In ways we have already discussed (and others we discuss below), however, the FTC seems to assume causation from the existence of an unauthorized disclosure coupled with virtually any conduct that deviates from practices that the Commission claims could have made disclosure less likely.

As we've discussed, this sort of inductive approach unaccompanied by an assessment of *ex ante* risks, costs, and benefits is insufficient to meet any reasonable interpretation of the limits placed upon the FTC by Section 5(n).

But the FTC's the problem runs deeper. In *LabMD*, instead of establishing a causal link between LabMD's conduct (i.e., its failure to adopt specific security practices) and even the breach itself (let alone the alleged harm), the Commission generates inferences based upon anecdotes. The FTC's opinion cites allegedly deficient practices,[75] but establishes no causal link between these and Tiversa's

---

[73] Interestingly, the FTC notes in its opinion that: "Complaint Counsel argues that LabMD's security practices risked exposing the sensitive information of all 750,000 consumers whose information is stored on its computer network and therefore that they create liability even apart from the LimeWire incident. We find that the exposure of sensitive medical and personal information via a peer-to-peer file-sharing application was likely to cause substantial injury and that the disclosure of sensitive medical information did cause substantial injury. Therefore, we need not address Complaint Counsel's broader argument." FTC LabMD Opinion, *supra* note 15, at 16. In theory, however, the FTC should have been able to make out a stronger case (and one that would have addressed the company's overall duty of care with respect to all *ex ante* threats against all of its stored PII) if its allegations were true and it had assessed the full extent of LabMD's practices and risks to all of its data. Presumably the reason it did not choose to do this is that it was unable to adduce any such evidence beyond the risk to the 1718 file from Tiversa. As the ALJ noted: "[Complaint Counsel's expert] fails to assess the probability or likelihood that Respondent's alleged unreasonable data security will result in a data breach and resulting harm. Mr. Van Dyke candidly admitted that he did not, and was not able to, provide any quantification of the risk of identity theft harm for the 750,000 consumers whose information is maintained on LabMD's computer networks, because he did not have evidence of any data exposure with respect to those individuals, except as to those that were listed on the 1718 File or in the Sacramento Documents." ALJ LabMD Initial Decision, *supra* note 21, at 83-84.

[74] 15 U.S.C. § 45(n) (2012).

[75] *See, e.g.*, FTC LabMD Opinion, *supra* note 15, at 2.

theft of the 1718 file—nor *could* it, at least for many of the practices it mentions, because the theft had nothing to do with, for example, password policies, operating system updates, or firewalls (all of which are mentioned in the opinion). Moreover, things like integrity monitoring and penetration testing (also mentioned) at best "'*might* have' aided detection of the application containing the P2P vulnerability[.]"[76] LabMD's alleged failure to do these things cannot be said to have caused the (alleged) harm. Even with respect to other security practices that *might* have a more logical connection to the breach (e.g., better employee training), the Commission offers no actual evidence demonstrating that failure to employ these actually caused, or even were likely to cause, any *harm*.

Whatever the standard for "unreasonableness," there must be a causal connection between the acts (or omissions) and injury. Even for "likely" harms this requires not merely *any* possibility but some high *probability* at the time the conduct was undertaken that it would cause future harm.[77] Instead, the Commission merely asserted that harm was sufficiently "likely" based on its own *ex post* assessment, in either 2012 or 2017, of the risks of P2P software in 2007—without making any concrete connections between the generalized risk and the specific circumstances at LabMD.

The FTC's Chief ALJ found this assertion manifestly wanting, ruling that the Commission had failed to establish a sufficient connection between LabMD's conduct and the data that was actually removed from the company.[78] But with respect to Complaint Counsel's assertion that, in effect, *all* data held by LabMD was at risk, the ALJ found that:

> Complaint Counsel's theory that harm is likely for all consumers whose Personal Information is maintained on LabMD's computer network, based on a "risk" of a future data breach and resulting identity theft injury, is without merit. First, the expert opinions upon which Complaint Counsel relies do not specify the degree of risk posed by Respondent's alleged unreasonable data security, or otherwise assess the probability that harm will result. To find "likely" injury on the basis of theoretical, unspecified "risk" that a data breach will occur in the future, with resulting identity theft harm, would require reliance upon a series of unsupported assumptions and conjecture. Second, a "risk" of harm is inherent in the notion of "unreasonable" conduct. To allow unfair conduct liability to be based on a mere "risk" of harm alone, without regard to the probability that such harm will occur, would effectively allow unfair conduct liability to be imposed upon proof of unreasonable data security alone. Such a holding would render the requirement of "likely" harm in Section 5(n) superfluous, and would contravene the clear intent of Section 5(n) to limit unfair conduct liability to cases of actual, or "likely," consumer harm.[79]

---

[76] *Id.* at 31, 4 n.13 (emphasis added).

[77] *See* ALJ LabMD Initial Decision, *supra* note 21, at 54.

[78] *Id.* at 53.

[79] ALJ LabMD Initial Decision, *supra* note 21, at 81.

But the Commission, in its turn, disagreed: "The ALJ's reasoning comes perilously close to reading the term 'likely' out of the statute. When evaluating a practice, we judge the likelihood that the practice will cause harm at the time the practice occurred, not on the basis of actual future outcomes."[80]

This is true, as far as it goes, and, as we have noted above, a proper reasonableness assessment would address expected risk, cost, and benefit of all harms and security practices, including those that don't factor into the specific circumstances at issue in the case. But even such an undertaking requires some specificity regarding expected risks and some proof of a likely causal link between conduct and injury.

More importantly, judgments about the likelihood that past conduct would cause harm must be informed by what has actually occurred. By the time the FTC filed its complaint, and surely by the time the FTC rendered its opinion, facts about what *actually* happened over the course of LabMD's existence should have informed the Commission about what was *likely* to occur.

Although the ALJ's Initial Determination focused heavily on the FTC's lack of evidence of actual harm, the judge went to great lengths to explain why this lack of harm is *also* relevant when evaluating "likely" harms:

> Complaint Counsel presented no evidence of any consumer that has suffered NAF, ECF, ENCF, medical identity theft, reputational injury, embarrassment, or any of the other injuries . . . . Complaint Counsel's response—that consumers may not discover that they have been victims of identity theft, or even investigate whether they have been so harmed, even if consumers receive written notification of a possible breach, as LabMD provided in connection with the exposure of the Sacramento Documents—does not explain why Complaint Counsel's investigation would not have identified even one consumer that suffered any harm as a result of Respondent's alleged unreasonable data security. Complaint Counsel's response to the absence of evidence of actual harm in this case, that it is not legally necessary under Section 5(n) to prove that actual harm has resulted from alleged unfair conduct, because "likely" harm is sufficient . . . fails to acknowledge the difference between the burden of production and the burden of persuasion. The express language of Section 5(n) plainly allows liability for unfair conduct to be based on conduct that has either already caused harm, or which is "likely" to do so. However . . . the absence of any evidence that any consumer has suffered harm as a result of Respondent's alleged unreasonable data security, even after the passage of many years, undermines the persuasiveness of Complaint Counsel's claim that such harm is nevertheless "likely" to occur. That is particularly true here, where the claim is predicated on expert opinion that essentially only theorizes how consumer harm could occur. Given

[80] FTC LabMD Opinion, *supra* note 15, at 23.

> that the government has the burden of persuasion, the reason for the government's failure to support its claim of likely consumer harm with any evidence of actual consumer harm is unclear.[81]

Moreover, the ALJ pointed out how reviewing courts are hesitant to allow purely speculative harms to support Section 5 actions:

> In light of the inherently speculative nature of predicting "likely" harm, it is unsurprising that, historically, liability for unfair conduct has been imposed only upon proof of actual consumer harm. Indeed, the parties do not cite, and research does not reveal, any case where unfair conduct liability has been imposed without proof of actual harm, on the basis of predicted "likely" harm alone. . . . In Southwest Sunsites v. FTC, 785 F.2d 1431, 1436 (9th Cir. 1986), the court interpreted the Commission's deception standard, which required proof that a practice is "likely to mislead" consumers, to require proof that such deception was "probable, not possible . . . ." Based on the foregoing, "likely" does not mean that something is merely possible. Instead, "likely" means that it is probable that something will occur. . . . Moreover, although some courts have cited the "significant risk" language from the Policy Statement, the parties have not cited, and research does not reveal, any case in which unfair conduct liability has been imposed without proof of actual, completed harm, based instead upon a finding of "significant risk" of harm.[82]

That the only available facts point to the complete *absence* of any injury suggests at the very least that injury was perhaps not "likely" caused by any of LabMD's conduct. It is thus the Commission that is in danger of reading "likely" out of the statute and replacing it with something like "could conceivably have contributed to any increase in the chance" of injury. It simply cannot be the case that Congress added the "likely to cause" language so that the Commission might avoid having to demonstrate a causal link between conduct and injury—even "likely" injury.

