
**Testimony of**

**TechFreedom**

Berin Szóka[1] & Graham Owens[2]

# FTC Stakeholder Perspectives: Reform Proposals to Improve Fairness, Innovation, and Consumer Welfare

*Hearing before the Subcommittee on Consumer Protection, Product Safety, Insurance, & Data Security of the U.S. Senate Committee on Commerce, Science, & Transportation*

**Tuesday, September 26, 2017**

**2:30 p.m.**

**Russell Senate Office Building**
**Room 253**

---

[1] Berin Szóka is President of TechFreedom, a nonprofit, *nonpartisan* technology policy think tank. J.D. University of Virginia School of Law; B.A. Duke University. He can be reached at bszoka@techfreedom.org. With thanks to my dedicated legal staff at TechFreedom, and in particular Vinny Sidhu and Sunny Seon Kang.

[2] I. Graham Owens is a Legal Fellow with TechFreedom. J.D. George Washington University School of Law; B.A. University of Virginia. He can be reached at gowens@techfreedom.org.

# Table of Contents

# I. Introduction

Over the last two decades, use of, and access to, the Internet has grown exponentially, connecting people and businesses and improving the human condition in ways never before imagined. In 2011, 71.7% of households reported accessing the Internet, a sharp increase from 18 percent in 1997 and 54.7% in 2003.[3] This digital growth — from a network of computers that only a few consumers could reach, to a seemingly infinite marketplace of ideas accessible by almost all Americans — has benefited society beyond measure, affording consumers the ability to access information, purchase goods and services, and interact with each other almost instantaneously without having to leave the home.[4]

However, as use and benefits of the Internet has grown, so too has the collection of personal data and, consequently, cyber-attacks endeavoring to steal that data. Since 2013, the number of companies facing data breaches has steadily increased.[5] In 2016, 52% of companies reported experiencing a breach — an increase from 49% in 2015 — with 66% of those who experienced a breach reporting multiple breaches.[6] Perhaps not surprisingly, not much has changed since 2000, where one report revealed that system penetration by outsiders grew by 30% from 1998 to 1999.[7] Interestingly, despite immense improvements in companies' ability to anticipate and prevent cyber-attacks, some of the largest and most sophisticated companies in the world, including Sony, Target, eBay, and JPMorgan, continue to experience data breaches today,[8] just as they did in 2000.[9] In spite of these statistics, the United States currently has no comprehensive legal framework in which to inform companies of the best

---

[3] THOM FILE, U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES 1 (May 2013), https://www.census.gov/prod/2013pubs/p20-569.pdf; *see also* Steve Case, The Complete History of the Internet's Boom, Bust, Boom Cycle, Business Insider (Jan. 14, 2011), *available at* http://www.businessinsider.com/what-factors-led-to-the-bursting-of-the-internet-bubble-of-the-late-90s-2011-1.

[4] *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 1 (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[5] PONEMON INST. LLC, FOURTH ANNUAL STUDY: IS YOUR COMPANY READY FOR A BIG DATA BREACH? 1 (2016), http://www.experian.com/assets/data-breach/white-papers/2016-experian-data-breach-preparedness-study.pdf [hereinafter PONEMON, DATA BREACH].

[6] *Id.*

[7] Hope Hamashige, *Cybercrime can kill venture*, CNN (March 10, 2000), http://cnnfn.cnn.com/2000/03/10/electronic/q_crime/index.htm (reporting the findings of the Computer Security Institute at Carnegie Mellon University).

[8] PONEMON INST. LLC, 2014: A YEAR OF MEGA BREACHES 1 (2015), http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL3.pdf.

[9] Hamashige, *Cybercrime* (noting that, just as today, in 2000, "[e]ven the biggest Internet companies with the most sophisticated technology are vulnerable to hackers, a trend highlighted last month when hackers stopped traffic on several popular Internet sites including Yahoo!, Amazon.com and eBay.").

practices to both prevent or respond to cyber-attacks, as well as to ensure that they're acting responsibly in the eyes of the Government.[10]

Absent a comprehensive statutory framework, the Federal Trade Commission ("FTC" or "Commission") happily stepped in to police the vast number of data security and privacy practices not covered by the few Internet privacy and cyber security statutes enacted at the time. For two decades, the FTC has grappled with the consumer protection issues raised by the Digital Revolution. Armed with vast jurisdiction and broad discretion to decide what is unfair and deceptive, the agency has dealt with everything from privacy to data security, from online purchases to child protection, and much more. The FTC has become the Federal *Technology* Commission — a term we coined,[11] but which the FTC and others have embraced.[12]

This was inevitable, given the nature of the FTC's authority. Enforcing the promises made by tech companies to consumers forms a natural baseline for digital consumer protection. On top of that deception power, the FTC has broad power to police other practices, without waiting for Congress to catch up. As the FTC said in its 1980 Unfairness Policy statement:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion.[13]

---

[10] *See, e.g.,* ALAN CHARLES RAUL, TASHA D MANORANJAN & VIVEK MOHAN, THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 268 (Alan Charles Raul, 1st ed. 2014) ("With certain notable exceptions, the US system does not apply a 'precautionary principle' to protect privacy, but rather, allows injured parties (and government agencies) to bring legal action to recover damages for, or enjoin, 'unfair or deceptive' business practices.").

[11] Berin Szóka & Geoffrey Manne, The Second Century of the Federal Trade Commission, TECHDIRT (Sept. 26, 2013), available at https://www.techdirt.com/blog/innovation/articles/20130926/16542624670/secondcentury-federal-trade-commission.shtml; see also Consumer Protection & Competition Regulation in a High-Tech World: Discussing the Future of the Federal Trade Commission, Report 1.0 of the FTC: Technology & Reform Project, 3 (Dec. 2013), available at http://docs.techfreedom.org/FTC_Tech_Reform_Report.pdf.

[12] Kai Ryssdal, The FTC is Dealing with More High Tech Issues, MARKETPLACE (Mar. 7, 2016) (quoting then-Chairman Edith Ramirez), available at http://www.marketplace.org/2016/03/07/tech/ftc-dealing-more-high-tech-issues.

*See, e.g.,* Omer Tene, *With Ramirez, FTC became the Federal Technology Commission*, IAPP (Jan. 18, 2017), https://iapp.org/news/a/with-ramirez-ftc-became-the-federal-technology-commission/.

[13] Fed. Trade Comm'n, FTC Policy Statement on Unfairness (1980), available at https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (hereinafter 1980 Unfairness Policy Statement).

The question is not whether the FTC *should* be the Federal Technology Commission, but *how* it wields its powers. For all that academics like to talk about creating a Federal Search Commission[14] or a Federal Robotics Commission,[15] and for all the talk in Washington of passing "comprehensive baseline privacy legislation" or data security legislation, the most important questions turn on the FTC's processes, standards, and institutional structure. How the FTC and Congress handle these seemingly banal matters could be even more important in determining how consumer protection works in 2117 than will any major legislative lurches over the next century. Indeed, with the costs of cybercrimes expected to reach $2 trillion by 2019,[16] the business community can ill afford to have to anticipate the approaches of both hackers and federal regulators simultaneously, and it would seem more practical for the agency to help guide businesses by providing best practices to better protect their consumers. Yet, rather than promulgate rules or provide any clear guidance, the FTC has instead chosen to approach the issue through case-by-case enforcement actions, almost always ending in consent decrees, which do not admit liability and only focus on prospective requirements of the specific defendant in that case.[17]

This approach, and the resulting ambiguity, has left companies facing uncertainty in terms of whether their data security and privacy practices are not only sufficient to safeguard against an FTC enforcement action, but more importantly, whether they're utilizing the best practices available to protect their consumers' data and privacy.

---

[14] *See, e.g.,* Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149 (2008), *available at* http://www.lawschool.cornell.edu/research/cornell-law-review/upload/Bracha-Pasquale-Final.pdf.

[15] *See, e.g.,* Ryan Calo, *The case for a federal robotics commission*, Brookings Institute (Sept. 15, 2014), *available at* https://www.brookings.edu/research/the-case-for-a-federal-robotics-commission/; Nancy Scola, *Why the U.S. might just need a Federal Commission on Robotics*, Washington Post (Sept. 15, 2014), *available at* https://www.washingtonpost.com/news/the-switch/wp/2014/09/15/why-the-u-s-might-just-need-a-federal-commission-on-robots/?utm_term=.38dfc4bec72e.

[16] Steve Morgan, *Cyber Crime Costs Projected to Reach $2 Trillion by 2019*, Forbes (Jan. 17, 2016), *available at* https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6e10063a3a91.

[17] *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257, n.22. (3d Cir. 2015). Notably, this practice is not entirely limited to data security and privacy enforcement — though for reasons later discussed, the effects on companies are arguably more severe in this context — by the Commission, with one study finding that 1,524 of the 2,092 enforcement action brought by the FTC in either federal or administrative courts have ended in consent decrees without any adjudication. This means that almost 73% of the FTC's enforcement actions have ended in legally enforceable orders, despite no impartial judicial guidance as to the factual and legal legitimacy of the FTC's claims. *See* Daniel A. Crane, *Debunking Humphrey's Executor*, 83 GEO. WASH. L. REV. 1835, 1867 (2015). But in tech-related cases its almost 100%, meaning the courts have played essentially no role at all in disciplining the FTC's use of unfairness in "informational injury" cases. *See infra* note 122 (providing list of a few cases that did not result in settlement).

Understandably, this ambiguity has frustrated judges and legal commentators alike, even resulting in one company's demise. Such frustration was made abundantly clear by the Third Circuit when, despite affirming the FTC's authority to regulate cyber security practices under the "unfair practices" prong of Section 5, the court nonetheless questioned the Commission's assertion that its consent decrees and "guidance" somehow create standards against which companies' cyber practices can be tested for "unfairness."[18] In fact, the Third Circuit emphatically agreed with the defendant's claim that "consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by § 45(a)."[19] The court continued:

> We recognize it may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees. Indeed, these may not be the kinds of legal documents they typically consulted. At oral argument we asked how private parties in 2008 would have known to consult them. The FTC's only answer was that "if you're a careful general counsel you do pay attention to what the FTC is doing, and you do look at these things." Oral Arg. Tr. at 51. We also asked whether the FTC has "informed the public that it needs to look at complaints and consent decrees for guidance," and the Commission could offer no examples. *Id.* at 52.[20]

The court's frustration did not end with the Commission's use of consent decrees either, making sure to also address issues with the FTC's 2007 guidebook, *Protecting Personal Information, A Guide for Businesses*, which, according the FCC, "describes a 'checklist[]' of practices that form a 'sound data security plan.'"[21] Ultimately, the court recognized that "[t]he guidebook does not state that any particular practice is required by [Section 5]," and "[f]or this reason, we agree … that the guidebook could not, on its own, provide "ascertainable certainty" of the FTC's interpretation of what specific cybersecurity practices fail [Section 5]."[22]

Despite being rebuked by practitioners and courts alike, the FTC has brushed aside this frustration and continued to rely on consent decrees, conclusory guidebooks/reports, and "blog posts" to inform businesses as to what constitutes reasonable data security and privacy practices. By contrast, the FTC has pursued a radically different course, providing significantly more thorough guidance in an area not considered to be the FTC's primary jurisdiction — environmental regulations through "Green Guides." As explained below, these Green Guides

---

[18] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 252-253, 255 (3d Cir. 2015).

[19] *Id.* at 257 n.22.

[20] *Id.* at 257 n.23.

[21] *Id.* at 257.

[22] *Id.* at 257 n.21.

reflect a sincere and thoughtful effort by the FTC to gather relevant data as the basis for analyzing not only "what" is required, but more significantly "why" is it essential and "how much" of a certain practice is necessary.

On privacy and data security, the Commission has refused to do such empirical work or to issue clear guidance, relying instead on consent decrees and conclusory reports and guidebooks that lack any evident empirical foundation. This has deprived businesses of the regulatory certainty and clarity they need to comply with the law — and deprived consumers of better, more consistent data security and privacy practices. The Commission has flaunted the warning given it by the D.C. Circuit over forty years ago, that "courts have stressed the advantages of efficiency and expedition which inhere in reliance on rule-making instead of adjudication alone," including in providing businesses with greater certainty as to what business practices are not permissible.[23] Ironically, the D.C. Circuit made that statement in a case where the FTC fought vehemently — and the court agreed — for the authority to provide the very guidance they refuse to provide to the digital economy today. Congress *did* provide that rulemaking authority a year later, with the Magnuson-Moss Act of 1975,[24] but also found it necessary to institute new procedural safeguards in 1980, after the FTC's gross abuse of its rulemaking powers in the intervening five years,[25] which culminated in the agency being denounced as the "National Nanny."[26]

With this backdrop in mind, I come before this Committee today with two goals. First, to inform this body — through a historical lens — of the FTC's ongoing procedural issues, particularly as they pertain to data security and privacy practices. Second, to use that historical analysis as a framework with which to propose practical process reforms that will ensure American businesses and the FTC work together as partners, not enemies, to make certain that consumers'—including Americans as well as foreign consumers who patronize U.S. businesses—data and privacy are afforded the greatest respect and protection possible.

---

[23] *Nat'l Petroleum Refiners Ass'n v. F.T.C.*, 482 F.2d 672, 675–76 (D.C. Cir. 1973), cert. denied, 415 U.S. 951 (1974).

[24] The Magnuson-Moss Warranty Federal Trade Commission Improvement (Magnuson-Moss) Act, Pub.L.No. 93-637, § 202(a), 88 Stat. 2193 (1975).

[25] The Federal Trade Commission Improvements Act of 1980 (Improvements Act), Pub.L. No. 96-252, 94 Stat. 374 (1980).

[26] Editorial, WASH. POST (Mar. 1, 1978), reprinted in MICHAEL PERTSCHUK, REVOLT AGAINST REGULATION, 69–70 (1982); *see also* J. Howard Beales III, *Advertising to Kids and the FTC: A Regulatory Retrospective that Advises the Present*, 8 n.37 (2004), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/advertising-kidsand-ftc-regulatory-retrospective-advises-present/040802adstokids.pdf. ("Former FTC Chairman Pertschuk characterizes the Post editorial as a turning point in the Federal Trade Commission's fortunes.").

