When "Reasonable" Isn't: The FTC's Standard-less Data Security Standard

By Geoffrey A. Manne and Kristian Stout

Forthcoming in THE JOURNAL OF LAW, ECONOMICS & POLICY

ICLE Antitrust & Consumer Protection Research Program

White Paper 2017-4

ICLE | 3333 NE Sandy Blvd., #207 | Portland, OR 97232 | 503.770.0652
icle@laweconcenter.org | @laweconcenter | www.laweconcenter.org

When "Reasonable" Isn't: The FTC's Standard-less Data Security Standard

By Geoffrey A. Manne and Kristian Stout[*]

Introduction

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."[1] 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*

---

[*] Geoffrey A. Manne is the founder and Executive Director of International Center for Law & Economics ("ICLE"), a nonprofit, nonpartisan research center based in Portland, OR. Kristian Stout is Associate Director for Innovation Policy at ICLE. The ideas expressed here are the authors' own and do not necessarily reflect the views of ICLE's advisors, affiliates or supporters. Please contact the authors with questions or comments at icle@laweconcenter.org.

[1] 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.

> *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.[2]

In its *LabMD* opinion, the Commission describes this approach as "cost-benefit analysis."[3] 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.

A few examples from the staff posting illustrate the point:

> [i]n 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 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.[4]

Twitter's conduct is described as having "increased the risk" of breach. 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 weight 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. Crucially, this extends not only

---

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

[3] Opinion of the Commission at 11, In the Matter of LabMD, Inc., (No. 9357), 2016-2 Trade Cas. (CCH July 29, 2016) [hereinafter "*FTC LabMD Opinion*"].

[4] Arias, *supra* note 1 (emphasis added).

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.*[5]

Can "reasonable" data security require firms to do *anything* that "could have reduced the risk" of breach? That, again, means that virtually no conduct need be sufficient, because there is almost always *something* that could further reduce risk — including limiting the scope or amount of normal business activity: Surely it reduces the "risk" of breach to, for instance, significantly limit the number of customers; eschew the use of computers; and conduct all business in a single, fortified location.

But, 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 FTC's recent *LabMD* case highlights the scope of the problem and the lack of economic analytical rigor endemic to the FTC's purported 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, masquerading as an economic framework.[6]

LabMD, a small diagnostics laboratory, was (up until the FTC got involved) in the business of providing cancer screening services to patients. As part of this business –

---

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

[6] *See, e.g.*, Maureen K. Ohlhausen, *Opening Keynote*, ABA 2017 Consumer Protection Conference, at 2-3 (Feb. 2, 2017), *available at* https://www.ftc.gov/system/files/documents/public_statements/1069803/mko_aba_consumer_protection_conference.pdf.

and as required by HIPAA and its implementing regulations – LabMD retained patient data, including personally identifiable information (PII).[7] In 2007, Tiversa, a "cyberintelligence" company that employed custom algorithms to exploit P2P network vulnerabilities, downloaded from the computer of a LabMD employee a file (dubbed the "1718 file") that contained PII of approximately 9,300 LabMD patients.[8] Shortly thereafter, Tiversa engaged in what LabMD has characterized (in our opinion, fairly) as a shakedown to induce LabMD to pay Tiversa for "remediation" services. LabMD refused and fixed the P2P vulnerability itself.[9]

Following some fairly questionable interactions between the FTC and Tiversa,[10] LabMD came under investigation by the agency for over three years. In its enforcement complaint the FTC 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 a dumpster 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 information," and "caused, or is likely to cause, substantial injury to consumers… constitut[ing] unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act…."[11]

The FTC brought the complaint before its ALJ, who 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,"[12] and that the FTC failed to demonstrate that LabMD's conduct had a high probability of injuring consumers. The ALJ here put down a critical marker in the case, one that gave some

---

[7] Brief of Petitioner at 2, LabMD Inc. v. FTC, (11th Cir. Sep. 29, 2016) (No. 16-16270) [hereinafter "*LabMD 11th Cir. Petitioner Brief*"].

[8] *Id.* at 3.

[9] *Id.* at 2-3.

[10] *See* Staff Report: *Tiversa, Inc.: White Knight or Hi-Tech Protection Racket?*, Committee on Oversight and Government Reform, U.S. House of Representatives, 113th Congress (Jan. 2, 2015).

[11] Brief of Complainant at 5, In re Matter LabMD, Inc., (No. 9357) [hereinafter "*FTC Complainant Brief*"].

[12] Initial Decision at 42, In the Matter of LabMD Inc., (No. 9357), 2015 WL 7575033 (Fed. Trade Comm. Nov. 13, 2015) [hereinafter "*ALJ LabMD Initial Determination*"]. 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.

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.

Unsurprisingly, the FTC voted to overturn the *ALJ LabMD Initial Determination*, finding, 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; and
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, further,
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.[13]

In actuality, however, the Commission's manufactured "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.

This paper explores these defects, paying particular attention to the FTC's decision in *LabMD*.

I. The inherent ambiguity of "reasonable" data security, particularly at the FTC

There is a great deal of ambiguity about how the law should treat data and data breaches. Within antitrust, for instance, there is a movement to incorporate firms' collection and use of data into standard merger and conduct analyses. But in this

[13] *FTC LabMD Opinion*, *supra* note 3, at 11. LabMD has appealed the case to the Eleventh Circuit Court of Appeals. LabMD, Inc. v. F.T.C., (11th Cir. 2016) (No. 16–16270).

context, it remains unclear how (and whether) to do so. Data stores and data collection and use practices are plausibly relevant components of non-price competition, but non-price components (like reputation) are notoriously difficult to quantify, not least because consumers have heterogeneous risk and privacy preferences. So, too, data *security* practices can contribute to the perceived value of a product or service from the consumer perspective, but quantifying that value with any degree of precision is difficult, if not impossible.