Moreover, if the FTC's "likely" authority is to have any meaningful limit, it must be understood *prospectively*, from the point at which the FTC issues its complaint. Thus, if an investigative target has *ceased* practices that the Commission claims "likely" to cause harm by the time a complaint is issued, the claim is logically false and, in effect, impossible to remedy: Section 5 is not punitive and the FTC has no authority to extract damages, but may only issue prospective injunctions. In other words, because Section 5 is intended to *prevent* (not punish) unfair practices that harm consumers, if a potential investigative target has *already ceased* the potentially unfair practices, the deterrent effect of Section 5 may be deemed to have been achieved by the omnipresent threat of FTC investigation. This is, in fact, the statute working properly. By contrast, the Commission's reading of its "likely to cause" authority—which would allow it to scan a company's *past* behaviors, regardless of when its complaint was issued, and force them through expensive investigations and settlements—would in effect grant it punitive powers.

---

[81] ALJ LabMD Initial Decision, *supra* note 21, at 52-53.

[82] *Id.* at 53-55.

The Commission's 2013 *HTC* complaint and settlement exemplifies its willingness to infer causation under the "likely to cause" language of Section 5(n) from the barest of theoretical risks and without connecting it in any concrete way to injury.

In *HTC*, HTC America had customized its Android mobile phones in order to include software and features that would differentiate them from competing devices.[83] In doing so, however, HTC had, in the FTC's opinion, "engaged in a number of practices that, taken together, failed to employ reasonable and appropriate security in the design and customization of the software on its mobile devices."[84] The end result was that HTC's engineers had created security flaws that *theoretically* could be used to compromise user data.[85]

There were not, however, *any* known incidents of data breach arising from consumers' use of the approximately ten to twelve million devices at issue.[86] Nonetheless, HTC's practice was still found to be "likely" to injure consumers despite the *practical* unlikeliness of finding zero flaws in a sample of ten million.[87] In the Commission's view:

> [M]alware placed on consumers' devices without their permission could be used to record and transmit information entered into or stored on the device . . . . Sensitive information exposed on the devices could be used, for example, to target spear-phishing campaigns, physically track or stalk individuals, and perpetrate fraud, resulting in costly bills to the consumer. Misuse of sensitive device functionality such as the device's audio recording feature would allow hackers to capture private details of an individual's life.[88]

Interestingly, not only does the FTC in *HTC* infer causation from a deviation from its idealized set of security protocols despite the absence of any evidence of breach, in doing so it also necessarily incorporates its own inferences about the magnitude of the risk of third-party conduct. It incorporates these inferences regardless of whether HTC's assumptions regarding the likelihood of third-party intervention were lower, and without (publicly, at least) assessing whether those assumptions were reasonable. At minimum, there is absolutely no way to infer from the FTC's guidance or previous consent orders what an appropriate estimate would be; again, the FTC fails to establish a baseline duty of care. Instead, it appears that the FTC believes that any risk of third-party intervention would be sufficient to merit protective security measures.

---

[83] HTC Am. Inc., 155 F.T.C. 1617, 2 (2013) [hereinafter HTC Complaint].

[84] *Id.* at 2.

[85] *Id.* at 2-6.

[86] Alden Abbot, *The Federal Trade Commission's role in online security: data protector or dictator?*, HERITAGE FOUND. (Sept. 10, 2014), http://www.heritage.org/report/the-federal-trade-commissions-role-online-security-data-protector-or-dictator.

[87] HTC Complaint *supra* note 83, at 6.

[88] *Id.*

But there is not a network-connected device in the world about which it could not be said that there is *some* risk of breach. Even the National Security Agency—America's top spy shop and, presumably, among the very least likely to be hacked by an outside party—was subject to a third-party data breach that resulted in the release of a large amount of confidential information.[89]

HTC also represented a fundamental shift in the Commission's approach. In that case it moved rather dramatically from policing fraud and deception to interjecting itself into the engineering process. HTC America was not accused of purposely creating loopholes that could be used to harm consumers: it was, in essence, found to be negligent in how it designed its software.[90]

C. The FTC's unreasonable approach to harm

There is a close connection between the problems with the FTC's approach to causation and its approach to injury, especially with respect to conduct that is deemed "likely to cause" injury (this is discussed in more detail in the following section).

1. Breach Is Not (Or Should Not Be) The Same Thing As Harm

One of the core deficiencies of *LabMD* is the assertion that breach alone can constitute harm. Flowing from this error is the assertion that conduct giving rise to the *possibility* of breach, even without an actual breach, can be deemed "likely to cause" harm.

Of course, as we have noted, the Commission's explicit statements hold that a mere breach alone is *not* harm.[91] And for most of its history, the Commission's decisions have also suggested that a breach alone cannot constitute a harm. Two watershed cases in the evolution of the Commission's data security enforcement practices help to illustrate this.

First, in 2002, the FTC entered into a consent order with Eli Lilly, holding the company responsible under Section 5 for deceptive conduct, based on its disclosure of the names of 669 patients who were taking Prozac to treat depression (in contravention of its stated policy).[92] That they were users of Prozac was apparent from the context of the disclosure, and, today at least, it is readily apparent why the disclosure itself (as opposed to any subsequent action taken as a consequence of the disclosure) might constitute actionable harm.

Although brought as a deception case, the conduct at issue was "respondent's failure to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer

---

[89] *See, e.g.*, Matt Burgess, *Hacking the hackers: everything you need to know about Shadow Brokers' attack on the NSA*, WIRED, Apr. 18, 2017, http://www.wired.co.uk/article/nsa-hacking-tools-stolen-hackers.

[90] HTC Complaint, *supra* note 83, at 2.

[91] *See, e.g.*, COMMISSION STATEMENT, *supra* note 36, at 1. ("The mere fact that a breach occurred does not mean that a company has violated the law.").

[92] Eli Lilly & Co., 133 F.T.C. 763, 766-767 (May 8, 2002).

information."[93] The case, commonly considered to be the FTC's first data security case, marked something of an evolution in the FTC's view of what constituted harm under Section 5's Unfair or Deceptive Acts or Practices language by finding purely *non-monetary* harm—the public disclosure of information in a potentially compromising and unambiguous context—to be material.[94]

The underlying theory of materiality or harm in *Eli Lilly*—while not explicated by the FTC, even in the accompanying Analysis of Proposed Consent Order to Aid Public Comment[95]—never mentions the word materiality. It also never seeks to defend its implicit assertion of either materiality or "detriment," nor does it even acknowledge the novelty of the theory of harm involved (although the theory is arguably recognizable, with origins in Warren & Brandeis' *The Right to Privacy* and common law concepts like the tort of intrusion upon seclusion).[96] But it seems clear that mere exposure of just *any* information alone would not be sufficient to cause harm (or establish materiality); rather, harm would depend on the context, and only embarrassing or otherwise reputation-damaging disclosures caused by certain people viewing certain information would suffice.

Second, in 2005, the Commission entered into a consent order with BJ's Wholesale Club, in its first unfairness-based data security case.[97] The FTC in *BJ's Wholesale Club* tried to identify concrete harms arising from the breach at issue:

> [F]raudulent purchases . . . were made using counterfeit copies of credit and debit cards the banks had issued to customers . . . [P]ersonal information . . . stored on respondent's computer networks . . . was contained on counterfeit copies of cards that were used to make several million dollars in fraudulent purchases. In response, banks and their customers cancelled and re-issued thousands of credit and debit cards that had been used at respondent's stores, and customers holding these cards were unable to use their cards to access credit and their own bank accounts.[98]

Problematic though both of these examples may be (and they are), they have one thing in common: *harm* (or materiality) is something different than *breach*; rather, it is a *consequence* of a breach. It need

---

[93] *Id.*

[94] *See* FED. TRADE COMM'N, POLICY STATEMENT ON DECEPTION (1983) [hereinafter DECEPTION POLICY STATEMENT], https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception. While "harm" is not a required showing in a deception case, materiality is meant to be a *proxy* for harm in the context of deception cases. The FTC's Deception Policy Statement, itself a compromise between then-Chairman Miller's preference for an explicit finding of harm and the *Colgate-Palmolive* Court's holding that deception required nothing more than a misleading statement, explicitly joins the two concepts together when it explains that "the Commission will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, *to the consumer's detriment*." *Id.* at 2 (emphasis added).