To that end, we herein provide a more in-depth historical analysis of the FTC's enforcement authority, including an examination of the problems that have arisen due to the FTC's current procedural issues. We detail how the FTC has utilized data-driven guidance in other contexts — namely the aforementioned Green Guides — to guide businesses through empirical analysis of available data. Finally, we use that historical context to frame ways that Congress can help urge the FTC to provide the same types of empirical guidance to the tech industry. Finally, I will discuss the underlying issues with the FTC's *very* low pleading standard and examine ways that Congress can address this problem.

## Background of FTC Enforcement in the Digital Economy

While the FTC began studying online privacy issues as early as 1995,[27] the FTC truly started dealing with consumer protection issues related to the Internet in 1997 — settling a series of assorted cases before, in 2001, it brought its first data security enforcement action premised on deception, settled against Eli Lilly in 2002.[28] In 2005, the FTC brought its first data security action premised on unfairness against BJ's Wholesale Club.[29] According to the FTC's most recent Privacy & Data Security Update, the Commission has brought over 60 data security cases since 2002, over 40 general privacy cases, and over 130 spam and spyware cases.[30] Yet, as discussed, rather than promulgate rules or provide any clear guidance, the FTC has instead chosen to approach the issue through case-by-case enforcement actions, almost always ending in consent decrees, which only focus on prospective requirements of the specific defendant in that case.[31] the FTC truly started dealing with consumer protection issues related to the Internet in 1997 — settling a series of assorted cases before, in 2001, it brought

---

[27] *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 2 (June 1998), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [hereinafter 1998 FTC Privacy Report] ("In April 1995, staff held its first public workshop on Privacy on the Internet, and in November of that year, the Commission held hearings on online privacy as part of its extensive hearings on the implications of globalization and technological innovation for competition and consumer protection issues."); *see also* FED. TRADE COMM'N, A REPORT FROM THE FEDERAL TRADE COMMISSION STAFF: THE FTC'S FIRST FIVE YEARS PROTECTING CONSUMERS ONLINE (Dec. 1999), *available at* https://www.ftc.gov/sites/default/files/documents/reports/protecting-consumers-online/fiveyearreport.pdf.

[28] *See* Press Release, Fed. Trade Comm'n, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), *available at* https://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach.

[29] See Complaint, In re BJ's Wholesale Club, Inc. (F.T.C. Sept. 20, 2005) (No. C-4-4148), available at https://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305comp0423160.pdf; see also Michael D. Scott, The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?, 60 Admin. L. Rev. 127, 146 (2008) (discussing BJ's Wholesale Club enforcement action and use of unfairness prong).

[30] *See* Fed. Trade Comm'n, 2016 Privacy & Data Security Update (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016 (providing overview of various enforcement actions).

[31] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 n.22 (3d Cir. 2015).

its first data security enforcement action premised on deception, settled against Eli Lilly in 2002.[32] In 2005, the FTC brought its first data security action premised on unfairness against BJ's Wholesale Club.[33] According to the FTC's most recent Privacy & Data Security Update, the Commission has brought over 60 data security cases since 2002, over 40 general privacy cases, and over 130 spam and spyware cases.[34] Yet, as discussed, rather than promulgate rules or provide any clear guidance, the FTC has instead chosen to approach the issue through case-by-case enforcement actions, almost always ending in consent decrees, which only focus on prospective requirements of the specific defendant in that case.[35]

In a speech last week, Acting Chairman Ohlhausen broadly summarized the "various types of consumer injury addressed in our privacy and data security cases" as "informational injury."[36] It's a useful shorthand: one term to describe a cluster of consumer protection problems behind a wide range of cases. But for the same reason, it's also a dangerous term — one that could, like "net neutrality," take on a life its own, and serve to obscure and frustrate analysis rather than inform it.[37] Of course, Chairman Ohlhausen chose her words carefully:

> [L]et me also emphasize that this is not a discussion of the legal question of what constitutes a 'substantial injury' under our unfairness standard. My topic today

---

[32] *See* Press Release, Fed. Trade Comm'n, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), *available at* https://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach.

[33] See Complaint, In re BJ's Wholesale Club, Inc. (F.T.C. Sept. 20, 2005) (No. C-4-4148), available at https://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305comp0423160.pdf; see also Michael D. Scott, The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?, 60 Admin. L. Rev. 127, 146 (2008) (discussing BJ's Wholesale Club enforcement action and use of unfairness prong).

[34] *See* Fed. Trade Comm'n, 2016 Privacy & Data Security Update (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016 (providing overview of various enforcement actions).

[35] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 n.22 (3d Cir. 2015).

[36] Maureen K. Ohlhausen, Acting Chairman, Fed. Trade Comm'n, Painting the Privacy Landscape: Information Injury in FTC Privacy and Data Security Cases, Address Before the Federal Communications Bar Association (Sept. 19, 2017), https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf [hereinafter Ohlhausen, *Informational Injury Speech*].

[37] Larry Downes, *The Tangled Web of Net Neutrality and Regulation*, Harvard Business Review (March 31, 2017), *available at* https://hbr.org/2017/03/the-tangled-web-of-net-neutrality-and-regulation ("Despite being a simple idea, net neutrality has proven difficult to translate into U.S. policy. It sits uncomfortably at the intersection of highly technical internet architecture and equally complex principles of administrative law. Even the term "net neutrality" was coined not by an engineer but by a legal academic, in 2003."). Gerard Stegmaier, a veteran attorney in the field of data security and privacy, explained it as such: "Words matter. Net Neutrality. Deep Packet Inspection. #Privacy. Businesses beware. There's a new label in town from the gov't and repeating it could have significant unintended consequences. From a speech yesterday the @FTC acting chair declared "informational injuries" exist. Let that sink in." Posting of Gerard Stegmaier on LinkedIn.com (Sept. 20, 2017), *available at* https://www.linkedin.com/feed/update/urn:li:activity:6316291846356115456 (also on file with author).

> may inform the substantial injury question, but I am speaking more broadly. Indeed, many of the cases I will mention are deception cases, or allege both deception and unfairness.
>
> …
>
> In my review of our privacy and data security cases, I have identified at least five different types of consumer informational injury. Certain of these types are more common. Many of our cases involve multiple types of injury. Courts and FTC cases often emphasize *measurable* injuries from privacy and data security incidents, although other injuries may be present. And to be clear, not all of these types of injury, standing alone, would be sufficient to trigger liability under the FTC Act. [38]

It is fitting that she should emphasize the word "measurable" — and also caveat it with the word "often" — because both speak to the central question facing the Federal Technology Commission as it grapples with an endless, and accelerating, parade of novel consumer protection issues: *how* does the agency determine what the right answer is in any particular case and what should be done about it? Ohlhausen defended the FTC's approach to privacy and data security enforcement:

> Case-by-case enforcement focuses on real-world facts and specifically alleged behaviors and injuries. As such, each case integrates feedback on earlier cases from advocates, the marketplace and, importantly, the courts. This ongoing process preserves companies' freedom to innovate with data use. And it can adapt to new technologies and new causes of injury.[39]

Yes, the courts' "feedback" is "important." Indeed, in a reply brief the FTC expressly agreed with TechFreedom on this importance of courts' guidance when it said it "agrees that the field would be aided by a body of law that includes 'Article III court decisions.'"[40] Yet, such assertions of the importance of courts' "feedback" by the FTC seem empty given there has been precious little of it. Since 1997, not counting a handful of cases where the FTC sought

[38] Ohlhausen, *Informational Injury Speech*, *supra* note 36, at 2-3.

[39] Ohlhausen, Informational Injury Speech, supra note 36, at 2.

[40] Plaintiff's Response In Opposition to the Motion to Dismiss, F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014), aff'd, 799 F.3d 236 (3d Cir. 2015) (No. 2:13-CV-01887-ES-SCM) at 22, n. 8.

injunctive relief against absent defendants (generally foreign scammers), the FTC has litigated, even partially, only a handful of cases: *LabMD*,[41] *Wyndham Worldwide Corp.*,[42] *Amazon.com, Inc.*,[43] and *D-Link Systems, Inc.*[44] Thus, the way the FTC works today is a far cry from what the FTC said about how it would operate back in 1980:

> The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time. As the Supreme Court observed as early as 1931, the ban on unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the gradual process of judicial inclusion and exclusion.'"[45]

What former FTC Chairman Tim Muris said of the Commission in 1981 remains true today: "Within very broad limits, the agency determines what shall be legal. Indeed, the agency has been 'lawless' in the sense that it has traditionally been beyond judicial control."[46] As he noted in his 2010 testimony before a Senate Subcommittee, "the Commission's authority remains extremely broad."[47] What Commissioner Wright said of the FTC's competition enforcement — where the Commission differs from the DOJ in enforcing (in theory, anyway) the same substantive laws — is even more true of consumer protection:

> The combination of institutional and procedural advantages with the vague nature of the Commission's Section 5 authority gives the agency the ability, in some cases, to elicit a settlement even though the conduct in question very likely may

---

[41] LabMD, Inc. v. F.T.C., No. 1:14-CV-00810-WSD, 2014 WL 1908716, at *1 (N.D. Ga. May 12, 2014), *aff'd*, 776 F.3d 1275 (11th Cir. 2015).

[42] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 n.22 (3d Cir. 2015).

[43] *F.T.C. v. Amazon.com, Inc.,* 71 F. Supp. 3d 1158 (W.D. Wash. 2014).

[44] *Fed. Trade Comm'n v. D-Link Sys., Inc.*, No. 3:17-CV-00039-JD, 2017 WL 4150873, at *1 (N.D. Cal. Sept. 19, 2017).

[45] 1980 Unfairness Policy Statement, *supra* note 12 (quoting *FTC v. Raladam Co.*, 283 U.S. 643, 648 (1931)).

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

[47] *Hearing on Financial Services and Products: The Role of the Fed. Trade Commission in Protecting Customers, before the Subcomm. on Consumer Protection, Product Safety, and Insurance of the S. Comm. on Commerce, Science, and Transportation*, 111th Cong. 2 (2010) (statement of Timothy J. Muris, Former Chairman, Fed. Trade Comm'n) *available at* http://lawprofessors.typepad.com/files/muris_senate_testimony_ftc_role_protecting_consumers_3-17- 101.pdf.

> not [violate any law or regulation]. This is because firms typically prefer to settle a Section 5 claim rather than going through lengthy and costly administrative litigation in which they are both shooting at a moving target and have the chips stacked against them. Significantly, such settlements also perpetuate the uncertainty that exists as a result of the ambiguity associated with the Commission's [Section 5] authority by encouraging a process by which the contours of Section 5 are drawn without any meaningful adversarial proceeding or substantive analysis of the Commission's authority.[48]

Without the courts to demand rigor from the FTC in defining "measurable" harm, what should the Commission do? And what should Congress do?

Chairman Ohlhausen's speech represents a major step in the right direction — precisely because it promises to give more analytical rigor to the term "informational injury" than such generalizations generally have. She concludes:

> This analysis raises several important questions. Is this list of injuries representative? When do these or other informational injuries require government intervention? Perhaps most importantly, how does this list map to our statutory deception and unfairness authorities?
>
> These are critical and challenging questions. That's why I am announcing today that the FTC will host a workshop on informational injury on December 12 of this year. This workshop will bring stakeholders together to discuss these issues in depth. I have three goals for this workshop: First, better identify the qualitatively different types of injury to consumers and businesses from privacy and data security incidents. Second, explore frameworks for how we might approach quantitatively measuring such injuries and estimate the risk of their occurrence. And third, better understand how consumers and businesses weigh these injuries and risks when evaluating the tradeoffs to sharing, collecting, storing, and using information. Ultimately, the goal is to inform our case selection and enforcement choices going forward.[49]

Amen. This is the kind of workshop the FTC should have held two decades ago — and several more times since. The FTC has, in fact, conducted such workshops, collected empirical data,

---

[48] Joshua D. Wright, *Revisiting Antitrust Institutions: The Case for Guidelines to Recalibrate the Federal Trade Commission's Section 5 Unfair Methods of Competition Authority*, 4 CONCURRENCES: COMPETITION L.J. 1 at 3 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/siting-antitrust-institutions-case-guidelines-recalibrate-federal-trade-commissions-section-5-unfair/concurrences-4-2013.pdf.

[49] Ohlhausen, *Informational Injury Speech*, *supra* note 36 , at 9.

and issued corresponding guidance based upon rigorous empirical analysis in another context: the Green Guides first issued for environmental marketing in 1992, and updated three times since then.[50] As discussed below, these offer an excellent model for how the Commission could begin to take a more substantive approach to defining informational injury, while also providing clearer guidance to industry.

Congress should support and encourage this effort — by holding the FTC to the high standards set by its work on the Green Guides. If this effort represents a significant departure with the analytically flimsy, "know-it-when-we-see-it" approach the FTC has generally taken to "informational injury" cases thus far, both consumers and companies would benefit from clearer, better substantiated guidance. But this will not be an easy change to make; it will require a new degree of rigor in how the Bureau of Consumer Protection operates, and a new closeness in BCP's engagement with the Bureau of Economics.

At best, this could be the beginnings of a "law and economics" revolution in consumer protection law — of the sort that transformed competition law in decades past, has guided the Bureau of Competition since, and has informed the courts in their development of antitrust case law.

But at worst, this process could result in blessing the FTC's current approach with a veneer of analytical rigor that merely validates the status quo. The report that comes out of this process *could* resemble the reports the FTC has produced since the 2012 Privacy Report, which make broad recommendations as to what industry best practices should be, without any real analysis behind those recommendations or how they relate to the Commission's powers under Section 5.[51]

Chairman Ohlhausen's initial thoughtful framing suggests reason for optimism, but everything will depend on how she and whoever becomes permanent Chairman (if it is not her) execute on the plan. In any event, the Commission's own more recent experience with the

---

[50] *See* Fed. Trade Comm'n, *Environmental Friendly Products: FTC's Green Guides* (last visited Sept. 24, 2017), available at https://www.ftc.gov/news-events/media-resources/truth-advertising/green-guides ("The Green Guides were first issued in 1992 and were revised in 1996, 1998, and 2012. The guidance they provide includes: 1) general principles that apply to all environmental marketing claims; 2) how consumers are likely to interpret particular claims and how marketers can substantiate these claims; and 3) how marketers can qualify their claims to avoid deceiving consumers.").