Similarly, when there is a data breach, the calculation of the extent of harm (if any) to consumers is difficult to measure. This is complicated, of course, by the fact that, even assuming that particularized harm can be accurately assessed, that harm needs to be balanced against the benefits conferred by decisions within the firm to optimize a product or service for lower prices or in favor of other consumer-valued features, such as ease-of-use, performance, and so forth.

Additionally, some, including the FTC, have asserted that exposure of information is, in and of itself, a harm to individuals, apart from any economic consequences. In the *FTC LabMD Opinion*, for instance, the Commission asserted that

> the disclosure of sensitive health or medical information [that] causes additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n). For instance... disclosure of the mere fact that medical tests were performed irreparably breached consumers' privacy, which can involve "embarrassment or other negative outcomes, including reputational harm."[14]

Legally, data security issues are addressed through either (or both) of two categories of law: public law, by regulatory agencies enforcing consumer protection statutes or provisions; and private law, typically by private litigants asserting tort claims like negligence and trespass, as well as contract and fraud claims.

The FTC — obviously a consumer protection agency engaged in the enforcement of public law — nevertheless evinces a curious pattern of enforcement that seems to

---

[14] *FTC LabMD Opinion*, *supra* note 3, at 17.

uneasily mix nominal principles derived from the common law of torts with an asserted authority under Section 5 largely unbounded by precedent, strict adherence to statutory language, or common law principles.

The Eleventh Circuit, in fact, took note of the problematic "heads I win, tails you lose" character of this interpretation of Section 5 during oral argument in LabMD's appeal from the *FTC LabMD Opinion*:

> **Judge Robreno**: 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…, 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**: Well I believe that's exactly what Congress intended when…
>
> **Judge Tjoflat**: Every time something happens, which heretofore was thought to be reasonable in the industry say, all of a sudden becomes unreasonable because in hindsight you realize well this could have been avoided…
>
> **FTC**: The Commission doesn't act in terms of hind sight; the Commission acted here in terms of what was reasonable at the time…
>
> **Judge Tjoflat**: I'm talking about your just plain unreasonable standard.
>
> **FTC**: It's certainly true that something that could be reasonable today might not be reasonable tomorrow…
>
> **Judge Wilson**: Doesn't that underscore the importance of, or the significance of, a rulemaking, otherwise you are regulating data security on a case by case basis, right?
>
> **FTC**: We are regulating data security on a case by case basis and that's exactly what the Supreme Court in *Bell Atlantic* and *Chenery* said that an agency is entitled to do…
>
> **Judge Tjoflat**: And it doesn't matter whether the subject has any notice at all?

> **FTC**: Correct. Correct.[15]

While the FTC's scattershot approach could be deemed to reflect the intensely fact-specific nature of reasonableness for data security, in practice it results largely in excessive ambiguity (which further reinforces its discretionary authority). One 2014 study, for example, combed through the (then) 47 FTC data security actions and cobbled together a list of 72 "reasonable practices" that might constitute a relevant benchmark.[16] Reviewing the FTC's own "guidance" — purportedly encompassing its approach to data security — the study found that

> the standard language that the FTC uses is terse and offers little in the way of specifics about the components of a compliance program. Consequently, anyone seeking to design a program that complies with FTC expectations would have to return to the complaints to parse out what the FTC views as "unreasonable" — and, by negation, reasonable — privacy and data security procedures.[17]

At the same time, at least one former Federal Trade Commissioner has described the 2014 NIST Cybersecurity Framework[18] as "fully consistent with the FTC's enforcement framework."[19] And yet the NIST Framework itself is a compendium of five separate industry standards, each comprising, respectively, only 66, 48, 28, 24 or 21

---

[15] Oral Argument at 34-36, 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).

[16] See Patricia Bailin, *What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices*, IAPP/Westin Research Center Study (Oct. 30, 2014), *available at* http://bit.ly/2hJkIWR.

[17] *Id.* at 1.

[18] Nat'l Inst. of Stds & Tech, *Framework for Improving Critical Infrastructure Cybersecurity, ver.1.0* (Feb. 12, 2014) [hereinafter "NIST Framework"], *available at* http://bit.ly/2hJslfy.

[19] FTC Commissioner Julie Brill, *On the Front Lines: The FTC's Role in Data Security*, Keynote Address Before the Center for Strategic and International Studies Conference, "Stepping into the Fray: The Role of Independent Agencies in Cybersecurity" (Sep. 17, 2014), *available at* http://bit.ly/2hJrrzJ (emphasis added)

of the 72 "reasonable" data security practices that a firm could derive from the FTC's consent orders.[20]

In other words, even the most comprehensive industry standards — the "fully consistent" NIST Framework — is *inconsistent* with the set of "reasonable" practices that might be derived from the FTC's consent orders between 2002 and 2014.[21] As one commenter noted, "no company could possibly execute every industry standard in the 400-plus-page NIST 800-53, even with a full IT department and certainly not without one."[22] Moreover, data security covers a wide scope of activities beyond technological measures, including such mundane practices as implementing password-change policies, searching employee bags on the way out of work, and best-practices education.

The primary problem, of course, is that, unlike the common law, the FTC's catalogue of possible practices is just that: a catalogue, without a discernible analytical framework to guide its application to specific facts. This is not how the common law operates.

To see this, imagine that a group of academics, lawyers, and judges were asked to draft a "Restatement of the Law of Data Security" based on the FTC's "common law" of consent decrees, guidance documents, and blog posts. Would it be possible to render an informative compendium describing the logic of the cases and the application of their outcomes to a range of factual, procedural, and legal circumstances? Would it, in other words, come close to looking like the Restatement of Torts?