[95] Federal Trade Commission, File No. 012 3214, Eli Lilly and Co.; Analysis to Aid Public Comment, 67 Fed. Reg. 4693 (Feb. 1, 2002).

[96] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195-97 (1890). *See also* Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 206-07 (2012).

[97] BJs Wholesale Club, Inc., 2005 WL 1541551 (F.T.C June 16, 2005), at *2.

[98] *Id.*

not be monetary, and it need not be well defined (which is bad enough). But there is a clearly contemplated sequence of events that gives rise to potential liability in a data security case:

1. A company collects sensitive data;

2. It purports to engage in conduct to keep that data secret, either in an explicit statement or by an implicit guarantee to use "reasonable" measures to protect it;

3. The information is nevertheless disclosed (i.e., there is a security breach) because of conduct by the company that enables the disclosure/breach; and

4. The context or content of the disclosure significantly harms (or is used to harm) consumers, or is likely to lead to significant harm to the consumer.

The last element (significant harm/materiality) and its separation from the third element (breach) is key. As Commissioner Swindle noted in 1999 in his dissent from the Commission's complaint in *Touch Tone*: "[W]e have never held that the mere disclosure of financial information, without allegations of ensuing economic or other harm, constitutes substantial injury under the statute."[99]

But by 2012, in its Privacy Report, the Commission asserted that disclosure itself of private information could give rise to harm (or, presumably, materiality), *regardless* of any other consequences arising from a breach. The harm and the breach became the same thing:

> These harms may include the unexpected revelation of previously private information, including both sensitive information (e.g., health information, precise geolocation information) and less sensitive information (e.g., purchase history, employment history) to unauthorized third parties . . . . [A] privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions.[100]

This connection between "unexpected revelation" and harm is not obvious, and certainly should be demonstrated by empirical evidence before the FTC proceeds on such a theory. Yet, without any such evidence, the FTC in *LabMD* brought this theory to fruition.

As it admitted, the Commission "does not know,"[101] whether any patient encountered a single problem related to the breach, and thus never articulated any actual injury caused by LabMD's conduct.[102]

---

[99] Touch Tone, 1999 WL 233879 (F.T.C Apr. 22, 1999), at *3 (Orson Swindle, Comm'r, dissenting).

[100] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS 8 (2012) [hereinafter FTC PRIVACY REPORT], https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[101] FTC LabMD Opinion, *supra* note 15, at 14.

[102] And although the Commission effectively blames LabMD for its (the FTC's) lack of knowledge of harm, that burden does not rest with LabMD. Moreover, the Commission had ample opportunity to collect such evidence if it existed, e.g., by

The Commission instead asserted that mere exposure of information suffices to establish harm.[103] But this amounts to saying that any conduct that causes breach causes harm. That not only violates the FTC's own claims that breach alone is not enough, it is insufficient to meet the substantial injury requirement of Section 5(n). The examples the Commission has adduced to support this point all entail not merely exposure, but actual dissemination of personal information to large numbers of unauthorized recipients who *actually read* the exposed data.[104] Even if it is reasonable to assert in such circumstances that "embarrassment or other negative outcomes, including reputational harm" result from that sort of public disclosure,[105] no such disclosure occurred in *LabMD*. That the third-party responsible for exposure of data itself viewed the data—which is effectively all that happened in that case—cannot be the basis for injury without simply transforming the breach itself into the injury.

2. *Purely informational harms present further difficulties*

Complicating any analysis of harm in the data security context is the fact that many (if not most) of the alleged harms are what the Commission has termed "informational injuries."[106] Such harms are "injuries . . . that consumers may suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data"[107] and which typically extend beyond the easily quantifiable economic harms such as unauthorized use of credit cards.

At the root of any concept of informational injury is the assertion that the unauthorized exposure of private information may be, in and of itself, a harm to individuals, apart from any concrete economic consequences that may result from the exposure. In the FTC's opinion *in LabMD*, for instance, the Commission asserted that:

> [T]he disclosure of sensitive health or medical information causes additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n).... [D]isclosure of the mere fact that medical tests were

actually asking at least a sample of patients whose data was in the 1718 file or subpoenaing insurance companies to investigate possible fraud. That the Commission still cannot produce any evidence suggests strongly that none exists.

[103] *See* FTC LabMD Opinion, *supra* note 15, at 15 ("Indeed, the Commission has long recognized that the unauthorized release of sensitive medical information harms consumers"). True, it limits this to "sensitive medical information," but disclosure of any number of types of "sensitive" medical information, especially if limited to a vanishingly small number of viewers, may not cause distress or other harm.

[104] *See generally* MTS, Inc., 137 F.T.C. 444 (2004), https://www.ftc.gov/enforcement/cases-proceedings/032-3209/mts-inc-et-al-matter (providing that Tower Records was liable for software error that allowed 5,225 consumers' billing information to be read by anyone, which actually occurred).

[105] FTC LabMD Opinion, *supra* note 15, at 15.

[106] *See, e.g.*, FTC, FTC INFORMATIONAL INJURY WORKSHOP (2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

[107] *Id.*

> performed irreparably breached consumers' privacy, which can involve "embarrassment or other negative outcomes, including reputational harm."[108]

Defining and evaluating these types of information harms, however, is impossible until many of the fundamental flaws in the Commission's approach to Section 5 are resolved.

The task of defining "informational" injury is fraught in a way that traditional analysis of harm is not. Traditional harms are analyzed against largely objective criteria such as monetary value, physical damage, and the like; their very nature allows for a more or less satisfactory definition of the harm involved. Although it is certainly possible that the incidence and magnitude of physical harms can be ambiguous — among other things, deception and time can make these assessments more difficult — fundamentally, and certainly relative to intangible injury, determining both is fairly (although far from perfectly) straightforward. So, too, by and large, is the framework for assessing causality and liability readily understood. Moreover, these objectively observable harms exist largely without reference to context: It does not depend on whether you are a CEO or a cashier in determining whether money was lost; it is irrelevant whether one is male or female in determining whether one's car was struck and whiplash was suffered.

Informational injuries, by contrast, are based substantially on *subjective* effects, and are often heavily dependent upon the context in which they were incurred — context that invariably changes over time and place. Whether one feels shame, anxiety, embarrassment, or other "psychic" effects from the unauthorized disclosure of personal information depends, in many instances, on the prevailing social conventions and mores surrounding the disclosed information and its recipients.

In *Eli Lilly*, for instance, the Commission asserted that the (somewhat) broad disclosure of the fact that someone was taking an antidepressant in 1999 could lead to harm (*e.g.*, shame) even absent other, concrete effects.[109] That may well have been true in 1999.

The difficulty is that, even in 1999, there would have been at least *some* people who would not feel such shame, yet the Commission seems to have assumed that all affected individuals did so. Absent objective criteria to assess such psychic effect, however, the fact of it occurring as a result of the disclosure cannot simply be assumed. Moreover, the *extent* of harm, even to people who did indeed experience it, would vary widely and be difficult, if not impossible, to measure. Although the Commission does not assess damages for such injuries, determination of the magnitude of harm is still crucial for assessing both whether victims suffered net harm, and whether a Commission action would satisfy the cost-benefit test of Section 5(n).

To make things more complicated, whatever the incidence and magnitude of the effects in 1999, there is no reason to think they would be the same 19 (or 29, or 39) years later. Today, although

---

[108] FTC *LabMD* Opinion, *supra* note 15, at 17.

[109] Eli Lilly & Co., 133 F.T.C. 763 (May 8, 2002).

some would surely feel shame at certain other people knowing that they take an antidepressant, the vast popularity of pharmacological treatment for emotional problems means that shame is surely both less likely and less significant (although, at the same time, that same popularity surely means that the aggregate magnitude of harm could actually be greater than in 1999).[110]

And not all informational injuries are the same. Some injuries are psychic in nature — shame or embarrassment, for example. Others uneasily mix what the FTC typically analyzes as "likely" injuries — inchoate harms such as the exposure of sensitive information that *could* be used to steal an identity, access a bank account, or otherwise lead to more concrete harms — with the psychic consequences of bearing that risk. A purely psychic harm like anxiety arising from exposure of information that could lead to identify theft is, from another point of view, a "likely" harm, with the actual, concrete harm being the financial loss. Thus the anxiety harm merges with the likely harm of financial loss, and evaluating the magnitude of such a harm would require evaluating both the objective likelihood of the loss, as well as each individual's subjective assessment of that risk. None of these is a straightforward measurement and, to our knowledge, the FTC has never undertaken such a measurement.