[51] *See* BERIN SZÓKA & GEOFFREY A. MANNE, THE FEDERAL TRADE COMMISSION: RESTORING CONGRESSIONAL OVERSIGHT OF THE SECOND NATIONAL LEGISLATURE 57-60 (2016), *available at* http://docs.house.gov/meetings/IF/IF17/20160524/104976/HHRG-114-IF17-Wstate-ManneG-20160524-SD004.pdf [hereinafter White Paper].

Green Guides — to say nothing of the last 15 years of experience with data security and privacy — suggests that self-restraint is unlikely to prove sustainable, on its own, in disciplining the agency. Ultimately, the kind of analytical quality that has defined antitrust law, and has sustained the law and economics approach there, requires *external* constraints — namely, regular engagement with the courts and oversight by Congress.

To that end, a careful reassessment of the Commission's processes is long overdue. The last time Congress seriously reconsidered, and revised, the FTC's processes was in 1994.[52] The agency has not been reauthorized since 1996.[53] Congress should return to its habit — the default assumption prior to Ken Starr, Monica Lewinsky, and impeachment — of reauthorizing the FTC every two years and, each time, re-examining how well the agency is working. Modifications to the statute should not be made lightly, but they should also happen more often than once in a generation.

Last year, the House Committee on Energy and Commerce considered no fewer than seventeen bills regarding the FTC. The attached white paper, co-authored with Geoffrey Manne, Executive Director of the International Center for Law & Economics, surveys those bills and provides recommendations to Congress on how to approach them.[54] Together, they form a starting point for the Senate Commerce Committee to begin its work, but they do not cover many of the most important aspects of how the agency works. Given this Committee's extensive knowledge and expertise, we hope that this Committee, along with the broader Senate, should start its own work on FTC reform legislation afresh.

## II. Summary of Proposed Legislative Reforms

Rather than repeat the full analysis provided in the aforementioned white paper we presented to the House Energy & Commerce Committee last year, we have instead provided a short overview of how to consider thinking about the main issues we believe need to be addressed through legislation.

---

[52] Federal Trade Commission Act Amendments of 1994, Pub. L. 103-312, 108 Stat. 1691 (Aug. 26, 1994) *available at* http://uscode.house.gov/statutes/pl/103/312.pdf.

[53] Federal Trade Commission Reauthorization Act of 1996, Pub. L. 104-216, 110 Stat. 3019 (Oct. 1, 1996), *available at* http://uscode.house.gov/statutes/pl/104/216.pdf.

[54] *See generally* White Paper, *supra* note 51.

### A. The Common Carrier Exception

The FTC Act excludes "common carriers subject to the Acts to regulate commerce."[55] What this provision means will be crucial — especially for technology cases in the coming years — and merits clarification from Congress.

The Federal Communications Commission has proposed to undo its 2015 reclassification of broadband providers as common carriers.[56] Doing so will return the controversial issue of "net neutrality" to the Federal Trade Commission by restoring the FTC's jurisdiction over broadband providers — or rather, there *should* be a seamless transition to ensure that consumers remain protected. But a Ninth Circuit panel decision last year calls into question whether the FTC's jurisdiction will be fully restored,[57] creating the possibility that a company providing broadband service, once that service is no longer considered a common carrier service by the FCC, might still remain outside the jurisdiction of the FTC either because (1) that particular corporate entity also provides a common carrier service such as voice (which will remain subject to Title II of the Communications Act even after the FCC's proposes re-reclassification of broadband) or (2) another corporate entity under common ownership provides such a common carrier service. In short, the panel decision rejected the FTC's longstanding "activity-based" interpretation of the statute in favor of an "entity-based" interpretation. The Ninth Circuit granted rehearing of that decision earlier this year, effectively vacating the panel decision.[58]

At oral arguments last week, AT&T stuck by its general arguments for an entity-bases interpretation, but clarified two things.[59] First, it read the statute to turn on the common carrier or non-common carrier status of each specific corporate entity, so that the FTC's jurisdiction over Oath, for example, the company formed by the Verizon parent company after it acquired AOL and Yahoo! and merged them together, would not be affected by the fact that Verizon Wireless provides a common carrier voice service. Second, AT&T argued that the FCC has plenary jurisdiction to, as it did in the *Computer Inquiries*, mandate such structural separation to ensure that there is no gap in consumer protection between the FTC and FCC.[60]

---

[55] 15 U.S.C. § 45(a).

[56] Notice of Proposed Rulemaking, Restoring Internet Freedom, WC Docket No. 17-108, 32 FCC Rcd 4434 (2017), https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-60A1_Rcd.pdf.

[57] *Fed. Trade Comm'n v. AT & T Mobility LLC*, 835 F.3d 993 (9th Cir. 2016), *reh'g en banc granted sub nom*., *Fed. Trade Comm'n v. AT&T Mobility LLC*, 864 F.3d 995 (9th Cir. 2017).

[58] Fed. Trade Comm'n v. AT&T Mobility LLC, 864 F.3d 995 (9th Cir. 2017).

[59] United States Court of Appeals for the Ninth Circuit, *Fed. Trade Comm'n v. AT&T Mobility LLC*, 864 F.3d 995 (2017), Oral Arguments, *available at* https://www.youtube.com/watch?v=Rs8EQU-KIEw.

[60] *Id.* at 13:50.

It is impossible to predict how the Ninth Circuit might resolve this case, but it is safe to say that if the FCC issues its Third Open Internet Order this year, or even early next year, that decision might well come out before the Ninth Circuit's decision.

Congress should not assume that the Ninth Circuit will fully restore the FTC's activity-based interpretation of its jurisdiction, even though appears to be the most likely result of the case. Congress should, instead, consider quickly moving legislation that would codify that interpretation. Even if the Ninth Circuit en banc panel accepts AT&T's argument and simply narrows the panel decision, that would only solve part of the problem raised by the panel decision. Requiring structural separation between "edge" companies like Oath and broadband companies like Verizon *might* make business sense anyway, but it might not — especially given the ongoing push to restrict the sharing of consumer data *even among corporate affiliates under common ownership*. Furthermore, AT&T's argument would still raise serious questions about which agency will deal with net neutrality and other consumer protection concerns about broadband services once they are returned to Title I: it is difficult to see how the common carrier services provided by these companies, if only telephony, could be functionally separated from the broadband service. Would consumers have to deal with, and subscribe to, two separate services, each offered by a separate corporate entity?

The Ninth Circuit may, of course, reject AT&T's arguments completely, fully reverse the panel decision, and restore the FTC's activity-based interpretation completely. But it would be far better for Congress to resolve this question before the FCC revises the regulatory classification of broadband. It could do so in a one-sentence bill.

Of course, many have argued that the common carrier exception should be abolished, and the Protecting Consumers in Commerce Act of 2016 (H.R. 5239) would have done just that.[61] Simply restoring the activity-based exemption need not be permanent; it could be stop-gap measure that allows Congress time to consider whether to maintain the exemption.

### B. More Economic Analysis

As many commentators have noted, the FTC has frequently failed to employ sufficient economic analysis in both its enforcement work and policymaking. Former Commissioner Josh Wright summarized the problem pointedly in a speech entitled "The FTC and Privacy Regulation: The Missing Role of Economics," explaining:

> An economic approach to privacy regulation is guided by the tradeoff between the consumer welfare benefits of these new and enhanced products and services

[61] Protecting Consumers in Commerce Act of 2016, H.R. 5239, 114th Cong. (2016), *available at* https://www.congress.gov/bill/114th-congress/house-bill/5239/text.

> against the potential harm to consumers, both of which arise from the same free flow and exchange of data. Unfortunately, government regulators have instead been slow, and at times outright reluctant, to embrace the flow of data. What I saw during my time at the FTC is what appears to be a generalized apprehension about the collection and use of data – whether or not the data is actually personally identifiable or sensitive – along with a corresponding, and arguably crippling, fear about the possible misuse of such data.[62]

As Wright further noted, such an approach would take into account the risk of abuses that will cause consumer harm, weighed with as much precision as possible. Failing to do so can lead to significant problems, including creating disincentives for companies to innovate and create benefits for consumers.

Specifically, Congress or the FTC should require the Bureau of Economics to have a role in commenting on consent decrees[63] and proposed rulemaking,[64] and a greater role in the CID process. But the most effective ways to engage economists in the FTC's decisionmaking would be to raise the FTC's pleading standards and make reforms to the CID process designed to make litigation more likely: in both cases, the FTC will have to engage its economists more closely, either in order to ensure that its complaints are well-plead or to prevail on the merits in federal court.

### C. Clarification of the FTC's Substantive Standards

The FTC has departed in significant ways from both the letter and spirit of the 1980 Unfairness Policy Statement and the 1983 Deception Policy Statement. This is mainly due to the FTC essentially having complete, unchecked, discretion to interpret these policy statements as it sees fit — including the discretion to change course regularly without notice. The courts simply have not had the opportunity to effectively implement Section 5(n), nor has the FTC ever really chosen to constrain its own discretion in meaningful ways (as it has done with the Green Guides). Making substantive clarifications to Section 5 will not be adequate without *process* reforms to ensure that these clarifications are given effect over time. But that does not mean they would be without value.

---

[62] Remarks of Joshua D. Wright, *The FTC and Privacy Regulation: The Missing Role of Economics*, George Mason University Law and Economics Center (Nov. 12, 2015), *available at* http://masonlec.org/site/rte_uploads/files/Wright_PRIVACYSPEECH_FINALv2_PRINT.pdf.

[63] *See* White Paper, *supra* note 51, at 42-43.

[64] *See id*. at 98-100.

In order to clarify the FTC's substantive standards under Section 5, we would suggest the following key changes:

1. Codifying other key aspects of the 1980 Unfairness Policy Statement into Section 5 that were not already added by the addition of Section 5(n) in 1994;
2. Codifying the Deception Policy Statement, just as Congress codified the Unfairness Policy Statement in a new Section 5(n).[65] This issue is explored in greater depth in my 2015 joint comments with Geoffrey Manne on the FTC's settlement of its enforcement action with Nomi Technologies, Inc.[66] Specifically, in codifying the Deception Policy Statement, Congress should:
    a. Clarify — or require the FTC to propose clarifications of — when and how the FTC must establish the materiality of statements about products: it made sense to presume that all express statements were material in the context of traditional advertising: because each such statement was calculated to persuade users to buy a product. But the same cannot *necessarily* be said of the myriad other ways that companies communicate with users today, such as through online help pages or privacy policies (which companies are required to post online, if only by California law).
    b. Require the FTC to meet the requirements of Section 5(n) when bringing enforcement actions based on the "reasonableness" of a company's practices, such as data security.[67]
3. Codify the FTC's 2015 Unfair Methods of Competition Policy Statement, with one small modification: the FTC should be barred from going beyond antitrust doctrine.[68]

[65] *See* White Paper, *supra* note 51, at 21-28.

[66] *In the Matter of Nomi Technologies, Inc.*, Comments of the International Center for Law & Economics & TechFreedom, File No. 1323251 (May 26, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/05/00011-96185.pdf.

[67] *See infra* 69.

[68] *See* White Paper, *supra* note 51, at 28-30; Fed. Trade Comm'n, Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act (Aug. 13, 2015), available at https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf.

### D. Clarifying the FTC's Pleading Standards

Several courts have already concluded that the FTC's deception enforcement actions must satisfy the heightened pleading standards of Section 9(b) of the Federal Rules of Civil Procedure, which applies to claims filed in federal court that "sound in fraud."[69] As explained below, this requirement would not be difficult for the FTC to meet, since the agency has broad Civil Investigative powers that are not available to normal plaintiffs before filing a complaint.[70] There is no reason the FTC should not have to plead its deception claims with specificity.

The same can be said for unfairness claims, even though they do not "sound in fraud." In both cases, getting the FTC to file more particularized complaints is critical, given that the FTC's complaint is, in essentially all cases, the FTC's last word on the matter, supplemented by little more than a press release, and an aid for public comment.

Indeed, the bar should likely be *higher*, not lower for unfairness cases. The attached white paper recommends a preponderance of objective standard for unfairness cases.[71] The critical thing to note is that there is no statutory standard for settling FTC enforcement actions — so the standard by which the FTC really operates is the very low bar set by Section 5(b): "reason to believe that [a violation may have occurred]" and that "it shall appear to the Commission that [an enforcement action] would be to the interest of the public."[72] In addition to the substantive clarifications to the FTC's substantive standards, Congress must clarify either the settlement standard or the pleading standard, if not both.

### E. Encouraging More Litigation to Engage the Courts in the Development of Section 5 Doctrine and Provide More Authoritative Guidance

Litigation is important for two reasons. First, having to prove its case before a neutral tribunal forces analytical rigor upon the FTC and thus forces it to make better, more informed decisions. Second, court decisions will provide guidance to regulated companies on how to comply with the law that is necessarily more authoritative (since the FTC cannot simply overrule a court decision the way it can change its mind about its own enforcement actions

---

[69] Rombach v. Chang, 355 F.3d 164, 170 (2d Cir. 2004) ("In deciding this issue, several circuits have distinguished between allegations of fraud and allegations of negligence, applying Rule 9(b) only to claims pleaded under Section 11 and Section 12(a)(2) that sound in fraud.").

[70] *See infra* at 19.

[71] *See* White Paper, *supra* note 51, at 18-21.

[72] 15 U.S.C. § 45(b).

or guidance) and also likely (but not necessarily) more detailed and better grounded in the FTC's doctrines.

One major reason companies settle so often across the board is that the FTC staff has the discretion to force companies to endure the process of litigating through the FTC's own administrative process, first before an administrative law judge and then before the Commission itself, before ever having the opportunity to go before an independent, neutral tribunal. The attached white paper explore three options:[73]

1. "[E]mpower one or two Commissioners to insist that the Commission bring a particular complaint in Federal court. This would allow them to steer cases out of Part III either because they are doctrinally significant or because the Commissioners fear that, unless the case goes to federal court, the defendant will simply settle, thus denying the entire legal system the benefits of litigation in building the FTC's doctrines. In particular, it would be a way for Commissioners to act on the dissenting recommendations of staff, particularly the Bureau of Economics, about cases that are problematic from either a legal or policy perspective."[74]
2. Abolish Part III completely, as former Commissioner Calvani has proposed.[75]
3. Require the FTC to litigate in federal court while potentially still preserving Part III for the supervision of the settlement process and discovery.[76] Requiring the FTC to litigate all cases in federal court (as the SMARTER Act would do for competition cases[77]) might, in principle, prove problematic for the Bureau of Consumer Protection, which handles many smaller cases. Retaining Part III but allowing Commissioners to object to its use might strike the best balance.