The FTC has (to our knowledge) never attempted to do any analysis that approaches the rigor of a judicial decision. Frequently, relevant facts are lumped together or elided over entirely in complaints and investigation notices, and rarely, if ever, does the Commission identify which facts were essential to its unfairness determination; certainly it never identifies the relative importance, scale, or impact of any of those

---

[20] See Kristina Rozan, *How Do Industry Standards for Data Security Match Up with the FTC's Implied "Reasonable" Standards – And What Might This Mean for Liability Avoidance?*, iapp.org (Nov. 25, 2014), *available at* http://bit.ly/2hJsiAs.

[21] See Nat'l Inst. of Stds & Tech, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53 Rev.4 (Apr. 2013) ["NIST 800-53"], *available at* http://bit.ly/2hJtB2j.

[22] Rozan, *How Do Industry Standards for Data Security Match Up with the FTC's Implied "Reasonable" Standards*, *supra* note 20.

facts on the FTC's decision to undertake an enforcement action or the specific elements of the resulting consent order. Thus, for example, none of the Commission's settlements or other statements addresses even the most basic question of how a target's size — or even of the size of the data breach in question — bears on the company's failure to undertake (and pay for) any particular data security practices.

Yet without that basic data it would be next to impossible to build something like a "Restatement of Data Security" sufficient to enable a lawyer to assess the likely liability risk of a firm's particular conduct given its particular circumstances.

Finally, because of the FTC's "flexible" and evolving standards, and because its standards are developed through one-sided consent decrees with limited application and little, if any, legal analysis, "we don't [even] know what we don't know:"

> *[W]e don't know what we don't know*, that is, whether other practices that have not yet been addressed by the FTC are "reasonable" or not. (In fact, we don't even know whether there is… a comprehensive FTC data security standard). Even in those cases that have been pursued, we don't know how high the reasonableness bar is set. Would it be enough for a company to elevate its game by just an increment to clear the reasonableness standard? Or does it have to climb several steps to clear the bar?[23]

II. 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).[24]

---

[23] 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).

[24] *See FTC LabMD Opinion*, *supra* note 3, at 26 (quoting In the Matter of Int'l Harvester Co., 104 F.T.C. 949, 1073 (1984) [hereinafter *"Unfairness Statement"*]) ("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.'").

In form, Section 5(n) and the Unfairness Statement from which it is derived incorporate a negligence-like standard,[25] 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 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.[26]

---

[25] In point of fact, Section 5 most likely contemplates *more* than mere negligence, *e.g.*, 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* Wyndham, 799 F.3d at 245 (suggesting that, to the extent "these are requirements of an unfairness claim," such requirements were met based on defendant's allegedly deceptive statements); In re 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.

LabMD 11th Cir. Petitioner Brief, *supra* note 7, at 28. 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).

[26] 15 U.S.C.A. 45(n).

Congress plainly intended to constrain the FTC's discretion in order to avoid the hasty assumption that imposing nearly *any* costs on consumers is "unfair."[27] 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).[28] 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.[29]

And the FTC itself has asserted that this language leads to 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.[30]

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

---

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

[28] *See, e.g.,* Restatement (Second) of Torts § 291 (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.").

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

[30] Commission Statement Marking the FTC's 50th Data Security Settlement, *supra* note 2, at 1.

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.

But the Commission seems to disagree that a predictable analysis — or even notice of how any analysis would work — is required at all. 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...
>
> **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.[31]

---

[31] *LabMD 11th Circuit Oral Argument*, *supra* note 15, at 35-36.

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

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' plain requirement that the Commission demonstrate duty, causality and substantiality, and perform a cost-benefit analysis of risk and avoidance costs. While the FTC pays lip service to addressing 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,"[32] and we don't know how the Commission would actually weigh them in an actual rigorous analysis.

In its *LabMD* opinion, for instance, the FTC 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, 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

---

[32] Tene, *The Blind Men, the Elephant and the FTC's Data Security Standards*, *supra* note 23.

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, the conditional probability that a company's security practices were unreasonable given the occurrence of a breach may be *higher* than average, but 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 woefully fails to accomplish this, and, as discussed in more detail below, imposes an effective strict liability regime on companies that experience a breach, despite its claim that "the mere fact that a breach occurred does not mean that a company has violated the law."

A. A duty without definition

Section 5(n) plainly requires a demonstrable connection between conduct and injury. While the anticompetitive harm requirement that now defines Sherman Act jurisprudence was a judicial construct,[33] 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. 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 taking the FTC at face value and assuming "reasonableness" is meant as shorthand for the full range of elements required by Section 5(n), the FTC's approach to reasonableness is fatally deficient.

The FTC purports to engage in a case-by-case approach to unreasonableness, eschewing prescriptive guidelines in an effort to avoid unnecessarily static definitions. While

---

[33] *See, e.g.*, Continental T.V., Inc. v. GTE Sylvania, Inc., 433 U.S. 36 (1977).

agencies do have authority to issue regulations through case-by-case adjudication,[34] 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,[35] *Chenery* does not provide quite the support that the FTC claims.

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.'[36]

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 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, however. In *Chenery*, the respondent, a company engaged in a corporate reorganization, was governed by statutory provisions that explicitly required it to apply to the SEC for permission to amend its filings in order to permit the conversion of its board members'

---

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

[35] Brief for Respondent at 49, LabMD Inc. v. FTC, No. 16-16270 (11th Cir. Sep. 29, 2016).

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

preferred stock into common stock in the new corporation.[37] 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.[38]

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 were well aware that they had to apply to the SEC for approval. Thus, the Court held, 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, however. Instead, the FTC seeks targets for investigation and exercises prosecutorial discretion without 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 is 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 developed remarkably consistent criteria for establishing it. Thus, under typical negligence standards, an actor must have — and breach — a duty

---

[37] Chenery, 332 U.S. at 201.