Social Context

Indeed, a major impediment to properly basing data security cases on the psychic flavor of informational injury is the difficulty of establishing a rigorous method (e.g., representative and comprehensive consumer surveys) of determining the baseline expectations that members of society have surrounding the protection of their personal information. And this method, moreover, will need to be regularly updated to ensure that the standards of, say, two years ago do not govern the changed notions of "today."[111]

There are a number of critical components that would have to factor into establishing this baseline, none of them yet identified comprehensively by the Commission. Among many other things, these will necessarily include, e.g.: to whom the information is disclosed; the nature of consumer expectations regarding the release or use of the information; whether the information is itself somehow harmful or could lead to a real concrete harm (like a bank account number or social security number); consumers' perception of the risk of harm; and, if the information could lead to a more concrete harm, the nature of that harm.

The necessary aim of attempting to establish such a baseline is to bring an administrable order to the chaos of subjectivity (if possible). The incidence and magnitude of these subjective effects will undoubtedly change rapidly as technology and society evolve, but a careful periodic analysis might

---

[110] Today, in fact, many people are not only unashamed at taking antidepressants, they are quite open about it. Some even write publicly about how antidepressant use has improved their lives. *See, e.g.,* Kimberly Zapata, *This is why taking antidepressants makes me a better mother*, WORLD OF PSYCHOLOGY, Feb. 13, 2016, *available at* https://psychcentral.com/blog/archives/2016/02/13/this-is-why-taking-antidepressants-makes-me-a-better-mother/. For these people it would, surely, be difficult to infer harm from additional, even unauthorized, disclosure.

[111] The FTC has some experience in establishing guidance like this. See, for example, the Green Guides, *available at* https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-issues-revised-green-guides/greenguides.pdf.

be able to reveal which subjective harms rise to the level of common social acceptance. But such an a regular analysis and public guidance on its results would be required because, without carefully crafted and constantly calibrated standard, subjective harms as the basis for regulatory or legal actions could quickly result in a race to the bottom where those relative few who are most sensitive to informational injuries dictate policy to the detriment of overall social welfare. Under Section 5's cost-benefit standard, in some cases this cost, coupled with the uncertainty of the underlying alleged harm, will mean the FTC must refrain from bringing an enforcement action.

Calculating Benefits

Further complicating matters, in the informational context, because often the same conduct that may lead to psychic harm may also confer *concrete* benefits, and because the effects of the conduct on each individual are subjective and variable, determining if conduct results in cognizable injury must entail a careful assessment of the benefits of the conduct to each individual, as well, in order to determine if the *net* effect is negative. In other words, even if, in the abstract, unanticipated disclosure of private information to, say, an advertiser might impose psychic costs on some consumers, it also confers actual benefits on some of them by enabling better targeted ads. Determining if there is injury on net requires assessing *both* of these effects.

Importantly, this is different than the cost-benefit assessment required by Section 5(n), which demands a weighing of costs and benefits not only for the potentially injured parties, but also a weighing of those net costs against the overall benefits of the conduct in question, where those benefits are enjoyed by consumers who do not also experience the costs. Here, instead, the costs and benefits may, in fact, be realized by the very same consumers.

Many of these informational harms may be bound up in the nature of the relevant industry itself. Even though there may exist an unexpected use that some individuals feel harms them, there may also exist a larger justification for the practice in overall increased social welfare. The benefit of having, for instance, certain valuable attributes of a platform like Gmail, Facebook, or Snapchat necessarily must be factored into the cost-benefit calculation. This is not to say that *any* unexpected use of data should be beyond reach, but that the benefit of the existence and optimal operation of the system, firm, or other analytically relevant entity must be taken into account.

Revealed Preferences

Important in evaluating informational injuries is the fact that, for at least some classes of injury, consumers themselves self-evidently engaged in the services that subsequently caused the injury. With the growing frequency of data compromises, it certainly must be a factor of any informational injury analysis that consumers, knowing that there was some chance that their information could be exposed, chose to engage with those services anyway. Thus, the cost to themselves in informational injury terms was to some extent "priced" into the cost of accessing services in exchange for their personal information.

This is important particularly from the perspective of Section 5(n), as its balancing test requires that harms incurred were not "reasonably avoidable" by consumers. Where users a) voluntarily choose to give their data to a service, b) with sufficiently accurate knowledge of the risk of harm, and c) where there are reasonable substitutes (including not engaging at all), it may, in fact, be reasonable to view their specific choice as prima facie evidence of reasonable avoidability in the event of unauthorized disclosure of their data.

And, critically, at least with tech platforms and apps, it is important to recognize that the reason these services become important is *because* so many users choose to adopt them. Sometimes there may not be an obvious alternative: In *LabMD*, for example, it is doubtful that consumers were either informed about or directly choosing among diagnostics laboratories. But for many services competitors are available, and meaningful consumer choice is viable: It is trivially easy to choose a fully-encrypted and secure email service instead of Gmail, or to opt for DuckDuckGo instead of Google Search. Consumers, however, opt for what they perceive as more accurate or convenient because *they value that over privacy to some significant extent*. In such circumstances it would be a mistake to deem generally customary practices unfair, even if consumers appear to be harmed *ex post*.

3. The Mere Storage of Sensitive Data Can Constitute Conduct "likely to cause" Harm

A crucial and troubling implication of the Commission's position—compounded by its willingness to infer "psychic" harm from the mere risk of disclosure—is that it effectively permits the FTC to read Section 5 as authorizing an enforcement action against any company that merely *stores* sensitive data, virtually *regardless* of its security practices or even the existence of a breach:

1. The standard adopted by the FTC permits it to infer injury from any unanticipated or unauthorized disclosure (regardless of concrete harm).

2. It makes this inference not necessarily because of the intervention of a third-party, but merely because data is exposed to anyone unauthorized to view it; third-party breach may often be the proximate cause of exposure, but it is unauthorized exposure per se that gives rise to injury, not the fact of a third-party's incursion.

3. This means that information leaving the company in *any* unauthorized manner would be sufficient to demonstrate harm.

4. As noted, the FTC has established a standard by which it may infer that conduct is *likely* to cause injury virtually regardless of the extent of increased risk of exposure attributable to the conduct: *any* increased risk may suffice.

5. Relative to not collecting data at all, or to collecting some lesser amount of data deemed "reasonable" by the FTC, any amount of data collection necessarily increases the risk of its exposure.

6. Thus merely a *potential* of data leaving the company (again, *ex ante* in any unauthorized manner, and not dependent upon a third-party) could amount to *likely* harm.

7. Because that potential *always* exists even with the most robust of security practices, the only thing limiting the Commission's authority to bring an enforcement action against *any* company that collects PII is prosecutorial discretion.

To be sure, the Commission is unlikely to bring a case absent *some* unauthorized disclosure of sensitive data. But the FTC's interpretation of its authority effectively removes any identifiable limits on its discretion to bring a data security action under Section 5.

In order to properly infer unreasonable security (even from evidence as "strong" as a single instance of unexpected exposure as with the 1718 file, let alone the absence of evidence of any exposure as with the rest of LabMD's data), the Commission should demonstrate that such exposure always or almost always occurs *only* when security is unreasonably insufficient. Although there may be specific circumstances in which this is the case, it manifestly is not the case in general. If every breach allows the FTC to infer unreasonableness without showing anything more, it can mean only one of two things: 1) that either the collection or storage of that data was so unambiguously perilous and costly in the first place that a strict liability standard is appropriate as a matter of deterrence; or else 2) that breach always or nearly always correlates with unreasonable security practices and the inference is warranted. Because we know the latter to be untrue, the FTC's theory of causation and harm places it in the unreasonable position of implicitly asserting that the data collection and retention practices crucial to the modern economy are inherently "unfair."

4. The FTC's Reading of "Likely To Cause" Gives it Unfettered Discretion Not Contemplated by Section 5

In its *LabMD* decision the Commission attempts to mitigate this position to a degree, demurring on the ALJ's holding regarding the inadequacy of Complaint Counsel's assertion that LabMD's security practices were likely to cause harm related to LabMD data *not* found in the 1718 file. But this is a small and insufficient concession.