### F. The Civil Investigative Demand Process

There are many reasons why companies do not litigate privacy and data security cases. Some of them are beyond the control of FTC or Congress — for example, the extreme sensitivity of these issues for companies. Studies by the Ponemon Institute found that "[d]ata breaches are more concerning than product recalls and lawsuits,"[78] with a company's stock price falling

[73] *See* White Paper, *supra* note 51, at 82-85.

[74] *Id.*

[75] *See id*. at 84-85.

[76] *Id.*

[77] Standard Merger and Acquisition Reviews Through Equal Rules Act of 2015, H.R. 2745, 114th Cong. (2015).

[78] PONEMON, DATA BREACH, *supra* note 5, at 6.

an average of 5% after a data breach is disclosed.[79] Witness the 30% hit Equifax took to its stock price upon revelation of its data breach.[80] Perhaps most illustrative of the sensitivity of these issues was the case of LabMD — a medical testing company and one of the handful of companies who dared litigate against the FTC — which ultimately went out of business due to litigation costs and reputational damage, even though the judge ultimately found that no consumer was injured.[81] But a very significant, if not the biggest, reason why companies reflexively, almost invariably settle their cases is that the process of the FTC's investigation can be punishment enough to make settlement seem more attractive. After enduring a burdensome investigative process, companies (especially start-ups) frequently lack additional resources to defend themselves and face an informational asymmetry given the intrusiveness inherent in the FTC's current process. Even Chris Hoofnagle, who has long advocated that the FTC be far more aggressive on privacy and data security, warns, in his new treatise on privacy regulation at the agency, that

> [T]he FTC's investigatory power is very broad and is akin to an inquisitorial body. On its own initiative, it can investigate a broad range of businesses without any indication of a predicate offense having occurred.[82]

This onerous the process inevitably leads to more false-positives as FTC staff becomes invested in fishing expeditions and force such consent decrees regardless of the actual harms on consumers.[83] Other systemic costs of this process include increased discovery burdens on (even blameless) potential defendants, inefficiently large compliance expenditures throughout the economy, under experimentation and innovation by firms, doctrinally questionable consent orders, and a relative scarcity of judicial review of Commission enforcement decisions. Ultimately, this phenomena distorts the FTC's consumer protection mission because the agency can self-select cases that are likely to settle and further its policy goals,

---

[79] *See* Help Net Security, *After a data breach is disclosed, stock prices fall an average of 5%* (May 16, 2017), https://www.helpnetsecurity.com/2017/05/16/data-breach-stock-price/ (detailing a study by Ponemon).

[80] Paul R. La Monica, *After Equifax apologizes, stock falls another 15%* (Sept. 13, 2017), *available at* http://money.cnn.com/2017/09/13/investing/equifax-stock-mark-warner-ftc-probe/index.html.

[81] *See, e.g.,* Cheryl Conner, *When The Government Closes Your Business*, Forbes (Feb. 1, 2014), https://www.forbes.com/sites/cherylsnappconner/2014/02/01/when-the-government-closes-your-business/#6e7c78971435; Dune Lawrence, *A Leak Wounded This Company. Fighting the Feds Finished It Off*, Bloomberg (April 25, 2016), https://www.bloomberg.com/features/2016-labmd-ftc-tiversa/ ("The one company that didn't settle with the FTC is LabMD. Daugherty hoped, at first, that if he were as cooperative as possible, the FTC would go away. He now calls that phase 'the stupid zone.'").

[82] Darren Bush, The Incentive and Ability of the Federal Trade Commission to Investigate Real Estate Markets: An Exercise in Political Economy, 20-21, available at http://www.antitrustinstitute.org/files/517c.pdf.

[83] *See* Geoffrey A. Manne, R. Ben Sperry & Berin Szoka, *In the Matter of Nomi Technologies, Inc.: The Dark Side of the FTC's Latest Feel-Good Case*, ICLE Antitrust & Consumer Protection Research Program White Paper 2015-1 (2015).

rather than choosing cases on the basis of stopping the most nefarious actors and truly protecting consumers. As even former FTC Commissioner Joshua Wright noted, such self-serving personal and agency goals may push agencies to pursue cases "with the best prospect for settlement, cases that will consume few investigative resources, settle quickly, and are more likely to result in a consent decree that provides a continuing role for the agency."[84] Thus, more than any other aspect of the FTC Act or the FTC's operations, it is here that reinvigorated congressional oversight is needed.

The attached white paper explores this topic in great depth. Specifically, we recommend:

1. Reporting on how the agency uses CIDs[85]
2. Making CIDs confidential by default and allowing companies to move to quash them confidentially.[86] Today, fighting an FTC subpoena means the FTC can make the fight public, which may have serious consequences for a company's brand and stock price.
3. Requiring a greater role for Commissioners and economists in supervising the discovery process.[87]

Ultimately, any examination of the FTC's processes should start with arguably the most sacred principle in the American judicial system: innocent until proven guilty. As the Supreme Court made clear in 1895, "[t]he principle that there is a presumption of innocence in favor of the accused is the undoubted law, axiomatic and elementary, and its enforcement lies at the foundation of the administration of our criminal law."[88] While it is inarguably true that these cases are very clearly not criminal, it is also true that these companies and their employees face the threat of losing their "life, liberty, and property" as a result of these actions, as evidenced by LabMD. Despite the Administrative Law Judge finding that "the evidence fails to show any computer hack for purpose of committing identity fraud," the employees of LabMD were nonetheless left without employment simply due to "speculation" by the FTC — a word that appeared seventeen times in the ALJ's decision.[89]

Given the sensitive nature of both the type of information involved in these cases, including financial and health information, as well as consumers' sensitivity to reports that their data

---

[84] D.H. Ginsburg & J.D. Wright, *Antitrust Settlements: The Culture of Consent, in* I. William E. Kovacic: An Antitrust Tribute – Liber Amicorum (Charbit et al. eds., February 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/antitrust-settlements-culture-consent/130228antitruststlmt.pdf.

[85] *See* White Paper, *supra* note 51, at 37-40.

[86] *Id.* at 46-48.

[87] *Id.* at 48-53.

[88] *Coffin v. United States*, 156 U.S. 432, 453 (1895).

[89] LabMD, Inc., No. 9357, 2015 WL 7575033, at *48 (MSNET Nov. 13, 2015), https://causeofaction.org/wp-content/uploads/2015/11/Docket-9357-LabMD-Initial-Decison-electronic-version-pursuant-to-FTC-Rule-3-51c21.pdf.

may be in jeopardy, it is of the utmost importance that Congress ensure that innocent businesses' reputations aren't irreparably damaged simply due to "speculation." To be clear: this is not to say that parties who are guilty of implementing nefarious practices should be protected from the court of public opinion. Indeed, as former Commissioner Wright alluded to, implementing processes that would, at the very least, require the FTC to plead its claims with specificity — and, ideally, subsequently prove it on the basis of data-driven standards — prior to dragging a companies' name through the mud would actually ensure the FTC was using its limited resources to *only* go after the worst actors, rather than merely those most likely to settle.

Requiring the FTC to first make a showing beyond "speculation" of harm it alleges before invoking its immensely broad investigatory power, would at least provide businesses and its employees with some level of protection before being labeled as having unsecure data practices and being forced to face the repercussions that inevitably come with such a label. In doing so, Congress would ensure one of the oldest maxims of law in democratic civilizations continues. As Roman Emperor Julian eloquently quipped in response to his fiercest adversary's statement that "Oh, illustrious Caesar! if it is sufficient to deny, what hereafter will become of the guilty?": "If it suffices to accuse, what will become of the innocent?"[90]

### G. Fencing-In Relief

The FTC has broad powers under Section 13(b) to include in consent decrees extraordinarily broad behavioral requirements that "fence in" the company in the future.[91] The courts have been exceedingly deferential to the FTC in applying these requirements, though at least one circuit court has rebuked the FTC's broad approach, as explained in the attached white paper.[92] Rather than attempting to limit how the FTC uses its 13(b) powers, Congress should focus on when Section 13(b) applies. As Howard Beales, former director of the Bureau of Consumer Protection, has argued, regarding deception:

> the Commission's use of Section 13(b) remedies should be reevaluated in light of the law's original purpose: [O]ne class of cases clearly improper for awarding redress under Section 13(b): traditional substantiation cases, which typically involve established businesses selling products with substantial value beyond the

[90] *Coffin v. United States*, 156 U.S. 432, 455 (1895).

[91] *See*, *e.g., Kraft, Inc. v. F.T.C.*, 970 F.2d 311, 326 (7th Cir. 1992) ("The F.T.C. has discretion to issue multi-product orders, so called 'fencing-in' orders, that extend beyond violations of the Act to prevent violators from engaging in similar deceptive practices in the future.") (citing *F.T.C. v. Colgate-Palmolive Co.*, 380 U.S. 374, 395 (1965)).

[92] *See* White Paper, *supra* note 51, at 73-75.

> claims at issue and disputes over scientific details with well-regarded experts on both sides of the issue. In such cases, the defendant would not have known ex ante that its conduct was "dishonest or fraudulent." Limiting the availability of consumer redress under Section 13(b) to cases consistent with the Section 19 standard strikes the balance Congress thought necessary and ensures that the FTC's actions benefit those that it is their mission to protect: the general public.[93]

The same logic goes for the kind of unfairness cases the FTC is bringing against high-tech companies, as Josh Wright noted in his dissent in the *Apple* product design case:

> The economic consequences of the allegedly unfair act or practice in this case — a product design decision that benefits some consumers and harms others — also differ significantly from those in the Commission's previous unfairness cases. The Commission commonly brings unfairness cases alleging failure to obtain express informed consent. These cases invariably involve conduct where the defendant has intentionally obscured the fact that consumers would be billed. Many of these cases involve unauthorized billing or cramming – the outright fraudulent use of payment information. Other cases involve conduct just shy of complete fraud — the consumer may have agreed to one transaction but the defendant charges the consumer for additional, improperly disclosed items. Under this scenario, the allegedly unfair act or practice injures consumers and does not provide economic value to consumers or competition. In such cases, the requirement to provide adequate disclosure itself does not cause significant harmful effects and can be satisfied at low cost. However, the particular facts of this case differ in several respects from the above scenario.[94]

The key point, as Wright argued, is that the Commission is increasingly using unfairness not to punish obviously bad actors or to proscribe conduct that merits *per se* illegality because it is inherently bad, but rather, conduct that presents difficult tradeoffs: How long should consumers remained logged in to an apps store to balance the convenience of the vast majority of users with the possibility that some users with children may find that their children make unauthorized purchases on the device immediately after the parent has logged in? How much, and what kind of, data security is "reasonable?" And so on. These reflect business decisions that are inevitable in the modern economy. The Commission might well be justified in declaring that a company has struck the wrong balance, but it should not treat them exactly as it would obvious fraudsters, who set out to defraud consumers.

---

[93] J. Howard Beales III & Timothy J. Muris, *Striking the Proper Balance: Redress Under Section 13(b) of the FTC Act*, 79 ANTITRUST L. J. 1, 6-7 (2013).

[94] Dissenting Statement of Commissioner Joshua D. Wright, In the Matter of Apple, Inc., FTC File No. 1123108, at 3 (Jan. 15, 2014), available at https://goo.gl/0RCC9E.

In order to deter the Commission from taking advantage of this frequent judicial deference by imposing such disconnected "fencing-in" remedies in non-fraud cases — which, of course, is compounded by the fact that most cases are never reviewed by courts at all — Congress should consider imposing some sort of minimal requirement that provisions in proposed orders and consent decrees be (i) reasonably related to challenged behavior, and (ii) no more onerous than necessary to correct or prevent the challenged violation.

### H. Closing Letters

While consent decrees might help companies understand what the FTC will deem illegal on a case-by-case basis, in unique fact patterns, closing letters could do the inverse, telling companies what the FTC will deem *not* to be illegal, which is potentially far more useful in helping companies plan their conduct. In the past, the FTC issued at least a few closing letters with a meaningful degree of analysis of the practices at issue under the doctrinal framework of Section 5(n).[95] But in recent years, the FTC has markedly changes its approach, issuing fewer letters and writing those it did issue at a level of abstraction that offers little real guidance and even less analysis.[96]

Rep. Brett Guthrie's (R-KY) proposed CLEAR Act (H.R. 5109) would require the FTC to report annually to Congress on the status of its investigations, including the legal analysis supporting the FTC's decision to close some investigations without action. This requirement would not require the Commission to identify its targets, thus preserving the anonymity of the firms in question.[97] Most importantly, the bill requires:

> (1) IN GENERAL.—The Commission shall, on an annual basis, submit a report to Congress on investigations with respect to unfair or deceptive acts or practices in or affecting commerce (within the meaning of subsection (a)(1)), detailing—
>
> (A) the number of such investigations the Commission has commenced;
>
> (B) the number of such investigations the Commission has closed with no official agency action;

[95] *Id.* at 40-43. *See, e.g.,* Letter from Joel Winston, Associate Director of Fed. Trade Comm'n to Michael E. Burke, Esq., Counsel to Dollar Tree Stores, Inc. (June 5, 2001) available at http://www.ftc.gov/sites/default/files/documents/closing_letters/dollar-tree-stores-inc./070605doltree.pdf .

[96] *See, e.g*., Letter from Maneesha Mithal, Associate Director of Fed. Trade Comm'n to Lisa J. Sotto, Counsel to Michael's Stores, Inc. (June 5, 2001) available at http://www.ftc.gov/sites/default/files/documents/closing_letters/michaels-storesinc./120706michaelsstorescltr.pdf.

[97] The Clarifying Legality and Enforcement Action Reasoning Act, H.R. 5109, 114th Cong. (2016) [hereinafter CLEAR Act] available at https://www.congress.gov/bill/114th-congress/house-bill/5109/text.