[38] *Id.* at 201.

of care before its conduct will be deemed unreasonable.[39] 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.[40] 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.[41]

In some other (non-data-security) contexts, the FTC *has* developed something approaching a duty analysis for its unfairness cases. In *In re Audio Communications, Inc.*, for instance, the Commission pursued a company that specifically targeted children with an advertisement bearing a cartoon rabbit that encouraged them to surreptitiously call a 900 number that would end up applying charges to their parents' phone bills.[42] In part, the Commission pursued the unfairness claim on the basis that children are relatively more vulnerable, and firms therefore owe a greater duty of care when marketing to them. As FTC Commissioner Leary noted about the case in a later speech:

> Some "unfairness" cases seem primarily dependent on the particular vulnerability of a class of consumers. Children are the most conspicuous example.... Because children were directly targeted through television ads on otherwise innocuous programs, parents had no reasonable way to avoid the charges. There was no claim of misrepresentation and the conduct might well have been entirely legal had the marketing appeals

---

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

[40] Restatement (Second) of Torts § 285 (1965).

[41] *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.").

[42] In the Matter of Audio Commc'ns Inc., 114 F.T.C. 414, 415 (1991).

> been directed at adults. Moreover, there is no suggestion that it is inherently wrong to advertise these particular services, or any others, in a way that appeals to children.[43]

But 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 in passing,[44] 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 operationalizable 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.

Because "perfect" data security is impossible, not all data security practices that "increase" a risk of breach are unfair.[45] *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.[46] 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."[47] While the Commission disputed some of these

---

[43] Thomas B. Leary, *Unfairness and the Internet* (Apr. 13, 2000), *available at* https://www.ftc.gov/public-statements/2000/04/unfairness-and-internet.

[44] *See, e.g., FTC LabMD Opinion*, *supra* note 3, at 12 (referring to HIPAA as "a useful benchmark for reasonable behavior").

[45] *See* Commission Statement Marking the FTC's 50th Data Security Settlement, *supra* note 2, at 1.

[46] *FTC LabMD Opinion*, *supra* note 3, at 17-25.

[47] *LabMD 11th Cir. Petitioner Brief*, *supra* note 7, at 2 (citations to the record omitted).

practices, for every practice the FTC claims LabMD did *not* engage in, there were other practices in which it inarguably *did* engage.[48]

And 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 measures to protect against them. Given this, the existence of P2P software on one computer, in one department, and against its policy was hardly inherently unreasonable in light of the protections LabMD *did* adopt. Despite successfully avoiding all other security breaches, the Commission invalidated all of LabMD's data protection measures because of the single (unlikely) 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. 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,[49] the FTC failed to establish that LabMD's practices, *as a whole*, were insufficient to meet a reasonable standard of care.

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.[50]

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

---

[48] *Id.*

[49] *See FTC LabMD Opinion*, *supra* note 3, at n. 23.

[50] Gerard Stegmaier and Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 675-77 (2013).

> **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.[51]

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.[52]

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 approach fail to

---

[51] *LabMD 11th Circuit Oral Arguments*, *supra* note 15, at 23-24.

[52] Stegmaier and Bartnick, *supra* note 50, 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, *Id.* at 680, and represents a relatively stronger version of the doctrine. By contrast, some other circuits require little more than actual notice. While the Fifth Circuit "may be consistent with the D.C. Circuit," *Id.* at 15 n.45, the Seventh Circuit requires that regulations are not "incomprehensibly vague." 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.*

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

Such an approach is tantamount to a strict liability regime — in marked contrast to the regime that Congress implemented in Section 5(n).

1. 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 some question whether the FTC Act contemplates conduct at all that merely facilitates (or fails to prevent) harm caused by third parties, rather than conduct that causes harm to consumers directly.[53] But even if the FTC does have authority to police third-party breaches (and thus the appropriate security measures to reduce their risk),[54] 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.[55] 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 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 is thus reasonably on notice about the behavior of *that* partic-

---

[53] *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).

[54] *See, e.g.*, Wyndham, 799 F.3d at 248–49.

[55] *See generally* Richard Craswell, *Identification of Unfair Acts and Practices by the Federal Trade Commission*, 1981 WISC. L. REV 107 (1981).

ular 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 attention to the nature of third-party conduct, despite its assertion that "reasonable and appropriate security is a continuous process of assessing and addressing risks."

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 (let alone its subsequent, rather suspicious conduct in working with FTC investigators to develop the case), 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 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 hacking. 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."[56] But, of course, 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

[56] *FTC LabMD Opinion*, *supra* note 3, at 21 (emphasis added).

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. Certainly, just because Tiversa identified and accessed the file says next to nothing about the likelihood that a typical P2P user would.[57]

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 it cannot establish that the 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 risk of inadvertent exposure, this may well have been sufficient (at minimum, the evidence in the case suggests that it was sufficient to confine P2P file-sharing to a single computer from which very little sensitive information was taken). 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.[58]

---

[57] 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 (*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 — least of all typical P2P users searching for music and videos.

[58] Interestingly, the FTC notes in its Decision 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.

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. 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 content 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 apparent disregard for its obligation to prove causation is even more stark. 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 FTC offers a series of *non sequiturs*, unsupported by evidence. The Order cites allegedly deficient practices,[59] but establishes no causal link between these and Tiversa's theft of the 1718 file — nor *could* it, because the theft had nothing to do with, for example, password policies, operating system updates, or firewalls. Moreover, things like integrity monitoring and penetration testing at best, "'might have'

FTC LabMD Opinion, *supra* note 3, 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 Determination, *supra* note 12, at 83-84.