The Commission reads a sort of "cyber Hand Formula" into the language of Section 5, sufficient to permit it to find liability for conduct that it deems in *any way* increases the chance of injury, even absent an actual breach or any other affirmative indication of "unreasonable" risk, provided the magnitude of potential harm is "significant" (which is, itself, almost entirely within the Commission's discretion to so label):

> Unlike the ALJ, we agree with Complaint Counsel that showing a "significant risk" of injury satisfies the "likely to cause" standard. In arriving at his interpretation of Section 5(n), the ALJ found that Congress had implicitly "considered, but rejected," text in the Unfairness Statement stating that an injury "may be sufficiently substantial" if it "raises a significant risk of concrete harm." . . . Yet the legislative history of Section 5(n) contains no evidence that Congress intended to disavow or reject this statement in the Unfairness Statement. Rather, it makes clear that in enacting Section 5(n) Congress specifically approved of the substantial injury discussion in the Unfairness Statement and existing case law applying the Commission's unfairness authority. . . . We conclude that the more

> reasonable interpretation of Section 5(n) is that Congress intended to incorporate the concept of risk when it authorized the Commission to pursue practices "likely to cause substantial injury."[112]

Thus, the Commission concludes: "In other words, contrary to the ALJ's holding that 'likely to cause' necessarily means that the injury was 'probable,' a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low."[113]

When establishing causality, however, Section 5(n) is not focused on the magnitude of the injury itself. Instead, the *likelihood* of injury and the *substantiality* of the injury are distinct concepts. Conduct does not become more *likely* to cause injury in the first place just because it might make whatever injury results more *substantial*.

This is clear from the statute: "substantial" modifies "injury," not "likely." Either conduct *causes* substantial injury, or it is *likely* to cause substantial injury, meaning it creates a sufficiently heightened risk of substantial injury. In each case the "substantial injury" is *literally* the same. The statute does not use a separate phrase to describe the range of harm relevant to conduct that "causes" harm and that relevant to conduct that is "likely to cause" harm; it uses the phrase only once. To reimport the risk component into the word "substantial" following the word "likely" makes no syntactic sense: "likely to cause" already encompasses the class of injuries comprising increased risk of harm. The only viable reading of this language is that conduct is actionable only when it both *likely* causes injury and when that injury is *substantial*.

Although the Unfairness Statement does note in footnote 12 that "[a]n injury may be sufficiently substantial . . . *if it raises a significant risk of concrete harm*,"[114] "raises" clearly does not mean "increases the degree of" here, but rather "stirs up" or "gives rise to."[115] If it meant the former it would refer to injury that "raises the risk of harm" or that "raises the significance of the risk of harm." Additionally, the relevant risk in footnote 12 is deemed to be "significant," not "substantial," suggesting it was intended to be of a different character. Moreover, that passage conveys the Commission's direction to address inchoate harms under Section 5—conduct "likely" to cause harm. As such, footnote 12 was incorporated into Section 5(n) by inserting the words "or is likely to cause" in the phrase "causes . . . substantial harm." Importing it *again* into the determination of substantiality is a patently unreasonable reading of the statute and risks writing the substantial injury requirement out of the statute.

At first blush, the FTC's proposed multiplication function may sound like the first half of footnote 12, but these are two very different things. Indeed, the fact that the footnote proposes a multiplication function for interpersonal aggregation of harms, but then, in the next breath, says no such thing about multiplying small risks times large harms, can have only one meaning: the Policy Statement

---

[112] *Id.* at 21.

[113] *Id.*

[114] *Id.* (quoting Unfairness Statement, at 1073 n.12) (emphasis added).

[115] *Raise*, MERRIAM-WEBSTER DICTIONARY (New Ed., 2016).

requires the FTC to prove the substantiality of harm, independent of its risk. Had Congress intended for the rather straightforward strictures of 5(n) to accommodate the large loophole proposed by the FTC, it surely would have spoken affirmatively. It did not. Instead, as is evident from the plain text of the statute, Congress structured Section 5(n) as a meaningful limitation on the FTC's potentially boundless unfairness authority.

The Commission claims that "[t]he Third Circuit interpreted Section 5(n) in a similar way in *Wyndham*."[116] It explains that defendants may be liable for practices that are likely to cause substantial injury if the harm was 'foreseeable,' . . . focusing on both the 'probability and expected size' of consumer harm."[117] But the *Wyndham* court did *not* declare that the first prong of Section 5(n) requires that the magnitude of harm be multiplied by the probability of harm when evaluating its foreseeability. Instead, the court included the magnitude of harm as one consideration in the *full* cost-benefit analysis implied by the *entirety* of Section 5(n):

> [T]his standard informs parties that the relevant inquiry here is a cost-benefit analysis . . . that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity.[118]

This is not the same as the Commission's proffered approach. The Third Circuit essentially recited the elements of a complete evaluation of Section 5(n), *not* the requirements for evaluating the first prong of the test.

Consequently, under the Commission's view of Section 5, the FTC has the power to punish entities that *have never had a breach*, since the mere *possibility* of a breach is a "likely" harm to consumers, provided the harm is substantial enough—and it invariably is. As the Commission believes:

> Finally, given that we have found that the very disclosure of sensitive health or medical information to unauthorized individuals *is itself a privacy harm*, LabMD's sharing of the 1718 file on LimeWire for 11 months *was also highly likely to cause* ***substantial*** *privacy harm* to thousands of consumers, in addition to the harm actually caused by the known disclosure.[119]

The position that the Commission upholds in the *LabMD* opinion was plainly put forward by Complaint Counsel in its oral arguments before the ALJ—and rejected by him: merely storing sensitive data and "plac[ing data] at risk"—*any risk*—are all that is required to meet the standard of unfairness

---

[116] FTC LabMD Opinion, *supra* note 15, at 21 (internal citations omitted).

[117] *Id.* (internal citations omitted).

[118] FTC v. Wyndham Worldwide, Inc., 799 F.3d 236, 255 (internal citations omitted).

[119] FTC LabMD Opinion, *supra* note 15, at 25 (emphasis added).

under Section 5.[120] Consider the following exchange between ALJ Chappell and Complaint Counsel:

> **Judge Chappell**: So again, mere failure to protect, is that a breach of or is that a violation of section 5?
>
> **Complaint Counsel**: A failure to protect, Your Honor, that places at risk consumer data—and by "consumer data" of course I don't just mean any data but the most sensitive kinds of consumer data, Social Security numbers, dates of birth, health insurance information and laboratory test codes—that increases the risk that that information will be exposed."[121]

Under this interpretation merely collecting data "increases the risk that information will be exposed" beyond the risk if data is not collected; storing it for n+1 days increases the risk beyond storing it for n days, and so on.

5. The Absence of Any Real Substantiality Of Harm Requirement (Whether It Is "Likely" Or Not)

Of course, according to the Commission's interpretation of Section 5, the magnitude of the threatened injury must be "substantial." As noted, however, the Commission's logic implies that breach alone, even absent specific injury to consumers, monetary or otherwise, can constitute injury—and, in circular fashion, a heightened *risk* of breach (from merely collecting data) can constitute likely injury. Even more troublingly, such a risk can itself constitute a *psychic* harm.

Although we cannot be sure from the available record *how large* a data collection practice is sufficient to be deemed "substantial," there is some evidence in the consent decrees suggesting that it's not very much. On the one hand, some consent decrees don't even identify how much data is at issue—suggesting either that the FTC did not know or did not care. On the other, some of the cases clearly (or explicitly) involve small amounts of data.[122]

But the FTC Act does not explicitly grant the FTC authority to pursue "trivial or merely speculative" harms (regardless of how likely they are to arise).[123] And in a 1982 letter to Senators Packwood and Kasten, FTC Chairman Miller further defined the Commission's approach to unfairness as "concern[ed] . . . with substantial injuries[,]" noting that the Commission's "resources should not be used

---

[120] *See* LabMD, ALJ Oral Argument, at https://laweconcenter.org/wp-content/uploads/2018/10/Lab-MD-Admin-Judge-Closing-Args.pdf.

[121] *Id.* (emphasis added).

[122] Geoffrey A. Manne & Ben Sperry, The Law and Economics of Data and Privacy in Antitrust Analysis, 2014 TPRC Conference Paper at 22, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418779

[123] Unfairness Policy Statement, *supra* note 26, at 1073 (Similarly, the Unfairness Statement notes that "[u]njustified consumer injury is the primary focus of the FTC Act" and such injury cannot be "trivial or merely speculative.").

for trivial or speculative harm."[124] Congress has similarly recognized the need for some meaningful limitation on the requirements of what counts as a likely harm: "In accordance with the FTC's December 17, 1980, letter, substantial injury is not intended to encompass merely trivial or speculative harm . . . . Emotional impact and more subjective types of harm alone are not intended to make an injury unfair."[125]

Commissioner Swindle did recognize in his *Touch-Tone* dissent some "subjective" contexts in which the disclosure of sensitive data could be a harm, even without tangible financial injury.[126] For instance, he noted that in other contexts the Commission had identified a "substantial injury stemming from the unauthorized release of children's personally identifiable information as being the risk of injury to or exploitation of those children by pedophiles."[127] Thus, while Section 5 unfairness authority isn't limited to cases where there is only tangible harm, at least some minimal level of analysis is required in order to connect challenged conduct with alleged harm.