> (C) the disposition of such investigations, if such investigations have concluded and resulted in official agency action; and
>
> (D) for each such investigation that was closed with no official agency action, a description sufficient to indicate the legal ***and economic*** analysis supporting the Commission's decision not to continue such investigation, and the industry sectors of the entities subject to each such investigation.

This bill, with our proposed addition noted, would go a long way to improving the value of the FTC's guidance. Indeed, such annual reporting could form annual addenda to guidance that the FTC issues in the guidance it provides on informational injury modeled on the Green Guides. Although the Green Guides themselves do not involve such reporting, it would make sense in this context, where the FTC is regularly confronted with far more novel fact patterns each year.

### I. Re-opening Past Settlements

The FTC may, under its current rules, re-open past settlements at any time — subject only to the Commission's assertion about what the "public interest" requires and after giving companies an opportunity to "show cause" why their settlements should *not* be modified.[98] By contrast, courts require far more for re-opening their orders. The FTC has, in fact, proposed to re-open four settlements entered into in 2013 under the Green Guides. Congress should write a meaningful standard by which the FTC should have to justify re-opening past settlements. If the Commission continues on its current course, it will be able to use its settlements to bypass the procedural safeguards of notice-and-comment rulemaking.

## III. Reasonable Siblings: Background on Section 5 and Negligence

The FTC's enforcement authority is derived from Section 5 of the Federal Trade Commission Act (FTC Act), which declares unlawful "[u]nfair methods of competition in or affecting commerce" and "unfair or deceptive acts or practices in or affecting commerce."[99] Under the broad terms of Section 5, the FTC challenges "unfair methods of competition" through their

[98] 16 C.F.R. 3.72(b).

[99] 15 U.S.C.A. § 45 (West 2017).

antitrust division and "unfair or deceptive practices" through their consumer protection division.[100] In pursuing its consumer protection mission there are different standards for "unfair" and "deceptive" practices, with its unfairness authority being "the broadest portion of the Commission's statutory authority."[101] Indeed, this "unfairness" authority was initially unrestrained by any statutory definition,[102] and remained so until Congress added Section 5(n) in 1994. In addition to Section 5 authority, however, the FTC has also asserted violations of other statutes in its data security enforcement, most notably the Gramm-Leach-Bliley Act ("GLBA"),[103] Children's Online Privacy Protection Act ("COPPA"),[104] as well as regulations promulgated under those statutes.[105]

Congress intentionally framed the FTC's authority under Section 5 in the general terms "unfair" and "deceptive" to ensure that the agency could protect consumers and competition throughout all trade and under changing circumstances.[106] To be sure, this broad authority has not been lost on the FTC, who readily acknowledges that "Congress intentionally framed the statute in general terms," which the agency interprets to mean "[t]he task of identifying unfair methods of competition" as being "assigned to the Commission."[107] Despite the addi-

---

[100] *See generally* Justin (Gus) Hurwitz, *Data Security and the FTC's Uncommon Law,* 101 Iowa L. Rev. 955, 964 (2016) (discussing in great lengths the FTC's "common law" approach) [hereinafter Hurwitz, *Uncommon Law*].

[101] *Id*.

[102] *See Id*.; *see also* Statement of Basis and Purpose of Trade Regulation Rule 408, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (July 2, 1964) (setting the three-factor contours of the "unfairness" prong for the first time through application of Section 5 to cigarette advertisements).

[103] *See* Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.* (2012) ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to … protect the security and confidentiality of … customers' nonpublic personal information.").

[104] The Child Online Privacy Protection Act of 1998, 15 U.S.C. § 6501, *et seq* (1994 & Supp. IV 1998) (making it unlawful under § 6502(a)(1) "for an operator of a website or online service directed to children … to collect personal information form a child in a manner that violates the regulations prescribed under subsection (b) of this section."); *see also* Melanie L. Hersh, Is Coppa A Cop Out? The Child Online Privacy Protection Act As Proof That Parents, Not Government, Should Be Protecting Children's Interests on the Internet, 28 Fordham Urb. L.J. 1831, 1878 (2001) (detailing how the FTC uses COPPA to regulate data security for children).

[105] *See, e.g.,* FTC Final Rule, 16 C.F.R. §§ 313.10–313.12 (2000); *Individual Reference Servs. Grp., Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 20 (D.D.C. 2001), *aff'd sub nom. Trans Union LLC v. F.T.C.*, 295 F.3d 42 (D.C. Cir. 2002) (holding that the FTC's final rule, promulgated under the GLBA "did not contravene plain meaning of Act and were permissible construction of that legislation" and "agencies' action in promulgating final rules was not arbitrary and capricious").

[106] *See* H.R. REP. NO. 63-1142, at 19 (1914) (Conf. Rep.) (observing if Congress "were to adopt the method of definition, it would undertake an endless task").

[107] Joshua D. Wright, Commissioner, Federal Trade Comm'n, Section 5 Recast: Defining the Federal Trade Commission's Unfair Methods of Competition Authority at the Executive Committee Meeting of the New York

tion of Section 5(n) to the Act in 1994 to *require* cost-benefit analysis, this lack of clear statutory guidance as to what constitutes "unfair" proved to be problematic, with at least one Commissioner recently recognizing that "nearly one hundred years after the agency's creation, the Commission has still not articulated what constitutes … unfair… leaving many wondering whether the Commission's Section 5 authority actually has any meaningful limits."[108] Commissioner Wright was referring to a lack of clarity around the meaning of unfairness in competition cases, but his point holds more generally.

Given the broad nature of Section 5, few industries are beyond the FTC's reach and the FTC has met the broad statutory language with an equally broad exercise of its authority to enforce Section 5.[109] The FTC has brought data security and privacy actions against advertising companies, financial institutions, health care companies, and, perhaps most significantly, companies engaged in providing data security products and services.[110] Further, not only are companies responsible for safeguarding their own data, but the FTC has also alleged that companies are responsible for any data security failings of their third-party clients and vendors, too.[111]

Companies who are the victims of such cyber-attacks are victims themselves. They suffer immense financial losses, stemming largely from reputational damage as customers are fearful of remaining loyal to companies who can't protect their personal and financial information.[112] According to one study, 76% of customers surveyed said they "would move away from companies with a high record of data breaches," with 90% responding that "there are

---

State Bar Association's Antitrust Section, 2 (June 19, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/section-5-recast-defining-federal-trade-commissions-unfair-methods-competition-authority/130619section5recast.pdf.

[108] *Id*.

[109] *See* Cho & Caplan, *Cybersecurity Lessons*; Stuart L. Pardau & Blake Edwards, The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity 12 J. Bus. & Tech. L. 227, 232 (2017) (discussing the FTC's enforcement of "everything from funeral homes, vending machine companies, telemarketing and mail marketing schemes, credit reporting, and the healthcare industry.") [hereinafter Pardau & Edwards, *New Legal Frontiers*].

[110] *See* Fed. Trade Comm'n, 2016 Privacy & Data Security Update (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016 (providing overview of various enforcement actions).

[111] *See id.* (For example, the consent decree agreed to in the FTC's enforcement action against Ashley Madison required the defendants to implement a comprehensive data-security program, including third-party assessments).

[112] *See generally* PONEMON, DATA BREACH; *see also Data breaches cost US businesses an average of $7 million – here's the breakdown*, Business Insider (April 27, 2017), http://www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4 (providing that the average cost of a data security breach is $7 million, with 76% of customers saying they would move away from companies with a high record of data breaches).

apps and websites that pose risks to the protection and security of their personal information."[113] Unquestionably, data security is the cornerstone of the digital economy and digitization of the physical economy. As Naveen Menon, President of Cisco Systems for Southeast Asia, put it "[s]ecurity is what protects businesses, allowing them to innovate, build new products and services."[114]

The recent Equifax breach illustrates just how strongly reputational forces encourage companies to invest in data security. As of the time this testimony was being written, Equifax's post-hack stock had plummeted 30%.[115] Given the enormous stakes for companies' brands, it is not difficult to understand why—with no clear guidance from Congress or the FTC—companies have opted to settle and enter into consent decrees rather than risk further reputational damage and customer loss through embarrassing and costly litigation.[116] Out of approximately 60 data security enforcement actions, only two defendants dared face an FTC armed with near absolute discretion as to the interpretation of "reasonable" data security practices. This hesitation to challenge the FTC in order to gain clarity from the courts about what actually constitutes unreasonable practices — in addition to the more obvious reason of escaping liability — was only reinforced by the *LabMD* case, where the company's decision to litigate against the FTC rather than enter into a consent decree led to its demise.[117]

Data security poses a unique challenge: unlike other unfairness cases, the company at issue is both the victim (of data breaches) and the culprit (for allegedly having inadequate data security). In such circumstances, the FTC should apply unfairness as more of a negligence standard than strict liability. Consider both a company that has been hacked and a business owner whose business has burned down. In both situations, it is very likely that employees and customers lost items they consider to be precious — perhaps even irreplaceable. Additionally, it is equally likely that neither *wanted* this unfortunate event to occur. Finally, in both situations, prosecutors would investigate the accident to determine the cause and as-

---

[113] *See* VANSONBOURNE, DATA BREACHES AND CUSTOMER LOYALTY REPORT (2015), http://www.vansonbourne.com/client-research/18091501JD.

[114] Naveen Menon, *There can be no digital economy without security*, World Economic Forum (May 8, 2017), https://www.weforum.org/agenda/2017/05/there-can-be-no-digital-economy-without-security/.

[115] *See, e.g.*, *Equifax Plummets After Huge Data Breach, Kroger Sinks on Profit drop, American Outdoor Brand Falls,* Yahoo Finance, Sept. 8, 2017, https://finance.yahoo.com/news/equifax-plummets-huge-data-breach-kroger-sinks-profit-drop-american-outdoor-brands-falls-144654294.html.

[116] *Id.*

[117] *Id.*

sess the damage and costs. However, under the FTC's current approach to Section 5 enforcement, how each business owner would be judged for liability purposes would vary greatly despite these similarities.

Under the common law of torts, absent some criminal intent (*e.g.*, insurance fraud) the businessman whose office burned down would only be held liable if he acted negligent in some way. At common law, negligence involves either an act that a *reasonable* person would know creates an unreasonable risk of harm to others.[118] Should a prosecutor or third party bring a lawsuit against the business owner, they would be required to put forth expert testimony and a detailed analysis showing exactly *how* and *why* the owner's negligence caused the fire.

Conversely, despite all of the FTC's rhetoric about "reasonableness" — which, as one might "reasonably" expect, should theoretically resemble a negligence-like framework — the FTC's approach to assessing whether a data security practice is unfair under Section 5 actually more closely resembles a rule of strict liability.[119] Indeed, rather than conduct any analysis showing that (1) the company owed a duty to consumers and (2) *how* that the company's breach of that duty was the cause of the breach — either directly or proximately— which injured the consumer, instead, as one judge noted, the FTC "kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes…."[120]

There is no level of prudence that can avert *every* foreseeable harm. A crucial underpinning of calculating liability in civil suits is that some accidents are unforeseeable, some damages fall out of the chain of causation, and mitigation does not always equal complete prevention. Thus our civil jurisprudence acknowledges that no amount of care can prevent *all* accidents (fires, car crashes, *etc*.), or at least the standard of care required to achieve an accident rate near zero would be wildly disproportionate, paternalistic, and unrealistic to real-world applications (*e.g.*, setting the speed limit at 5 mph).

The chaos theory also applies to the unpredictability of data breaches. Thus, if the FTC wants to regulate data security using a "common law" approach, then it must be willing to accept that certain breaches are inevitable and liability should only arise where the company was truly negligent. This is not simply a policy argument; it is the weighing of costs and benefits that Section 5(n) requires — at least in theory. Companies do not want to be hacked any

---

[118] *See* Restatement (Second) of Torts § 284 (1965).

[119] *See* Geoffrey A. Manne & Kristian Stout, *When "Reasonable" Isn't: The FTC's Standard-Less Data Security Standard*, Journal of Law, Economics and Policy, Forthcoming (Aug. 31, 2017), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3041533.

[120] Transcript of Proceedings at 91, 94–95, LabMD, Inc. v. Fed. Trade Comm'n, No. 1:14-CV-810-WSD, 2014 WL 1908716 (N.D. Ga. May 7, 2014).)).

more than homeowners want their houses to burn down. The FTC should begin its analysis of data security cases with that incentive in mind, and ask whether the company has acted as a "reasonably prudent person" would.

This, then, presents the key question: what constitutes "reasonably prudent" data security and privacy practices for purposes of avoiding liability under Section 5? To help inform Congress — and, in turn, the FTC — on how to go about answering this question, the remainder of this testimony will focus on determining three key elements of this question: (1) the types of injuries that should merit the FTC's attention, (2) the analytical framework, built upon empirical research and investigations, which should determine what constitutes "reasonable," and (3) the pleading requirements to determine the specificity with which the FTC must state its claim in the first instance.

## IV. Informational Injuries In Practice: Data Security & Privacy Enforcement to Date

In 2005, the FTC brought its first data security case premised solely on unfairness — against a company (BJ's Warehouse) not for violating the promises it had made to consumers, but for the underlying adequacy of its data security practices.[121] Whether this was a proper use of Section 5 is not the important question — although it is essential to note that *BJ's Warehouse* was the consent decree that launched the FTC's use of unfairness for data security.a thousand" more (or closer to "hundreds" in the context of privacy and data security). Even if one stipulates that the FTC could have, and likely *would* have, prevailed on the merits, had the case gone to trial, the important question is this: how might the Commission have changed its approach to data security? That question becomes even more salient if one tries to project back, asking what the Commission should have done then if it had known what we know today: that twelve years later, we would still not have a single tech-related unfairness case resolved on the merits (and only four that had made it to federal court).[122]

The Commission had, of course, asked Congress for comprehensive privacy legislation in 2000.[123] Besides asking again, what else could the Commission have done? It could have be-

[121] Fed. Trade Comm'n, *BJ's Wholesale Club Settles FTC Charges* (June 16, 2005), *available at* https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges.