[59] *See, e.g.*, *FTC LabMD Opinion*, *supra* note 3, at 2.

aided detection of the application containing the P2P vulnerability," in the FTC's own words.[60] 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.[61] 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 Administrative Law Judge found this assertion 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.[62] 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

---

[60] *Id.* at 31, 4 n.13.

[61] *See ALJ LabMD Initial Determination*, *supra* note 12, at 54.

[62] *Id.* at 53.

> 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.[63]

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.[64]

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 will 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,

---

[63] *ALJ LabMD Initial Determination*, *supra* note 12, at 81.

[64] *FTC LabMD Opinion*, *supra* note 3, at 23.

> 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 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.[65]

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

---

[65] *ALJ LabMD Initial Determination*, *supra* note 12, at 52-53.

> 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.[66]

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.

---

[66] *Id.*

1. An abuse of the FTC's "likely to cause" authority: The HTC *Case*

The Commission's 2013 *HTC* complaint and settlement exemplifies its willingness to infer causation under Section 5(n)'s "likely to cause" language 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.[67] 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."[68] The end result was that HTC's engineers had created security flaws that *theoretically* could be used to compromise user data.[69]

There were not, however, *any* known incidents of data breach arising from consumers' use of the approximately ten to twelve million devices at issue.[70] 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.[71] 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.[72]

---

[67] In the Matter of HTC Am. Inc., 155 F.T.C. 1617, *2 (2013) [hereinafter "*HTC Complaint*"].

[68] *Id.* at *2.

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

[70] Alden Abbot, *The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?*, THE HERITAGE FOUND. (Sep. 10, 2014), *available at* http://www.heritage.org/report/the-federal-trade-commissions-role-online-security-data-protector-or-dictator.

[71] *HTC Complaint*, *supra* note 67, at *6.

[72] *Id.*

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, 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.

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.[73]

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.[74]

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.

1. Breach is not (or should not be) the same thing as harm

One of the core errors committed by the FTC in *LabMD* (particularly by Complaint Counsel before the ALJ, but also, although less obviously, by the Commission itself

---

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

[74] *HTC Complaint*, *supra* note 67, at *2.

in its *LabMD Opinion*) is the assertion that breach alone can constitute harm. Similarly flawed (and 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.[75] 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 FTC'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).[76] 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 information."[77] 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.[78]

---

[75] *See , e.g.,* Commission Statement Marking the FTC's 50th Data Security Settlement, *supra n*ote 2, at 1. ("The mere fact that a breach occurred does not mean that a company has violated the law").

[76] In the Matter of Eli Lilly & Co., 133 F.T.C. 763, 766-767 (May 8, 2002).

[77] *Id.*

[78] *See* Letter from James C. Miller III, Chairman, Fed Trade Comm., to Rep. John D. Dingell, Chairman, Committee on Energy and Commerce (Oct. 14, 1983) [hereinafter "*Deception Policy Statement*"], *available at* 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

The underlying theory of materiality or harm in *Eli Lilly* — while not in any way explicated by the FTC, even in the accompanying Analysis of Proposed Consent Order to Aid Public Comment, 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).[79] 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 Warehouse, in its first unfairness-based data security case.[80] While hardly a model of rigorous analysis assessing all of the required elements of an unfairness case under Section 5(n), the FTC in *BJ's Warehouse* at least 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 reissued 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.[81]

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 not be monetary, and it need not be well-defined

---

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.

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

[80] In the Matter of BJs Wholesale Club, Inc., 2005 WL 1541551, at *2 (June 16, 2005).

[81] *Id.*

(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 (*e.g.*, there is a security breach) because of conduct by the company that causes 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* (a precursor case to the FTC's current line of data security cases involving clearly fraudulent conduct by an "information broker"):

> We have never held that the mere disclosure of financial information, without allegations of ensuing economic or other harm, constitutes substantial injury under the statute.[82]

But by 2012, in its Privacy Report, the Commission asserted that disclosure 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

[82] In the Matter of Touch Tone, 1999 WL 233879, at *3 (April 22, 1999).

> reveal previously private information even absent physical or financial harm, or unwarranted intrusions.[83]

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, absent any such evidence, *LabMD* brought this theory to fruition.

As it admitted, the Commission "does not know,"[84] whether any patient encountered a single problem related to the breach, and thus never articulated any actual injury caused by LabMD's conduct.[85] The Commission instead asserted that mere exposure of information suffices to establish harm.[86] 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.[87] 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,[88] no such disclosure occurred in *LabMD*. That the third-party responsible for exposure of data itself viewed the data — which is effectively all that

---

[83] FTC, *Protecting Consumer Privacy in an Era of Rapid Change; Recommendations for Business and Policymakers*, at 8 (March 2012) [hereinafter "*FTC Privacy Report*"], *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[84] *FTC LabMD Opinion*, *supra* note 3, at 17

[85] 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 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.

[86] *See FTC LabMD Opinion*, *supra* note 3, at 18 ("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.

[87] *See generally* In the Matter of MTS, Inc., 137 F.T.C. 444 (May 28, 2004) (No C-4110), *available at* https://goo.gl/4emzhY (Tower Records liable for software error that allowed 5,225 consumers' billing information to be read by anyone, which actually occurred).

[88] *FTC LabMD Opinion*, *supra* note 3, at 17.

happened in that case — cannot be the basis for injury without simply transforming the breach itself into the injury.

D. The troubling implication of the FTC's approach: Mere storage of sensitive data can constitute conduct "likely to cause" harm

A crucial and troubling implication of the Commission's position is that it effectively permits the FTC to read Section 5 to authorize an enforcement action against any company that stores sensitive data, regardless of its security practices and regardless of the existence of a breach.

To be sure, the Commission is unlikely to bring a case absent *some* unauthorized disclosure of sensitive data. But the standard adopted by the FTC permits it to infer injury from *any* unauthorized disclosure and to infer that conduct is likely to cause injury virtually regardless of the extent of increased risk of exposure attributable to the conduct. The FTC's interpretation thus effectively removes any identifiable limits on its discretion to bring a data security action under Section 5.