Among settled cases, however, the line between what is a harm and what is not can often be rather blurred. In theory, proper economic analysis of the actual and expected costs and benefits of conduct can illuminate the distinction—and do so in accordance with the statute.

6. Section 5 "Harms": Costs Without Benefits

The Commission's willingness to regard the existence of harm (or the risk of harm), without more, as the beginning and end of liability under Section 5's authority is also decidedly problematic. While a firm that does a poor job protecting user's data may deserve to be penalized, such a conclusion is impossible absent evaluation of the benefits conferred by the same conduct that risks consumers' data and the benefits the firm may confer by investing the saved costs of heightened security elsewhere. As the Commission has itself committed, it "will not find that a practice unfairly injures consumers unless it is injurious in its *net* effects."[128] From a public perspective, there is little or no evidence that the Commission evaluates net effects.

Of crucial importance, the FTC's unbalanced approach to evaluating the costs and benefits of data security dramatically over-emphasizes the risks of data exposure (not least by treating even the most trivial risk as potentially actionable) and fails to evaluate at all (at least publicly) the constraints on innovation and experimentation imposed by its de facto strict-liability approach.

Even if one concludes that the FTC has the correct approach in general—i.e., that it is preferable for the agency to adopt an approach that errs on the side of preventing data disclosure—this still says

---

[124] Letter from FTC Chairman J.C. Miller, III to Senator Packwood and Senator Kasten (March 5, 1982), reprinted in H.R. REP. No. 156, Pt. 1, 98th Cong., 1st Sess. 27, 32 (1983).

[125] S. REP. NO. 103-130, at 13 (1994).

[126] F.T.C., Statement of Commissioner Orson Swindle, Touch Tone, File No. 982-3619 at 3-4 (Apr. 22, 1999).

[127] *Id.* at 3 n. 7.

[128] Unfairness Policy Statement, *supra* note 26, at 1073 (emphasis added).

nothing about how this approach should be applied in specific instances. Unless we are to simply accede to the construction of Section 5 as a strict liability statute, the Commission must put down some markers that clearly allow for a consideration of the *benefits* of imperfect data protection along with the attendant costs.

Consider the recent FTC complaint against D-Link in which it claims that:

> [D-Link] repeatedly . . . failed to take reasonable software testing and remediation measures to protect their routers and IP cameras against well- known and easily preventable software security flaws, such as "hard-coded" user credentials and other backdoors, and command injection flaws, which would allow remote attackers to gain control of consumers' devices; Defendant D-Link has failed to take reasonable steps to maintain the confidentiality of the private key that Defendant D-Link used to sign Defendants' software, including by failing to adequately restrict, monitor, and oversee handling of the key, resulting in the exposure of the private key on a public website for approximately six months; and . . . Defendants have failed to use free software, available since at least 2008, to secure users' mobile app login credentials, and instead have stored those credentials in clear, readable text on a user's mobile device.[129]

The complaint does not describe the calculation that led the FTC to determine that D-Link failed to take "reasonable steps." It is possible, of course, that D-Link's security design decisions that, for instance, led it to avoid using encrypted credentials versus storing them locally in plain text were unsupported by any business case. But the opposite is also true, and the cost savings (or other possible benefits) of such decisions may outweigh the costs. Yet the complaint fails to evidence any evaluation of relative costs and benefits, concluding simply that D-Link's actions "caused, or are likely to cause, substantial injury to consumers in the United States that is not outweighed by countervailing benefits to consumers or competition."[130] As D-Link's Motion to Dismiss notes:

> Pleading this element as a legal conclusion, as the FTC has done here, is insufficient. With the sole exception of a passing reference to "free software," the Complaint contains no factual allegations whatsoever regarding the monetary costs, let alone the time- and labor-related costs, of conducting whatever "software testing and remediation measures" and other actions the FTC believes Defendants should have implemented.[131]

So too the FTC avoids recognizing that the security decisions made for an Internet-connected appliance used behind a Wi-Fi network would have a different set of security and safety considerations than a camera that streams to the open Internet. And, most important, it completely fails to address whether and how D-Link's behavior objectively failed to live up to an identifiable standard of conduct.

---

[129] Complaint at 5, FTC v. D-Link Corp., No. 3:17-CV-00039-JD (N.D. Cal. Mar. 20, 2017) [hereinafter D-Link Complaint].

[130] *Id.* at 29.

[131] Defendant Motion to Dismiss at 8, FTC v. D-Link Corp., No. 3:17-CV-00039-JD (N.D. Cal. Jan. 31, 2017).

The FTC's claims are thus insufficient to provide (or reflect) any sort of discernible standard that, applied here, would permit a firm to determine what conduct that may lead to harm will nevertheless offer sufficient benefit to avoid liability.

And, indeed, the court recognized precisely this failing when it dismissed many of the claims from the case:

> The pleading problem the FTC faces concerns the first element of injury. The FTC does not allege any actual consumer injury in the form of a monetary loss or an actual incident where sensitive personal data was accessed or exposed. Instead, the FTC relies solely on the likelihood that DLS put consumers at "risk" because "remote attackers could take simple steps, using widely available tools, to locate and exploit Defendants' devices, which were widely known to be vulnerable."[132]

Echoing the ALJ's Initial Decision in the *LabMD* case, the court goes on to note that these are "effectively the sum total of the harm allegations, and they make out a mere possibility of injury at best."[133]

Relying on *Twombly*, the court noted the insufficiency of the FTC's unfairness pleading because "[t]he absence of any concrete facts makes it just as possible that [D-Link's] devices are not likely to substantially harm consumers, [on net,] and the FTC cannot rely on wholly conclusory allegations about potential injury to tilt the balance in its favor."[134]

And again highly reminiscent of the problematic theory of harm in *LabMD*, the judge noted that "[t]he lack of facts indicating a likelihood of harm is all the more striking in that the FTC says that it undertook a thorough investigation before filing the complaint . . . ."[135]

On Occasion, Only The Barest Of Benefits

Even where the Commission does advert to possible benefits from a firm's risk-increasing conduct, it has done so incompletely. In its *LabMD* opinion, for instance, the Commission states that:

> A "benefit" can be in the form of lower costs and then potentially lower prices for consumers, and the Commission "will not find that a practice unfairly injures consumers unless it is injurious in its net effects.". . . This cost-benefit inquiry is particularly important in cases where the allegedly unfair practice consists of a party's failure to take actions that would prevent consumer injury or reduce the risk of such injury . . . . When a case concerns the failure to provide adequate data security in particular, "countervail-

---

[132] FTC v. D-Link, Case No. 3:17-cv-00039-JD Order Re Motion to Dismiss (N.D. Cal. 2017)

[133] *Id.*

[134] *Id.*

[135] *Id.*

> ing benefits" are the foregone costs of "investment in stronger cybersecurity" by comparison with the cost of the firm's existing "level of cybersecurity." . . . [W]e conclude that whatever savings LabMD reaped by forgoing the expenses needed to remedy its conduct do not outweigh the "substantial injury to consumers" caused or likely to be caused by its poor security practices.[136]

This construction assumes that the inquiry into countervailing benefits is strictly limited to the question of the direct costs and benefits of the data security practices themselves. But the potential benefits to consumers are derived from the business *as a whole*, and the data security practices of the business are just one component of that. The proper tradeoff isn't between more or fewer resources invested in making data security practices "reasonable," as if those resources materialize out of thin air. Rather, the inquiry must assess the opportunity costs that a business faces when it seeks to further a certain set of aims—chief among them, serving customers—with limited resources.

A proper standard must also take account of the cost to the business (in this case, LabMD) not only of adopting more stringent security practices, but also of identifying and fixing its security practices *in advance* of the breach. It may be relatively trivial to identify a problem and its solution after the fact, but it's another matter entirely to ferret out the entire range of potential problems ex ante and assign the optimal amount of resources to protect against them based on (necessarily unreliable) estimates of their likelihood and expected harm. And this is all the more true when the "problem" is an unknown thief intent on quietly constructing exactly the sort of problems that would catch the attention of the Commission.

No doubt LabMD could have done *something* more to minimize the likelihood of the breach. But it's not clear that any reasonable amount of time or money could have been spent in advance to identify and adopt the *right* something under the FTC's strict-liability-like standard. As former Commissioner Wright noted in his dissent in the *Apple* case:

> When designing a complex product, it is prohibitively costly to try to anticipate *all* the things that might go wrong. Indeed, it is very likely impossible. Even when potential problems are found, it is sometimes hard to come up with solutions that that one can be confident will fix the problem. Sometimes proposed solutions make it worse. In deciding how to allocate its scarce resources, the creator of a complex product weighs the tradeoffs between (i) researching and testing to identify and determine whether to fix potential problems in advance, versus (ii) waiting to see what problems arise after the product hits the marketplace and issuing desirable fixes on an ongoing basis . . . . The relevant analysis of benefits and costs for allegedly unfair omissions requires weighing of the benefits and costs of discovering and fixing the issue that arose *in advance* versus the benefits and costs of finding the problem and fixing it *ex post*.[137]

---

[136] FTC LabMD Opinion, *supra* note 15, at 26.