[122] *See Fed. Trade Comm'n v. D-Link Sys., Inc.*, No. 3:17-CV-00039-JD, 2017 WL 4150873, at *1 (N.D. Cal. Sept. 19, 2017); *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236, 253 (3d Cir. 2015); *LabMD, Inc. v. F.T.C.*, No. 1:14-CV-00810-WSD, 2014 WL 1908716, at *1 (N.D. Ga. May 12, 2014), *aff'd,* 776 F.3d 1275 (11th Cir. 2015); *F.T.C. v. Amazon.com, Inc.,* 71 F. Supp. 3d 1158 (W.D. Wash. 2014).

[123] Fed. Trade Comm'n, *Privacy Online: Fair Information Practices in the Electronic Market Place- A Report to Congress* (2000) [hereinafter Privacy Report].

gun a rulemaking under the Magnusson-Moss Act of 1975, subject to the procedural safeguards imposed by Congress in 1980 (after the FTC's abuse of its rulemaking powers in the intervening five years). But, as many have noted, it would be difficult to craft prescriptive rules for data security or privacy in any rulemaking, and the process would have taken several years.

There *was* a third way: the FTC could have sought public comment on the issues of data security and privacy, issued a guidance document, then repeated the process every few years to update the agency's guidance to reflect current risks, technologies, and trade-offs. In short, the Commission could have followed the model established by its Green Guides.

## V. The Green Guides as Model for Empirically Driven Guidance

As the FTC proceeds with Chairman Ohlhausen's plans for a workshop on "informational injuries," it should consider its own experience with the Green Guides as a model. The parallel is not exact: the Guides focus entirely on deception, and primarily on consumer expectations, while the FTC's proposed "informational injuries" would involve both deception and unfairness. However, the Guides do still delve into substantiation of environmental marking claims, and, thus, the underlying merits of what companies were promising their customers. FTC guidance on the meaning of "informational injuries" in the context of data security and privacy would necessarily cover wider ground, ultimately attempting to understand harms as well as "reasonable" industry practices under both deception and unfairness prongs. Still, the Guides emphasis on empirical substantiation would serve the FTC well in attempting to provide a clearer analytical basis for *why* a practice or action is deemed to have caused "informational injury" in certain cases, rather than merely stating *what* practices the FTC has determined likely to cause such harm.

Though court guidance in this context may seem rarer than the birth of a giant panda, the Third Circuit nonetheless provided some insight into the value of previous FTC guidance — namely the FTC's 2007 guidebook titled "Protecting Personal Information: A Guide for Business," — in understanding harms and "reasonable" practices that constitute violations of Section 5.[124] Discussing this guidebook, which "describes a 'checklist[]' of practices that form a 'sound data security plan,'" the court notably found that, because "[t]he guidebook does not state that any particular practice is required by [Section 5]," it, therefore, "could not, on its own, provide 'ascertainable' certainty' of the FTC's interpretation of what specific cybersecurity practices fail [Section 5]."[125] Despite this recognition, the court still noted that the

[124] *Wyndham*, 799 F.3d at 256.

[125] *Id*. at 256 n.21.

guidebook did "counsel against many of the specific practices" alleged in that specific case, and thus, provided sufficient guidance in that very narrow holding to inform the defendant of "what" conduct was not considered reasonable.[126] Specifically, the court noted that the guidebook recommended:

> [T]hat companies "consider encrypting sensitive information that is stored on [a] computer network ... [, c]heck ... software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches." It recommends using "a firewall to protect [a] computer from hacker attacks while it is connected to the Internet," deciding "whether [to] install a 'border' firewall where [a] network connects to the Internet," and setting access controls that "determine who gets through the firewall and what they will be allowed to see ... to allow only trusted employees with a legitimate business need to access the network." It recommends "requiring that employees use 'strong' passwords" and cautions that "[h]ackers will first try words like ... the software's default password[ ] and other easy-to-guess choices." And it recommends implementing a "breach response plan," *id.* at 16, which includes "[i]nvestigat[ing] security incidents immediately and tak[ing] steps to close off existing vulnerabilities or threats to personal information."[127]

Most notably, nowhere in the court's discussion did it identify a single instance of the FTC explaining *why* a certain practice is necessary or reasonable; instead the FTC had merely asserted that companies should just accept the FTC's suggestions, without any consideration or analysis as to whether the immense costs that might be associated with implementing many of these practices are in the consumers' best interest. This is far from the weighing of costs and benefits that Section 5(n) requires. By comparison, the Green Guides, while focused on deception, reflect a deep empiricism about substantiation of environmental marketing claims, informed by a notice and comment process and distilled into clear guidance accompanied by detailed analysis.

While multi-national corporations such as Wyndham *might* (arguably) possess the resources to blindly implement any and all suggestions the FTC makes, and to follow the FTC's pronouncements in each consent decree, the economic principle of scarcity will inevitably require smaller businesses with vastly fewer resources to make difficult decisions as to which practices they should utilize to provide the greatest security possible with its limited resources. For example, using the list above, would a company with limited resources be acting "reasonable" if it implemented a "breach response plan," but failed to check *every* software vendors' website regularly for alerts? Further, would a company be engaging in "deceptive"

[126] *Id*. at 256-57.

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

practices if it failed to notify customers that, due to limited resources, it could only implement half of the FTC's recommended practices? The answer to these questions matter and will undoubtedly have significant consequences on how competitive small businesses remain in this country. As mentioned earlier, one study suggests that 76% of customers "would move away from companies with a high record of data breaches," with 90% responding that "there are apps and websites that pose risks to the protection and security of their personal information."[128] This shows that consumers are understandably concerned about how well a company protects their data. If a company is essentially required to choose between admitting that it lacks the resources to implement advanced security practices on par with large, established businesses, or risk an FTC action for "deception," how can any startup or small business expect to compete and grow in these polarizing circumstances?

Under the FTC's current enforcement standards, this all shows how easily small businesses may find themselves in a catch-22. On the one hand, if the business wishes to pretend it has the resources to implement the same data security standards as multi-national corporations in order to attract and maintain customers weary of their data being hacked, the business will be acting "deceptively" in the eyes of the FTC, and will be open to the costly litigation, reputational damage, and massive fines that come with it. On the other hand, if the small business wishes to be open and readily admit that, due to resource constraints, its data security practices are anemic when compared to multi-national corporations, it will be open to the loss of customers and businesses invariably linked to such claims. As this illustrates, how can any startup or small business expect to compete without the FTC providing guidance as to best practices based on empirical research — including economies of scale?

Thus, to ensure the ability of businesses to compete and make sound decisions as to the allocation of their finite resources, it is imperative that the FTC not only endeavor to provide guidance as to *what* practices are sound, but also explain *why* such practices are necessary, as well as "how much" is necessary, especially in relation to a business's size and available resources.

### A. The Green Guides (1992-2012)

First published in 1992, the Guides represented the Commission's attempt to better understand a novel issue before jumping in to case-by-case enforcement. By 1991, it was becoming increasingly common for companies to tout the environmental benefits of their products. In some ways, these claims were no different from traditional marketing claims: the FTC's job was to make sure consumers "got the benefit of the bargain." But in other ways, it was less

[128] *See* VANSONBOURNE, DATA BREACHES AND CUSTOMER LOYALTY REPORT (2015), http://www.vanson-bourne.com/client-research/18091501JD.

clear exactly what that "benefit" was — such as regarding recycling content, recyclability, compostability, biodegradability, refillability, sourcing of products, etc. Rather than asserting how much of each of these consumers *should* get, the Commission sought to ground its understanding of these concepts in empirical data about what consumers actually expected. As the Commission summarized its approach in the Statement of Basis and Purpose for the 2012 update:

> The Commission issued the Guides to help marketers avoid making deceptive claims under Section 5 of the FTC Act. Under Section 5, a claim is deceptive if it likely misleads reasonable consumers. Because the Guides are based on how consumers reasonably interpret claims, consumer perception data provides the best evidence upon which to formulate guidance. As EPA observed, however, perceptions can change over time. The Guides, as administrative interpretations of Section 5, are inherently flexible and can accommodate evolving consumer perceptions. Thus, if a marketer can substantiate that consumers purchasing its product interpret a claim differently than what the Guides provide, its claims comply with the law.[129]

Of course, as the Deception Policy Statement notes, "If the representation or practice affects or is directed primarily to a particular group, the Commission examines reasonableness from the perspective of that group."[130] Thus, the Commission immediately added the following:

> the Green Guides are based on marketing to a general audience. However, when a marketer targets a particular segment of consumers, such as those who are particularly knowledgeable about the environment, the Commission will examine how reasonable members of that group interpret the advertisement. The Commission adds language in Section 260.1(d) of the Guides to emphasize this point. Marketers, nevertheless, should be aware that more sophisticated consumers may not view claims differently than less sophisticated consumers. In fact, the Commission's study yielded comparable results for both groups.[131]

This bears emphasis because many speak of privacy-sensitive consumers as a separate market segment, and argue that we should apply deception in privacy cases based upon their expectations. But here, unlike in privacy, the Commission actually undertook empirical research — which turned not to support an idea that probably seemed intuitively obvious: that

---

[129] Fed Trade Comm'n, Statement of Basis and Purpose (2012 Update), *at* 24-25, https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-issues-revised-green-guides/greenguidesstatement.pdf [hereinafter "Statement of Basis and Purpose"].

[130] Fed. Trade Comm'n, FTC Policy Statement on Deception (Oct. 14, 1983), *at* 1, https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

[131] *See* Statement of Basis and Purpose, *at* 25.

more environmentally knowledgeable or "conscious" consumers had different interpretation of environmental marketing claims.

The Commission issued the first Green Guides in August 1992, thirteen months after two days of public hearings, including a 90-day public comment period in between. The Commission followed this process in issuing revised Green Guides in 1996, 1998, and 2012. So detailed was the Commission's analysis, across so many different fact patterns, that, while the 2012 Guides ran a mere 12 pages in the Federal Register,[132] the Statement of Basis and Purpose for them ran a staggering 314 pages.[133] In each update, the FTC explored how the previous version of the Guides addresses each, the FTC's proposal, comments received on the proposal and justification for the final rule. In short, the FTC was doing something a lot like rulemaking. Except, of course, the Guides are not themselves legally binding.

The FTC has never done anything even resembling this type of comprehensive guide for data security or privacy. Indeed, just this year, the FTC touted "a series of blog posts" as a grand accomplishment in the FTC's "ongoing efforts to help businesses ensure they are taking reasonable steps to protect and secure consumer data."[134] The FTC has regularly trumpeted its 2012 Privacy Report, but that document does something very different. Most notably, the Report calls on industry actors to self-police in the most general of terms, making statements like "to the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work."[135] Unlike the focus on substance and comprehensiveness of the Green Guides, the 2012 Privacy Report speaks in generalities, dictating "areas where the FTC will be active," such as in monitoring Do Not Track implementation or promoting enforceable self-regulatory codes.[136] The lack of a Statement of Basis and Purpose akin to that issued in updating the Green Guides (the 2012 Statement totaled a whopping 314 pages) introduces unpredictability into the enforcement process, and chills industry action on data security and privacy.

---

[132] 16 C.F.R. 260 (2012).

[133] *See generally* note *129*.

[134] Press Release, Fed. Trade Comm'n, Stick with Security: FTC to Provide Additional Insights on Reasonable Data Security Practices (July 21, 2017), https://www.ftc.gov/news-events/press-releases/2017/07/stick-security-ftc-provide-additional-insights-reasonable-data.

[135] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), *at* 73, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. [hereinafter "2012 Privacy Report"].

[136] *Id.* at 72.

In all, the Green Guides offer a clear, workable model for how the FTC could provide empirically grounded guidance on data security and privacy — even without any action by Congress. The key steps in issuing such guidance would be:

1. Study current industry practices across a wide range of businesses;
2. Gather data on consumer *expectations*, rather than making assumptions about consumer preferences;
3. Engage the Bureau of Economics and the FTC's growing team of in-house technologists in analysis of the costs and benefits of practice; and
4. Issue (at least) biennial or triennial guidance to reflect the changing nature, degree, and applicability of data security and privacy regulations.

Short of rulemaking, this rulemaking-like approach offers the most clarity, comprehensibility, and predictability for both FTC enforcement staff and industry actors.

## B. What the Commission Said in 2012 about Modifying the Guides

There is an obvious tension between conducting thorough empirical assessments to inform updating Commission guidance and how often that guidance can be updated: the more regular the update, the more difficult it will be to for the Commission to maintain methodological rigor in justifying that update. The 2012 Statement of Basis and Purpose noted requests that the Commission review and update the Guides every two or three years, but concluded:

> Given the comprehensive scope of the review process, the Commission cannot commit to conducting a full-scale review of the Guides more frequently than every ten years. The Commission, however, need not wait ten years to review particular sections of the Guides if it has reason to believe changes are appropriate. For example, the Commission can accelerate the scheduled review to address significant changes in the marketplace, such as a substantial change in consumer perception or emerging environmental claims. When that happens, interested parties may contact the Commission or file petitions to modify the Guides pursuant to the Commission's general procedures.[137]

This strikes a sensible balance. Unfortunately, this is not at all how the Commission has handled modification of the 2012 Green Guides. Within a year, the FTC would modify the Green guides substantially with no such process for empirical substantiation to justify the new change. And this year, not five years after the issuance of the Guides, it modified the Guides yet again.

[137] *See* Statement of Basis and Purpose, *at* 26-27.

## VI. Eroding the Green Guides and their Empirical Approach

While the Green Guides offer a model for empirically grounded consumer protection, the Commission has gradually moved away from that approach since issuing its last update to the Green Guides in 2012 — following an approach that more closely resembles its approach to data security and privacy.

### A. Modification of the Green Guides by Policy Statement (2013)

In 2013, FTC issued an enforcement policy statement clarifying how it would apply the Green Guides,[138] updated just the year after taking notice-and-comment, to architectural coatings such as paint. The Commission appended this Policy Statement onto its settlement with PPG Architectural Finishes, Inc. ("PPG") and The Sherwin-Williams Company ("Sherwin-Williams") to settle alleged violations of Section 5 for marketing paints as being "Free" of Volatile Organic Compounds (VOCs).[139] Specifically, the Policy Statement focused on application of the 2012 Green Guides' trace-amount test, which provided:

> Depending on the context, a free-of or does-not-contain claim is appropriate even for a product, package, or service that contains or uses a trace amount of a substance if: (1) the level of the specified substance is no more than that which would be found as an acknowledged trace contaminant or background level; (2) the substance's presence does not cause material harm that consumers typically associate with that substance; and (3) the substance has not been added intentionally to the product.[140]

The Policy Statement made two clarifications specific to architectural coatings:

> First, the "material harm" prong specifically includes harm to the environment and human health. This refinement acknowledges that consumers find both the environmental and health effects of VOCs material in evaluating VOC-free claims for architectural coatings.