If a third-party breach alone is a "harm," it is not because of the intervention of a third-party but merely the fact that data is exposed to anyone unauthorized to view it. This means that information leaving the company in *any* unauthorized manner would be sufficient to demonstrate actual harm — and therefore a *potential* of it leaving the company would amount to *likely* harm. 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 with PII is prosecutorial discretion.

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 FTC should have to 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."

1. The FTC's reading of "likely to cause" gives it unfettered discretion not contemplated by Section 5

In its *LabMD* Decision the FTC attempts to mitigate this position to a degree, demurring on the adequacy 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 FTC reads a sort of superficial "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."[89]

Thus, the Commission concludes:

---

[89] *FTC LabMD Opinion*, *supra* note 3, at 21.

> 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.[90]

But when establishing causality, 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 both cases 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*,"[91] "raises" clearly does not mean "increases the degree of" here, but rather "stirs up" or "gives rise to."[92] And 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.

---

[90] *Id.*

[91] *FTC LabMD Opinion*, *supra* note 3, at 21 (quoting *Unfairness Statement*, at 1073 n.12) (emphasis added).

[92] *Raise*, MERRIAM-WEBSTER.COM (last visited Jun. 1, 2017), *available at* https://goo.gl/R2sVhm.

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 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*.[93] 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."[94] 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.[95]

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

---

[93] Complaint Counsel's Reply Brief, In the Matter of LabMD, Inc., Dkt. No. 9357, 2016-2 Trade Cas. At 33 (CCH July 29, 2016) [hereinafter "*FTC ALJ Reply Brief*"].

[94] *FTC LabMD Opinion*, *supra* note 3, at 21 (internal citations omitted).

[95] *Wyndham*, 799 F.3d at 255 (internal citations omitted).

"likely" harm to consumers, provided the harm is substantial enough — which it invariably is. As the Commission claims:

> 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.[96]

The position that the Commission upholds in the *FTC LabMD Opinion* was plainly put forward by Complaint Counsel in its oral arguments before the ALJ: merely storing sensitive data and "plac[ing data] at risk" — *any risk* — are all that is required to meet the standard of unfairness under Section 5. 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[.]" (emphasis added)[97]

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.

---

[96] *Id.* at 25 (emphasis added).

[97] *LabMD 11th Circuit Oral Argument*, *supra* note 15, at 48.

2. *The FTC's interpretation of "likely to cause" gives it a temporally unbounded power over every company. Ever.*

LabMD (in our opinion, correctly) argued that the scope of a "likely to cause" authority must be bounded in some fashion in order to create some meaningful limitation on the FTC's power to police conduct.[98] In essence, the phrase "likely to cause" needs to be constrained in a way that focuses the FTC's authority on a contextually relevant period of time. LabMD argued that the relevant time period was upon the issuance of an order — if conduct was no longer ongoing at the time an order was issued, the Commission had no power to find that a respondent was "likely to cause" harm.[99]

In its turn, the Commission offered a textual analysis that suggested that the whole of Section 5 taken together indicates that the "likely to cause" language does not restrict the FTC to a persistently forward-looking analysis.[100] Further, the Commission argued that allowing respondents to alter their conduct in expectation of an investigation would permit "malfeasors to evade FTC enforcement by stopping their illegal behavior upon learning of an FTC investigation."[101]

On the textual analysis argument, the FTC has some basis for argument that it has the ability to look at prospective conduct from the vantage of a past time period. But it goes too far to suggest that this examination should be unbounded in order to prevent malfeasors from getting off scot-free. First, as noted above, the FTC does not have the power to extract damages — that is to exact punitive ends from its enforcement power — but only to prospectively deter conduct. Thus, the purpose of Section 5 can be broadly stated as one of, either through threat of enforcement or though actual enforcement, guarantees that companies do not treat consumers unfairly.

Second, once a complaint has been issued, any conduct that "is likely to cause" harm is a proper target of action for the Commission. To not require some temporal

---

[98] Brief of Petitioner LabMD, Inc. at 22-23, In the Matter of LabMD, Inc., , 2016-2 Trade Cas. (CCH July 29, 2016) (No. 9357) [hereinafter "*LabMD ALJ Brief*"].

[99] *Id.* at 23.

[100] *FTC ALJ Reply Brief*, *supra* note 93, at 35-36.

[101] *Id.* at 36.

marker against which the FTC can be said to examine prospective conduct is to essentially let the FTC regulate any behavior of any company that has possessed data since the creation of Section 5 (or at least since it started policing data security).

In LabMD, the FTC has used its authority to pursue a company that was "likely to cause" harm *after* the company had already remedied its behavior and before the FTC ever instituted an investigation. Under this reading of Section 5, there is nothing to stop the FTC from looking back at, for instance, Amazon in the year 2001 and issuing a new complaint against it because something it had done then was "likely to cause" harm to consumers — even though Amazon had long since identified and rectified the alleged harm. On the FTC's account, if a firm has remedied its conduct *even before the FTC investigates it*, that firm should be liable under an "is likely to cause" harm theory.

And consider the perversity in the FTC's reasoning. It is concerned that requiring a contextually-bound "likely to cause" authority will allow malfeasors to evade enforcement. But, at least theoretically, the purpose of the FTC is to encourage private firms to do the right thing in the first place. Yet the FTC is concerned that if a firm fears an investigation and remedies its bad conduct the Commission will be powerless to pursue it. This is to say that, if aware of any failures of its data security program as well as the FTC's power to police data security, a firm voluntarily remedies its conduct, it is "getting away" with something. Such a perverse reading requires one to believe that voluntary conduct in the shadow of the law somehow constitutes illicit activity.