[137] *In re* Apple, Inc., 15-16 (Jan. 15, 2014) (No. 12-31008) (Joshua D. Wright, Comm'r, dissenting), https://www.ftc.gov/sites/default/files/documents/cases/140115applestatementwright_0.pdf.

Moreover, while *some* LabMD patients might have benefited on net from heightened data security along with higher prices or reduced quality along some other dimension in exchange for it, it is by no means clear that all LabMD patients would so benefit. As Commissioner Wright also discussed at length in his *Apple* dissent, an appropriate balancing of countervailing benefits would weigh the costs of greater security to marginal patients (those for whom LabMD's services plus the FTC's asserted "reasonable" security practices at a higher price would have induced them to forego using LabMD) against the benefits to inframarginal patients who would have been willing to pay more to have the FTC's imposed security practices.

> Staff has not conducted a survey or any other analysis that might ascertain the effects of the consent order upon consumers. The Commission should not support a case that alleges that [LabMD] has underprovided [data security] without establishing this through rigorous analysis demonstrating – whether qualitatively or quantitatively – that the costs to consumers from [LabMD's data security] decisions have outweighed benefits to consumers and the competitive process.
>
> . . .
>
> The Commission has no foundation upon which to base a reasonable belief that consumers would be made better off if [LabMD] modified its [security practices] to conform to the parameters of the consent order. Given the absence of such evidence, enforcement action here is neither warranted nor in consumers' best interest."138

Unfortunately, making this assessment would require surveying consumers and estimating the harm caused (or likely to be caused, and discounted by the likelihood) and its magnitude, as well as the ex ante costs of identifying the possible harm and preventing it. But, to date, the Commission does not have that evidence. Thus, again, in the end the practical effect is to convert Section 5 into a strict liability statute in which any breach (or potential breach) runs the risk of FTC scrutiny, regardless of what steps were taken or could have been taken.

III. Suggested data security reforms

Given the above noted deficiencies in current practice on data security issues, we believe that a series of modest reforms may greatly improve matters. The core problem is that the FTC's processes have enabled it to operate with discretion that lacks no obvious boundaries in developing the doctrine by which its three high level standards are applied in real-world cases. Chiefly, the FTC has been able to circumvent judicial review through its "common law of consent decrees," and to effectively circumvent the rulemaking safeguards imposed by Congress in 1980 through a variety of forms of "soft law": guidance and recommendations that have, if indirectly and through amorphous forms of pressure, essentially regulatory effect.

---

[138] *Id.* at 14, 17.

Our aim is not to hamstring the Commission, but to ensure that it wields its power with greater analytical rigor — something that should significantly benefit consumers. Ideally, the impetus for such rigor would be provided by the courts, through careful weighing of the FTC's implementation of substantive standards in at least a small-but-significant percentage of cases. Those decisions would, in turn, shape the FTC's exercise of its discretion in the vast majority of cases that will — and should, in such an environment — inevitably settle out of court. The Bureau of Economics and the other Commissioners would also have far larger roles in ensuring that the FTC takes its standards seriously. But reaching these outcomes requires adjustment to the Commission's processes, not merely further codification of the standards the agency already purports to follow.

A. Giving more weight to economic analysis

Many of what we see as the most needed reforms go to the lack of explicit economic analysis. The core problem with the FTC's current approach to data security is that it enjoys a largely unconstrained discretion. The FTC proclaims the advantages of this ex post approach, which relies on case-by-case enforcement, rather than rigid ex ante rulemaking. Although there is much to commend an ex post enforcement regime, relative to the prescriptive regulatory paradigm that characterizes many other agencies (especially abroad), the required balancing of tradeoffs inherent in unfairness and deception have little public meaning if the courts do not review, follow or enforce them; if the Bureau of Economics has little role in the evaluation of these inherently economic considerations embodied in the enforcement decision-making of the Bureau of Consumer Protection or in its workshops; and if other Commissioners are able only to quibble on the margins about the decisions made by the FTC Chairman.

This could partially be achieved by ensuring that, whenever possible, the Bureau of Economics be involved in making important decisions (including the issuance of complaints and consent decrees), and in the production of important guidance materials (notably the best practices that the FTC commonly recommends in reports). Absent that instruction, the FTC, especially the Bureau of Consumer Protection, will likely resist fully involving the Bureau of Economics in its processes. For instance, for each such investigation that was closed with no official agency action, a description sufficient to indicate the legal and economic analysis supporting the Commission's decision not to continue such investigation, and the industry sectors of the entities subject to each such investigation.

Of course, there will be many cases where the economists have essentially nothing to say. The point is not that each case merits detailed economic analysis. Rather, the recommendation is intended to ensure that, at the very least, the opportunity to produce and disseminate a basic economic analysis by the Bureau of Economics is built into the enforcement process. Moreover, if an economic analysis is deemed appropriate, the determination of what constitutes an appropriate level of analysis should be made by the Bureau of Economics alone. Given the general scope of the FTC's investigations, it likely already collects the kind of data that could allow the Bureau of Economics to adequately per-

form these duties. Further involving economists is the Commission's complex data security assessments is perhaps the greatest opportunity to begin bringing the analytical rigor of law and economics to this field.

Another possibility would be to include more economic data in the FTC's closing letters. Doing so would allow companies to better identify those instances where a given course of conduct is unlikely to give rise to data security enforcement. Of course, the Commission may be (quite understandably) reluctant to include economic data in company-specific closing letters for reasons pertaining to confidentiality. Instead of writing company-specific letters, the FTC could thus aggregate the information, obscure the identity of the company at issue in each specific case, and thus speak more freely about the details of its situation. Although the tension between the goals of providing analytical clarity and maintaining confidentiality for the subjects of investigation is obvious, it is not an insurmountable conflict, and thus no reason not to require more analysis and disclosure, in principle.

B. Transparency

An additional important reform would be for the FTC to provide greater transparency regarding the reasoning that underpins its less-visible decisions, most notably consent decrees and closing letters.

The FTC might, for instance, synthesize closing decisions and enforcement decisions into doctrinal guidelines. When the FTC submitted the Unfairness Policy Statement to Congress, it noted, in its cover letter:

> In response to your inquiry we have therefore undertaken a review of the decided cases and rules and have synthesized from them the most important principles of general applicability. Rather than merely reciting the law, we have attempted to provide the Committee with a concrete indication of the manner in which the Commission has enforced, and will continue to enforce, its unfairness mandate. In so doing we intend to address the concerns that have been raised about the meaning of consumer unfairness, and thereby attempt to provide a greater sense of certainty about what the Commission would regard as an unfair act or practice under Section 5.[139]

This synthesis is what the FTC needs to do as far as data security enforcement is concerned. It could do so, through better organized reporting on its consent decrees and closing decisions. This is essentially what the various Antitrust Guidelines issued jointly by the DOJ and the FTC's Bureau of Competition do. The guidelines are rich with examples that illustrate the way the agencies will apply their doctrine. They explain how the kind of concepts articulated at the high conceptual level of, say, the FTC's Unfair, Deceptive or Abusive Acts and Practices ("UDAP") policy statements, can actually be applied to real world circumstances.[140]

---

[139] Unfairness Policy Statement, *supra* note 26.

[140] *See* Fed. Trade Comm'n & Dep't Of Justice, Antitrust Guidelines For Collaborations Among Competitors ii (Apr. 2000), *available at* https://www.ftc.gov/sites/default/files/documents/public .

One obvious challenge is that the antitrust guidelines synthesize litigated cases, of which the FTC has few relating to data security matters. This makes it difficult, though not impossible, for the FTC to do precisely the same thing on data security matters as the antitrust guidelines do. But that does not mean the FTC could not benefit from writing "lessons learned" retrospectives on its past enforcement efforts and closing letters.

Importantly, publication of these guidelines would not actually be a constraint upon the FTC's discretion; it would merely require the Commission to better explain the rationale for what it has done in the past, connecting that arc across time. Like policy statements and consent decrees, guidelines are not technically binding upon the agency. Yet, in practice, they would steer the Commission in a far more rigorous way than its vague "common law of consent decrees." It would allow the FTC to build doctrine in an analytically rigorous way as a second-best alternative to judicial decision-making — and, of course, as a supplement to judicial decisions, to the extent they happen.