---

[138] Fed. Trade Comm'n, Enforcement Policy Statement Regarding VOC-Free Claims for Architectural Coatings (Mar. 6, 2013), https://www.ftc.gov/sites/default/files/ documents/cases/2013/03/130306ppgpolicystatement.pdf.

[139] Press Release, Fed. Trade Comm'n, FTC Approves Final Orders Settling Charges Against The Sherwin-Williams Co. and PPG Architectural Finishes, Inc.; Issues Enforcement Policy Statement on "Zero VOC" Paint Claims (Mar. 6, 2013), https://www.ftc.gov/news-events/press-releases/2013/03/ftc-approves-final-orderssettling-charges-against-sherwin.

[140] 16 C.F.R. § 260.9(c) (2012).

> Second, the orders define "trace level" as the background level of VOCs in the ambient air, as opposed to the level at which the VOCs in the paint would be considered "an acknowledged trace contaminant." The harm consumers associate with VOCs in coatings is caused by emissions following application. Thus measuring the impact on background levels of VOCs in the ambient air aligns with consumer expectations about VOC-free claims for coatings.[141]

In both respects, the Policy Statement amended the Green Guides — while purporting merely to mirror the Guides. Most notably, the Guides had always been grounded in claims about environmental harms. For example, the Statement of Basis and Purpose for the 2012 Update had said:

> In this context [the "free of" section of the Guides"], the Commission reminds marketers that although **the Guides provide information on making truthful environmental claims**, marketers should be cognizant that consumers may seek out free-of claims for non-environmental reasons. For example, as multiple commenters stated, chemically sensitive consumers may be particularly likely to seek out products with free-of claims, and risk the most grievous injury from deceptive claims.[142]

But now the FTC's enforcement framework would, for the first time, focus on "human health" as well. In principle, this is perfectly appropriate: after all, "Unjustified consumer injury is the primary focus of the FTC Act," as the Unfairness Policy Statement reminds us.[143] But note that the Commission was *not* bringing an unfairness claim — which would have required satisfying the cost-benefit analysis of Section 5(n). Instead, the Commission was bringing a pure deception claim, as with any Green Guides claim. But unlike deception cases brought under the Green Guides, the Commission provided none of the kind of empirical evidence about how consumers understood green marketing claims that had informed the Green Guides. The Commission did not seek public comment on this proposed enforcement policy statement, nor did it supply any such evidence of its own.

In short, the 2013 Policy Statement represented not merely a *de facto* amendment of the Green Guides, undermining the precedential value of the Guides and of all other FTC guidance documents, but a break with the empirical approach by which the FTC had developed

---

[141] Fed. Trade Comm'n, Enforcement Policy Statement Regarding VOC-Free Claims for Architectural Coatings, *at* 2, https://www.ftc.gov/sites/default/files/documents/public_statements/voc-free-claims-architectural-coatings/130306ppgpolicystatement.pdf.

[142] *See* Statement of Basis and Purpose, *at* 138 n. 469.

[143] 1980 Unfairness Policy Statement.

the Guides since 1992. This alone should call into question the FTC's willingness, in recent years, to ground consumer protection work in empirical analysis. But worse was yet to come.

### B. Modification of the Green Guides by Re-Opening Consent Decree (2017)

This July, Ohlhausen, now Acting Chairwoman, effectively proposed amending the FTC's Green Guides — first issued in 1992 and updated in 1996, 1998 and 2012 — via proposed consent orders issued to four paint companies accused of deceptively promoting emission-free or zero volatile organic compounds in violation of Section 5 of the FTC Act.[144] In the corresponding press release, the Commission said it plans to "propose harmonizing changes to two earlier consent orders issued in the similar PPG Architectural Finishes, Inc. (Docket No. C-4385) and the Sherwin Williams Company (Docket No. C-4386) matters," and plans to "issue orders to show cause why those matters should not be modified pursuant to Section 3.72(b) of the Commission Rules of Practice, 16 C.F.R. 3.72(b)," if the consent orders are finalized.[145]

This repeated, and compounded, the two sins committed by the FTC in 2013: (1) undermining the value of Commission guidance (here, both the 2012 Guides and the 2013 Enforcement Policy Statement) by reminding all affected parties that guidance provided one day can be changed or revoked the next and (2) failing to provide empirical substantiation for its new approach. To these sins, the Commission added two more: (3) revoking guidance that had been treated as authoritative, and relied upon, by regulated parties for the previous four years through a consent decree and (4) re-opening the two consent decrees to which the 2013 Enforcement policy was attached to "harmonize" them with the FTC's new approach. Revoking guidance treated as authoritative raises fundamental constitutional concerns about "fair notice." Re-opening consent decrees raises even more serious concerns about the FTC's process.

These concerns are reflected in recently proposed FTC settlements. In the 2013 PPG and Sherwin-Williams consent orders, the Commission specified the scope of its jurisdiction in Article II of the orders, stating:

---

[144] Press Release, Fed. Trade Comm'n, Paint Companies Settle FTC Charges That They Misled Consumers; Claimed Products Are Emission- and VOC-free and Safe for Babies and other Sensitive Populations, (July 11, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/07/paint-companies-settle-ftc-charges-they-misled-consumers-claimed.

[145] *Id.* at ¶ 13.

> IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, trade name, or other device, in connection with the manufacturing, labeling, advertising, promotion, offering for sale, sale, or distribution of any covered product in or affecting commerce, shall not make any representation, in any manner, expressly or by implication, regarding:
>
> A. The VOC level of such product; or
>
> B. Any other *environmental* benefit or attribute of such product,
>
> unless the representation is true, not misleading, and, at the time it is made, respondent possesses and relies upon competent and reliable scientific evidence that substantiates the representation.[146]

In the same orders, the Commission defined "trace" levels of VOCs as including a "human health" component, stating:

> 7. "Trace" level of VOCs shall mean:
>
> A. VOCs have not been intentionally added to the product;
>
> B. The presence of VOCs at that level does not cause material harm that consumers typically associate with VOCs, including but not limited to, harm to the environment or *human health*; and
>
> C. The presence of VOCs at that level does not result in concentrations higher than would be found at background levels in the ambient air.[147]

While the inclusion of language that specified health as a VOC-related hazard created no immediate substantive changes, it laid the groundwork for a broadening of what constitutes a legitimate claim under the definition of VOC. Specifically, this would mean that the FTC would only have to take one additional step to claim a VOC-related violation if a company did not meet some broad, amorphous standard of "human health" conceived by the FTC. In fact, the 2017 Benjamin & Moore Co., Inc., ICP Construction Inc., YOLO Colorhouse LLC, and Imperial Paints, LLC consent orders took this additional step in an updated Article II, stating:

> IT IS FURTHER ORDERED that Respondent …. must not make any representation, expressly or by implication … regarding:

---

[146] Fed. Trade Comm'n, *In the Matter of PPG Architectural Finishes, Inc.*, Agreement Containing Consent Order (Oct. 25, 2012), *at* 4, https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121025ppgagree.pdf; *see also* Fed. Trade Comm'n, *In the Matter of Sherwin-Williams Company*, Agreement Containing Consent Order (Oct. 25, 2012), *at* 4, https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121025sherwinwilliamsagree.pdf.

[147] *Id.* at 3.

A. The emission of the covered product;

B. The VOC level of the covered product;

C. The odor of the covered product;

D. *Any other health benefit or attribute* of, or risk associated with exposure to, the covered product, including those related to VOC, emission, or chemical composition; or

E. Any other environmental benefit or attribute of the covered product, including those related to VOC, emission, or chemical composition, unless the representation is non-misleading, including that, at the time such representation is made, Respondent possesses and relies upon competent and reliable scientific evidence that is sufficient in quality and quantity based on standards generally accepted in the relevant scientific fields, when considered in light of the entire body of relevant and reliable scientific evidence, to substantiate that the representation is true.

Given the nature and type of these products, it is possible that health-related hazards should have been included in these particular consent orders. This would imply that it is the specific context of these cases that serves as a justification for the inclusion of the health-related language. However, the harmonization of these new orders with the 2013 PPG and Sherwin-Williams orders would create new, broader obligations on those two companies. More generally, this would imply that the basis of the FTC's authority emanates not from the context in which the claim is brought, but instead from the very nature of VOCs, i.e. as newly-deemed health hazards.

As a general principle, this means that, under its deception authority, the FTC could create *ex post facto* justifications for expanding its enforcement powers arbitrarily and with no forward guidance. For example, although the voluminous 2012 Green Guides Statement of Basis and Purpose made no mention of health risks,[148] the Commission found a way to add it on to previous consent agreements in a unilateral, non-deliberative way. This places industry actors at the mercy of the FTC, which can alter previous consent orders based on present or future interpretations of "deception."

### C. Remember Concerns over Revocation of the Disgorgement Policy?

It is ironic that it should be this particular FTC that would modify a Policy Statement, which was treated as authoritative by regulated parties for four years and which was itself a surreptitious modification of a Guide issued through public notice and comment (and resulting

[148] *See generally* Statement of Basis and Purpose.

in a 314-page Statement of Basis and Purpose), through such summary means — given that Acting Chairman Ohlhausen had previously urged greater deliberation and public input in withdrawing a policy statement.

In July 2012, the FTC summarily revoked its 2003 Policy Statement on Monetary Equitable Remedies in Competition Cases (commonly called the "Disgorgement Policy Statement")[149] on a 2-1 vote.[150] Commissioner Ohlhausen, the sole Republican on the Commission at the time, objected: "we are moving from clear guidance on disgorgement to virtually no guidance on this important policy issue."[151] She also objected to the cursory, non-deliberative nature of the underlying process:

> I am troubled by the seeming lack of deliberation that has accompanied the withdrawal of the Policy Statement. Notably, the Commission sought public comment on a draft of the Policy Statement before it was adopted. That public comment process was not pursued in connection with the withdrawal of the statement. I believe there should have been more internal deliberation and likely public input before the Commission withdrew a policy statement that appears to have served this agency well over the past nine years.[152]

What then-Commissioner Ohlhausen said then about revocation of a policy statement remains true now about substantial modification of a policy statement (which is effectively a partial withdrawal of previous guidance): both internal debate and public input are essential. Burying the request for public comment in a press release about new settlements hardly counts as an adequate basis for reconsidering the 2013 Policy Statement — let alone modifying the 2012 Green Guides.

### D. What Re-Opening FTC Settlements Could Mean for Tech Companies

The Commission could have, at any time over the last twenty years, undertaken the kind of empirical analysis that led to the Green Guides, and published guidance about interpretation of Section 5, but never did so. Instead, the Commission issued only a series of reports making broad, general recommendations. In fact, in one of the only two data security cases not to

---

[149] Fed. Trade Comm'n, Policy Statement on Monetary Equitable Remedies in Competition Cases, 68 Fed. Reg. 45,820 (Aug. 4, 2003).

[150] Press Release, Fed. Trade Comm'n, FTC Issues Policy Statement on Use of Monetary Remedies in Competition Cases (July 31, 2003), available at http://www.ftc.gov/opa/2003/07/disgorgement.shtm.

[151] *See* Statement of Commissioner Maureen K. Ohlhausen Dissenting from the Commission's Decision to Withdraw its Policy Statement on Monetary Equitable Remedies in Competition Cases, *at* 2 (July 31, 2012), https://www.ftc.gov/public-statements/2012/07/statement-commissioner-maureen-k-ohlhausen-dissenting-commissions-decision.

[152] *Id.* at 2.

end in a consent decree, a federal district judge blasted the FTC's decision not provide *any* data security standards:

> No wonder you can't get this resolved, because if [a 20-year consent order is] the opening salvo, even I would be outraged, or at least I wouldn't be very receptive to it if that's the opening bid…. You have been completely unreasonable about this. And even today you are not willing to accept any responsibility…. *I think that you will admit that there are no security standards from the FTC*. You kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes…. [H]ow does any company in the United States operate when . . . [it] says, well, tell me exactly what we are supposed to do, and you say, well, all we can say is you are not supposed to do what you did…. *[Y]ou ought to give them some guidance as to what you do and do not expect, what is or is not required*. You are a regulatory agency. I suspect you can do that.[153]

In recent years, the Commission has proudly trumpeted its "common law of consent decrees" as providing guidance to regulated entities.[154] Now, everyone must understand that those consent decrees may be modified at any time, particularly those consent decrees that are ordered by the Commission (as opposed to a federal court). As the Supreme Court made clear, "[t]he Commission has statutory power to reopen and modify its orders at all times."[155] In order to reopen and modify an order, the Commission faces an incredibly low bar, having to merely show that it has "reasonable grounds to believe that public interest at the present time would be served by reopening."[156] Meanwhile, the FTC's consent decrees often stipulate that the defendant "waives… all rights to seek judicial review or otherwise challenge or contest the validity of the order entered pursuant to this agreement."[157]

---

[153] Transcript of Proceedings at 91, 94-95, LabMD, Inc. v. Fed. Trade Comm'n, No. 1:14-CV-810-WSD, 2014 WL 1908716 (N.D. Ga. May 7, 2014)) (emphasis added).

[154] Julie Brill, Comm'r, Fed. Trade Comm'n, "Privacy, Consumer Protection, and Competition," Address at the 12th Annual Loyola Antitrust Colloquium (Apr. 27, 2012), http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-consumer-protection-and-competition/120427loyolasymposium.pdf (stating the FTC consent decrees have "created a 'common law of consent decrees,' producing a set of data protection rules for businesses to follow").

[155] Atl. Ref. Co. v. F.T.C., 381 U.S. 357, 377 (1965).

[156] *Elmo Co. v. F.T.C.*, 389 F.2d 550, 552 (D.C. Cir. 1967), *cert. denied*, 392 U.S. 905 (1968).

[157] *See, e.g.,* Agreement Containing Consent Order at 3(C), In re Oracle, No. 132 3115 (F.T.C. Dec. 21, 2015), https://www.ftc.gov/system/files/documents/cases/151221oracleorder.pdf.