Thus, even though no one was *actually* hurt (remember, this is a "likely" harm), and the firm remedied its conduct before the Commission got involved, the Commission believes it should be able to mete out punishment. It is hard to understand exactly where the boundary of the FTC's power exists under this view of its authority.

E. The problems with the FTC's approach to substantiality of harm (whether it is "likely" or not)

Of course the threatened injury must be "substantial." As noted, however, 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. Although we cannot be sure from either the Commission's opinion or the complaint counsel's closing arguments before the ALJ

how large a data collection practice is sufficient to trigger the FTC's rules, there is some evidence in the FTC's consent decrees suggesting a scale. In short, 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.[102]

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).[103] 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 for trivial or speculative harm." 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."[104]

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. [105] 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."[106] 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.

---

[102] Geoffrey Manne and Ben Sperry, *FTC Process and the Misguided Notion of an FTC "Common Law" Of Data Security*, at 22, *available at* http://masonlec.org/site/rte_uploads/files/manne%20%26%20sperry%20-%20ftc%20common%20law%20conference%20paper.pdf.

[103] 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." *Unfairness Statement*, *supra* note 24, at 1073.

[104] S. Rep. 103-130, at 13 (1994) (emphasis added).

[105] In the Matter of Touch Tone, 1999 WL 233879, at *1.

[106] *Id.*

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. Yet the FTC regularly falls short of meaningful analysis.

Even in *Wyndham*, where the FTC had a relatively strong set of facts to work with, it couldn't resist the urge to manufacture elements of consumer harm. The Commission asserted that every consumer whose information was exposed was harmed because, among actual harms like identity theft, there were losses associated with "cash-back, reward points, and other loyalty benefit programs."[107]

And, although not in an enforcement context, the FTC's 2014 Data Brokers Report at many points captures the FTC's general approach to preventing highly speculative harms. For instance, it recommended that Congress enact legislation to prevent possible harms to consumers when having their identity verified as part of applications for things like mobile phones.[108] But the report explicitly notes that

> The Commission does not have any information on the prevalence of errors in the consumer data that underlie data brokers' risk mitigation products. In a different context, a recent Commission Report assessed the accuracy of consumer information in credit reports and found that 5.2% of consumers had errors on at least one of their three major credit reports that could lead to them paying more for products such as auto loans and insurance.[109]

As Commissioner Wright noted in "dissenting" from various assertions in the Report,

> this recommendation is premature because there is no evidence about the existence or scope of this hypothetical problem. As noted in supra

---

[107] Plaintiff's Responses and Objections to Defendants' Fourth Set of Requests for Admissions at 10, FTC v. Wyndham Worldwide Inc., 799 F.3d 236 (3d Cir. 2015) (No. 14-3514).

[108] FTC, *Data Brokers: A Call for Transparency and Accountability*, at 53 (May 2014) [herein after "*Data Brokers Report*"], *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[109] *Id.* at 53 n.95.

> note 95, the Commission does not have any information on the prevalence of errors in the consumer data that underlie data brokers' risk mitigation products.[110]

Thus, the Commission felt confident to recommend legislation that could affect millions of consumers and thousands of businesses without any direct support for its feared harms, and where, even in the meager evidence it draws from a "related" context, only a small handful of consumers experienced an unknown degree of harm. As Commissioner Wright further noted:

> [I am] wary of extending FCRA-like coverage to other uses and categories of information without first performing a more robust balancing of the benefits and costs associated with imposing these requirements.[111]

F. Section 5 "harms:" Costs without benefits

The Commission's willingness to regard 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."[112] In practice 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 effectively 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 nothing about how this approach should be applied in

---

[110] *Id.* at 54 n.96.

[111] *Id.* at 52 n.88.

[112] *Unfairness Statement*, *supra* note 24, at 1073 (emphasis added).

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 where 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.[113]

What the complaint assiduously avoids is describing the calculation that led it 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 Complaint fails to evidence any evaluation of relative costs and benefits, concluding simply that D-Link's conduct "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."[114] 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 soft-

---

[113] FTC v. D-Link Corp., No. 3:17-CV-00039-JD, at 5 (N.D. Cal. filed Mar. 20, 2017), [hereinafter "*D-Link Complaint*"], *available at* https://www.ftc.gov/system/files/documents/cases/d-link_complaint_for_permanent_injunction_and_other_equitable_relief_unredacted_version_seal_lifted_-_3-20-17.pdf.

[114] *Id.* ¶ 29.

> ware," 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.[115]

So too it 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 — because the FTC has never offered any such standard to guide firm conduct. The FTC's claims are thus insufficient both to meet even its own "reasonableness" standard — let alone Section 5's cost-benefit requirement — as well as 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.

The Commission consistently avoids taking seriously the costs (*i.e.*, foregone benefits) of incremental increases in harm avoidance. For instance, in its Privacy Report, the Commission says that:

> In terms of weighing costs and benefits, although it recognizes that imposing new privacy protections will not be costless, the Commission believes doing so not only will help consumers but also will benefit businesses by building consumer trust in the marketplace.[116]

In other words: "There are costs to the data security requirements we might adopt, and there are benefits. Because we assert that *some* benefit exists, the magnitude of the costs does not matter." One would search the document in vain for a more-rigorous statement of how (or whether) the FTC will weigh the costs and benefits of data security practices; it just isn't there — which is odd for a purported "framework" adopted in accordance with a statute that *explicitly* demands such a weighing. As Commissioner Rosch pointedly noted, dissenting from the Report:

> There does not appear to be any... limiting principle applicable to many of the recommendations of the Report. If implemented as written, many

---

[115] Defendant Motion to Dismiss, FTC v. D-Link Corp., No. 3:17-CV-00039-JD, at 5, 8 (N.D. Cal. filed Mar. 20, 2017).