C. Heightened judicial review

Of course, publishing guidelines is no substitute for actual judicial review. In that regard, an underappreciated aspect of the FTC's processes is investigation; for it is here that the FTC wields incredible power to coerce companies into settling lawsuits rather than litigating them. As former FTC Chairman Tim Muris observed, "Within very broad limits, the agency determines what shall be legal. Indeed, the agency has been 'lawless' in the sense that it has traditionally been beyond judicial control."[141] If meaningful judicial review is ever to be brought to bear on the final agency decisions embodied in consent orders, it is crucial that the complaints that give rise to those settlements be subjected to a more meaningful standard that imposes some evidentiary and logical burden on the Commission beyond the mere exercise of its discretion.

While it would certainly be an improvement to adopt even a "preponderance of the evidence" standard for the approval of consent decrees (relative to the status quo), we believe that this should be the standard for the approval of complaints, and that approval of consent decrees should be even higher (although the "preponderance of the evidence" is not a particularly high standard). The standard and process required by the Tunney Act for antitrust settlements would be a good place to begin. That act requires the FTC to file antitrust consent decrees with a federal court, and requires the court make the following determination:

> Before entering any consent judgment proposed by the United States under this section, the court shall determine that the entry of such judgment is in the public interest. For the purpose of such determination, the court shall consider:
>
> the competitive impact of such judgment, including termination of alleged violations, provisions for enforcement and modification, duration of relief sought, anticipated

[141] Timothy J. Muris, *Judicial Constraints*, in THE FEDERAL TRADE COMMISSION SINCE 1970: ECONOMIC REGU-LATION AND BUREAUCRATIC BEHAVIOR, 35, 49 (Kenneth W. Clarkson & Timothy J. Muris, eds., 1981).

> effects of alternative remedies actually considered, whether its terms are ambiguous, and any other competitive considerations bearing upon the adequacy of such judgment that the court deems necessary to a determination of whether the consent judgment is in the public interest; and
>
> B) the impact of entry of such judgment upon competition in the relevant market or markets, upon the public generally and individuals alleging specific injury from the violations set forth in the complaint including consideration of the public benefit, if any, to be derived from a determination of the issues at trial.[142]

If anything, a standard for settlements should require more analysis than this, as the Tunney Act has been relatively ineffective. In particular, any approach based on the Tunney act should allow third parties to intervene to challenge the FTC's assertions about the public interest.[143] This reform could go a long way toward inspiring the agency to perform more rigorous analysis.

However, merely requiring that Commission staff satisfy a "preponderance of the evidence" standard for issuing consumer protection complaints would already help, on the margin, to embolden some defendants not to settle. Even such a slight change could produce a significant shift in the agency's model, by injecting more judicial review into the FTC's doctrine. Though a preponderance of the evidence standard would hardly impose an insurmountable burden on the agency, it would at least impose a standard that is more than purely discretionary, and thus reviewable by courts and subject to recognizable standards upon which such review could proceed. Most importantly, enacting such a standard should, on the margin, embolden defendants to resist settling cases, thus producing more judicial decisions, which could in turn constrain the FTC's discretion.

More broadly, the FTC should recall that its ultimate goal is not to "prevail" over firms, but to work towards the emergence of a sound body of law and, most importantly, the deterrence of data security problems.[144] It would thus do well to prosecute more cases than it currently does. Judicial review is a necessary step for the creation of a body of common law, and although the FTC may lose many of these cases, the precedential value of these cases would be significant.

D. A More reasonable, less punitive, approach to security

For most firms facing data security challenges, the most significant impediment to implementing "reasonable" data security is simply that it can be unreasonably difficult to do well. A number of factors confound the goal of promulgating a general "reasonableness" standard across the economy, including the size of most firms, their sophistication, the state of the software

---

[142] 15 U.S.C. § 16(b)(1).

[143] The act currently provides that "Nothing in this section shall be construed to require the court to conduct an evidentiary hearing or to require the court to permit anyone to intervene." 15 U.S.C. § 16(b)(2).

[144] *See* Justin Hurwitz, *Data security and the FTC's uncommon law*, 101 IOWA L. REV., 1013 (2015).

ecosystem (including, not just availability but cost and ease of implementation), and the diverse nature of the threats.

Although a well-developed sense of "causation," as meant under Section 5(n) and as we discuss *supra*,[145] is of course necessary, most of the investigative and enforcement attention of the Commission should be focused on the duty of firms given their particular circumstances, and the "reasonableness" (or lack thereof) of their precautions relative to similarly situated firms. To date, Section 5(n) has largely been focused on the "likelihood of substantial harm" inquiry, which tends to flatten the unique features of firms across the economy, holding each to the same standard — which ultimately results in either an extremely overbroad standard (holding every firm to the same duty as Google, Facebook, Netflix or Amazon) or an extremely underdeveloped standard (holding every firm to the same duty as a small hobby e-commerce site).

But in a world where the most basic challenge of data security is that a firm exercising subjectively reasonable caution is not necessarily reasonably secure in objective terms, relying primarily on the likelihood of harm inquiry to determine liability creates a regime in which firms face effectively random punishment for the misfortune of being hacked. Thus, the use of the "reasonableness" duty inquiry should function as a predicate for the Section 5(n) likelihood inquiry, and not the currently applied approach of using the likelihood of a harm as the proxy for "reasonableness."

In practice, for the millions of small- and medium-sized firms that make up the majority of the American economy, such an inquiry would ask whether they put good-faith effort into data security, proportional to their sophistication, risks and sensitivity of the data they hold, resources, and other constraints. This approach would operate akin to the business judgement rule, deferring to the good-faith efforts of businesses to assess and address their security needs – and focusing enforcement efforts on cases where businesses either failed entirely to address (that is, to make judgements about) their data security needs or did so in a way that was so improper as to be *per se* unreasonable (a much lower bar for businesses to pass than objective or subjective reasonableness).

Following from this, the Commission could promulgate policies that encourage firms both more explicitly to consider their data security policies as well as to communicate them to their users, with a failure to do so amounting to evidence of an unfair practice under Section 5. Firms that failed to abide by their stated policies could be investigated for engaging in deception. And, of course, a firm that experiences an actual security incident would presumptively be on notice about that type of incident – and a failure to address it (demonstrated, for instance, by repeated similar security incidents) could suggest a failure to exercise reasonable security judgement.

In effect, the FTC would thus place more emphasis on encouraging firms to think about security in the first place (and not on evaluating how well they understand or address their security needs) and

---

[145] *See* notes 74-90 and accompanying text.

on how firms communicate their data security practices to consumers, instead of questioning the appropriateness of these underlying data security measures.

The Commission already focuses on this very question in its deception cases, where it examines whether firms have accurately portrayed their data security practices to consumers. Our suggestion is to extend this type of inquiry to unfairness cases. In essence, a firm's failure to affirmatively communicate its data security measures to consumers would amount to an unfair practice. In conjunction with enforcement on deception grounds, this would incentivize firms to reveal their true data security efforts, or lack thereof.

The most important virtue of this approach is that it would give consumers, investors, competing firms and enforcers a much clearer picture of the data security practices that are being deployed throughout the economy. As a result, the FTC and courts would not have to reconstruct the hypothetical data security policy that a careful firm would have adopted in a given case. Instead, these authorities will be in a position to benchmark a given firm's data security practices against the relevant community standard. This would undoubtedly mark a better starting point for decision-making than the status quo. Perhaps more importantly, sanctioning firms that have not revealed their data security policies would encourage them to actually consider these issues and come up with a data security strategy appropriate to their circumstances. In other words, encouraging firms to think about data security would be beneficial in and of itself.

Additionally, under this approach to data security, the FTC would play the role of advocate for firms struggling with data security, instead of their antagonist. As mentioned above, the challenge that most firms face in adopting reasonable security practices is that it is unreasonably hard for most firms to secure their systems. There is little question that security breaches are harmful, in general, to consumers – the FTC could do significant good for consumers by focusing its efforts on improving the overall quality of the security ecosystem and making it easier for firms to secure their systems.

Of course, any initiatives along these lines should remain within the confines of Section 5 (n) of the FTC Act. A firm's failure to communicate its data security policy to its users would thus only be actionable, at least on the basis of unfairness, when the cumulative conditions of Section 5 (n) are met.[146] So any lack of disclosure should (i) cause or be likely to cause substantial injury to consumers; (ii) this injury should not be reasonably avoidable by consumers themselves; (iii) and should not be outweighed by countervailing benefits to consumers or to competition.

[146] *Id.* at 1016-1017.