[116] *FTC Privacy Report*, supra note 83, at 8.

> of the Report's recommendations would instead apply to almost all firms and to most information collection practices. It would install "Big Brother" as the watchdog over these practices not only in the online world but in the offline world. That is not only paternalistic, but it goes well beyond what the Commission said in the early 1980s that it would do, and well beyond what Congress has permitted the Commission to do under Section 5(n).[117]

But the Privacy Report was just that — a report. In theory, at least. Although replete with language that the contents represent "best practices," and are meant to assist companies in devising their own privacy and security practices, in reality the Report reads like a set of vague commands from the Commission that will undoubtedly form the basis for enforcement actions in the future.

The Commission does assert in the Report that

> The privacy framework is designed to be flexible to permit and encourage innovation. Companies can implement the privacy protections of the framework in a way that is proportional to the nature, sensitivity, and amount of data collected as well as to the size of the business at issue.[118]

But as we have shown elsewhere, the FTC's past actions and imposed remedies belie this claim:

> What is clear is that, almost without regard to *any* underlying characteristics, size of injury, number of injured parties, etc., an almost identical set of practices is prescribed by the agency to remedy alleged unreasonableness in data security, meaning, no matter what industry, size, or extent of possible harm, every business regulated by the FTC should know what is expected of it. The FTC has been remarkably consistent in this.
>
> Now, we believe this is actually a *bad* thing. The absence of any apparent connection between different circumstances and different remedies – or, put differently, the absence of any explanation why very different circumstances are properly addressed by the very same data security processes –

---

[117] *Id.* at C-5 (Dissenting Statement of Comm'r J. Thomas Rosch).

[118] *Id.* at 9.

> is never much explained and hasn't evolved in over a decade. The likelihood that this consistency reflects the optimal outcome is extremely low.[119]

Emblematic of the FTC's failure to account for benefits of challenged conduct as well as harms is the *Apple* product design case.[120] In that matter, the Commission brought charges against Apple for allegedly designing the iOS app store in a way that led to "unfair" billing practices. Historically, the Commission would bring such cases where a defendant affirmatively endeavored to mislead consumers — including cases of outright fraud, unauthorized billing, and cramming.[121]

In the *Apple* case, however, the Commission alleged that Apple had designed the App Store in a way that made it too easy for children to make purchases without parental consent.[122] The core of the Commission's complaint revolved around the fact that the App Store would permit a 15 minute window for password-free purchases and downloads once a person had entered their password.[123]

This case highlights a crucial part of the FTC's mandate embodied in Section 45(n) that is all too frequently ignored: a likely harm can be deemed "unfair" only if there are no countervailing benefits from the challenged practice, and if consumers could not themselves reasonably avoid the harm. But there the FTC essentially replaced its own judgment for that of Apple's — a company whose very existence depends upon it making products for which consumers are willing to pay.

The Commission completely failed to perform an adequate analysis to determine if the "harm" suffered by parents of children who were able to make a purchase within the 15 minute window was not counterbalanced by the greater degree of convenience that an overwhelming number of consumers enjoyed by virtue of the feature. Moreover, there was scant attention paid to assessing whether parents themselves were

---

[119] Manne and Sperry, *supra* note 102, at 13.

[120] *In the Matter of Apple Inc.*, 112-31008, 2014 WL 253519, at *1 (MSNET Jan. 15, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140327applecmpt.pdf.

[121] *See id.* at *2.

[122] *Id.* at *1.

[123] *Id.* at *15.

actually unable to avoid the potential harm, despite the likelihood of their proximity to their phones and their children.

Nonetheless, Apple settled, despite the fact that the company had likely performed a wealth of its own consumer research in order to discover the optimal balance of features for its products. It would be surprising indeed if the ambiguity implicit in the loosely interpreted unfairness standard played no part in the decision to settle.

1. On occasion, only the barest of benefits

Even where the Commission does advert to possible benefits from a firm's risk-increasing conduct, it does so in a crabbed and insufficient fashion. 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, "countervailing 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.[124]

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. Of course this can't be correct. 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.

---

[124] *FTC LabMD Opinion*, *supra* note 3, at 26.

A proper standard must also take account of the cost to 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 FTC.

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. As former Commissioner Wright noted in his dissent in the *Apple* case, in which the Commission committed this same error:

> 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*.[125]

Moreover, while *some* LabMD patients might have benefited from higher prices or reduced quality along some other dimension in exchange for heightened security, 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

---

[125] Dissenting Statement of Comm'r Joshua D. Wright, In the Matter of Apple, Inc., (Jan. 15, 2014) (No. 12-31008), *available at* https://www.ftc.gov/sites/default/files/documents/cases/140115applestatementwright_0.pdf.

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."[126]

Unfortunately for the FTC, making this assessment would require surveying consumers or estimating the harm caused (or likely to be harmed — and discounted by the likelihood) and its magnitude, as well as the *ex ante* costs of identifying the possible harm and preventing it. But because the FTC has steadfastly adopted its "all inferences without evidentiary support" framework, it neither has, nor is it willing to entertain even estimating, 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.

Conclusion

The Commission has a decidedly fatalistic view, one that effectively implies that data security practices sufficient to meet the standard of Section 5 are impossible. This

---

[126] *Id.*

means that once a company collects sensitive data, it is presumptively in violation of the statute. It is only prosecutorial discretion that separates legal and illegal conduct. And even where breaches occur, the FTC's position is strange. Inferring unreasonable security practices from the fact of disclosure alone, without any demonstration of concrete harm or even rigorous assessment of the *likelihood* of harm (in clear contravention of the statute), the FTC effectively reads a European-style "fundamental right to privacy" into Section 5 of the FTC Act.