But in cases where the FTC needs a court to issue a consent decree (e.g., to obtain an injunction or restitution), if the FTC wishes to modify the decree, it must at least meet the requirements imposed by Federal Rule of Civil Procedure 60:[158] the FTC must meet a heightened pleading standard through a showing of, for example, "fraud," "mistake," or "newly discovered evidence" necessitating such a modification.[159] Furthermore, the FTC does not have the freedom to modify court ordered consent decrees "at any time," as with settlements, but must file a motion "within a reasonable time" — the same standard that applies to all litigants in federal court.[160]

Why should there be such radically different standards? It is true that violating court-ordered consent decrees can result in criminal liability penalties, while violating Commission-ordered consent decrees means only civil penalties — but those penalties may be significant. For example, in 2015, the FTC imposed a $100 million fine against Lifelock for violating a 2010 consent decree by failing to provide "reasonable" data security[161] — over eight times the amount of the company's 2010 settlement and two thirds of the company's entire revenue that quarter ($156.2 million).[162] In general, arbitrarily-imposed, post-hoc civil liability carries the risk of causing significant economic loss, reputational harm, and even business closure. For example, the Commission could re-open *all* its past data security and privacy cases to modify the meaning of the term "covered information." To the extent that companies are found to be in non-compliance with the new standard, they would be liable for prosecution to the full extent of the FTC's powers. Besides compromising the ability of existing industry actors to comply, invest, and grow, this would have the effect of deterring new actors from entering a data-based industry for fear of uncertainty and retroactive prosecution.

Congress should reassess the standard by which the FTC may reopen and modify its own orders. In doing so, it should begin with the question articulated long ago by the Supreme Court: "whether any thing has happened that will justify … changing a decree."[163] In answering this question, the Court made clear that "[n]othing less than a clear showing of grievous

---

[158] Fed. R. Civ. P. 60 (stating that "the court may relieve a party or its legal representative from a final judgment, order, or proceeding" for certain reasons, including "mistake," "newly discovered evidence," "fraud," and "any other reason that justifies relief.").

[159] Fed. R. Civ. P. 60(b).

[160] Fed. R. Civ. P. 60(c).

[161] Fed. Trade Comm'n, *LifeLock to Pay $100 Million to Consumers to Settle FTC Charges it Violated 2010 Order* (Dec. 17, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated.

[162] LifeLock, Inc., *LifeLock Announces 2015 Fourth Quarter Results* (Feb. 10, 2016), *available at* https://www.lifelock.com/pr/2016/02/10/lifelock-announces-2015-fourth-quarter-results-2/

[163] *United States v. Swift & Co*., 286 U.S. 106, 119 (1932).

wrong evoked by new and unforeseen conditions should lead us to change what was decreed ... with the consent of all concerned."[164] The reason for the Court's hesitation to modify consent decrees should be obvious: despite retaining the force of a court order, consent decrees are, at their core, stipulated terms *mutually* agreed to by the parties to the litigation, similar to traditional settlements of civil litigation. Thus, by choosing to settle and enter into consent decrees, "[t]he parties waive their right to litigate the issues involved in the case and thus save themselves the time, expense, and inevitable risk of litigation."[165]

In federal court, Rule 60 forces parties to show that circumstances have indeed changed enough to justify modification of a court order. However, having to only show that it believes the "public interest" would be served, the FTC essentially is not required to make *any* showing of necessity that would counterbalance the value of preserving the terms of the settlement. Given the enormous weight the FTC itself has placed upon its "common law of consent decrees," as a substitute both for judicial decisions and clearer guidance from the agency, Congress should find it alarming that the FTC is now undermining the value of that pseudo-common law.

Ultimately, allowing the FTC to modify such agreements without showing any real cause not only negates the value of such agreements to each company (in efficiently resolving the enforcement action and allowing the company to move on), but more systemically and perhaps more importantly, it diminishes the public's trust in the government to be true to its word. Procedure matters. When agencies fail to utilize fair procedures in developing laws, the public's faith in both the laws and underlying institutions is diminished. This, in turn, undermines their effectiveness and further erodes the public's trust in the legal institutions upon which our democracy rests.[166] Thus, even in instances where the policy behind the rule may be sound, a failure by the implementing agency to follow basic due process will undermine the public's faith and deprive businesses of the certainty they need to thrive.[167]

---

[164] *Id*.

[165] *Local No. 93, Int'l Asso. of Firefighters, etc. v. Cleveland*, 478 U.S. 501, 522 (1986) (quoting *United States v. Armour & Co.*, 402 U.S. 673, 681-682 (1971)).

[166] *See, e.g*, Pew Research Center, Beyond Distrust: How Americans View Their Government (2015) ("Only 19% of Americans today say they can trust the government in Washington to do what is right "just about always" (3%) or "most of the time" (16%).").

[167] *See, e.g., Nat'l Petroleum Refiners Ass'n v. F.T.C.*, 482 F.2d 672, 675–76 (D.C. Cir. 1973), cert. denied, 415 U.S. 951 (1974) (recognizing that "courts have stressed the advantages of efficiency and expedition which inhere in reliance on rule-making instead of adjudication alone," including in providing businesses with greater certainty as to what business practices are not permissible).

## VII. Better Empirical Research & Investigations

Why *doesn't* the FTC do more empirical research — the kind that went into the Green Guides? What should the process around, and following, its forthcoming workshop on "informational injuries" look like?

### A. What the FTC Does Now

Since 2013, the FTC has published each January an annual report titled the "Privacy & Data Security Update."[168] The 2016 Report[169] boasts the FTC's "unparalleled experience in consumer privacy enforcement[170]" and the wide spectrum of offline, online, and mobile privacy practices that the Commission has addressed with enforcement actions:

> [The FTC] has brought enforcement actions against well-known companies, such as Google, Facebook, Twitter, and Microsoft, as well as lesser-known companies. The FTC's consumer privacy enforcement orders do not just protect American consumers; rather, they protect consumers worldwide from unfair or deceptive practices by businesses within the FTC's jurisdiction.[171]

Given the far-reaching scope of the FTC's jurisdiction on Section 5 enforcement and the wide range of companies that have settled "informational injury" cases, one might expect the these annual "Updates" to do more than merely summarize the previous year's activities, and instead provide empirical research into the privacy and data threats facing consumers. By failing to do so, the Commission not only leaves businesses in the dark as to what constitutes "reasonable" practices in the Government's eyes, but fails to inform them of the best practices available to ensure that Americans' data and privacy is adequately protected.

For example, if the Commission is to proudly report that consumer protection was achieved from settling charges with a mobile ad network on the grounds that "[the company] deceived consumers by falsely leading them to believe they could reduce the extent to which the company tracked them online and on their mobile phones,"[172] that Commission's work should not have ended there as a single bullet-point of the Commission's many highlights. As an

---

[168] FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE: 2013 (June 2012), *available at* https://www.ftc.gov/policy/reports/policy-reports/commission-and-staff-reports?title=data+security&items_per_page=20.

[169] FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE: 2016 (Jan 2017), *available at* https://www.ftc.gov/reports/privacy-data-security-update-2016.

[170] *Id*. *at* 2.

[171] *Id*.

[172] *Id.*

enforcement agency with vast interpretive powers on deceptive practices, and an investigative body with considerable analytical resources, the Commission has a further duty to clearly explain the empirical rationale that substantiates the settlement: Just how do consumers understand privacy in the use of advertising cookies? How might companies use Do Not Track signals, given those consumer expectations, to provide an effective opt-out mechanism? How should the standard differ based on the sizes of companies and the services they provide? What "informational injuries" occur when consumers unknowingly receiving tailored advertisements through the use of unique device identifiers? It is one thing to say that the Commission should not have to answer all these questions in its pleadings, or even in order to prevail in a deception case. It is quite another to say that the Commission should not be expected to perform any research even after the fact, especially on matters that recur across a larger arc of enforcement actions.

Unforeseen vulnerabilities are the inevitable side-effect of rapid technological advancements; in the area of data privacy and security, new consumer risks will arise continually, raising questions that *should* merit careful quantitative and qualitative analyses. However, in its "Privacy & Data Security Update," the FTC essentially asserts an answer without "showing its work."

This is in stark comparison to the FTC's approach on the Green Guides, where "the Commission sought comment on a number of general issues, including the continuing need for, and economic impact of, the Guides, as well as the Guides' effect on environmental claims":[173]

> [B]ecause the Guides are based on consumer understanding of environmental claims, consumer perception research provides the best evidence upon which to formulate guidance. The Commission therefore conducted its own study in July and August of 2009. The study presented 3,777 participants with questions calculated to determine how they understood certain environmental claims. The first portion of the study examined general environmental benefit claims ("green" and "eco-friendly"), as well as "sustainable," "made with renewable materials," "made with renewable energy," and "made with recycled materials" claims. To examine whether consumers' understanding of these claims differed depending on the product being advertised, the study tested the claims as they appeared on three different products: wrapping paper, a laundry basket, and kitchen flooring. The second portion of the study tested carbon offset and carbon neutral claims.[174]

Here is an excellent example of the FTC's use of consumer perception data to study the effect of environmental labels, with variables on consumer behavioral segments and changes on

[173] Statement of Basis and Purpose, *at* 8.

[174] *Id.* at 9-10.

perception over time, to substantiate deception claims. Even with the empirical research grounded in a large sample size, the Commission continued to reanalyze "claims appearing in marketing on a case-by-case basis because [the Commission] lacked information about how consumers interpret these claims."[175] The "Green Guides: Statement of Basis and Purpose"[176] is a 314 page document that comprehensively reviews the Commission's economic and consumer perception studies and weighs different empirical methodologies on the appropriate model of risk assessment. It meaningfully fleshes out the Green Guides' core guidance on the "(1) general principles that apply to all environmental marketing claims; (2) how consumers are likely to interpret particular claims and how marketers can substantiate these claims; and (3) how marketers can qualify their claims to avoid deceiving consumers," with self-awareness of the economic impact of regulations and a robust metric on consumer expectations to materialize the Commission's enforcement policies.

It is deeply troubling that this level of thoroughness evades the Commission's privacy enforcement, where the toolbox of economics remains unopened in managing the information flows of commercial data in boundless technology sectors pervading everyday life. The FTC's history of consent decrees provides nothing more than anecdotal evidence that *some* guiding principle is present, within the vague conceptual frameworks of "privacy by design," "data minimization", or "notice and choice."[177]" Data privacy and security regulations do not exist in a silo, abstracted and harbored from real-life economic consequences for the consumers, firms, and stakeholders—whose interests intersect at the axis of the costs and benefits of implementing privacy systems, the need for working data in nascent industries, and the market's right to make informed decisions. Consumer protection through privacy regulation is undoubtedly a matter of economic significance parallel to antitrust policies or the label marketing in the Green Guides. Personally identifiable information ("PII") is a valuable corporate asset like any other,[178] with competitive market forces affecting how it is processed, shared, and retained. Modern consumers are cognizant of the tradeoffs they make at the convenience of integrated technology services, and the downstream uses of their data. Accordingly, not every technical deviation from a company's privacy policy is an affront to consumer welfare that causes "unavoidable harms not outweighed by the benefits to consumers or competition."[179] The FTC has too long failed to articulate the privacy risks it intends to rectify, nor to

[175] *See* Statement of Basis and Purpose, *at* 27.

[176] *See generally* Statement of Basis and Purpose.

[177] *See generally* 2012 Privacy Report.

[178] Clearwater Compliance LLC, *The Clearwater Definition of an Information Asset*, https://clearwatercompliance.com/wp-content/uploads/2015/11/Clearwater-Definition-of-Information-Assets-with-Examples_V8.pdf.

[179] 12 U.S.C. § 5331(c)(1).

quantify the "material" consumer harm through behavioral economics or any empirical metric substantiated beyond its usual *ipso facto* assertion of deception.

### B. The Paperwork Reduction Act

A noteworthy legislation that defined the FTC's administrative authority after Congress imposed additional safeguards upon the FTC's Magnuson-Moss rulemaking powers in 1980 is the Paperwork Reduction Act of 1980 ("PRA").[180] These two 1980 enactments must be understood together as embodying Carter-era attempts to reduce the burdens of government. Specifically, Congress intended the PRA to serve as an administrative check on the Federal agency's information collection policy, with the goal of reducing paperwork burdens for individuals, businesses, and nonprofits by requiring the FTC to seek clearance from the Office of Management and Budget ("OMB") on compulsory process orders surveying ten or more members of the public.

The "collection of information" that falls under the constraints of the PRA is defined as:

> the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of form or format, calling for either— answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the United States.[181]

Some have claimed that the PRA has hampered the FTC's ability to collect data from companies and thus to perform better analysis of industry practices, informational injuries, and the like. The FTC's power to gather information *without* "a specific law enforcement purpose" derives from Section 6(b) of the FTC Act, which the FTC has summarized in relevant part as follows:

> Section 6(b) empowers the Commission to require the filing of "annual or special reports or answers in writing to specific questions" for the purpose of obtaining information about "the organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals" of the entities to whom the inquiry is addressed. [182]

---

[180] Paperwork Reduction Act of 1980, Pub. L. No. 96-511, 94 Stat. 2812 (codified as amended at 44 U.S.C. §§ 3501–3520 (2012)).

[181] 44 U.S.C. § 3502(3).

[182] Fed. Trade Comm'n, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority (July 2008), *available at* https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

Such reports would certainly be helpful for providing better substantiated guidance regarding data privacy and security practices. It is worth carefully considering what the PRA requires and how it might affect the FTC's collection of data. There is indeed some circumstantial evidence to suggest that the FTC may be structuring its 6(b) inquiries to avoid the PRA, by limiting the number of firms from which the FTC requests data to fewer than ten[183] — the threshold for triggering the PRA's requirements.

A case study on the FTC's survey of Patent Assertion Entities ("PAEs")[184] illustrates two potential ways the PRA might affect the FTC's collection of empirical data and thus the quality of its analysis and guidance in data security and privacy cases. First, by its own terms, the PRA applies even to *voluntary* data-collection of the sort that could allow the FTC compile "line of business" studies that consider wider practices beyond a single case:

> [T]he obtaining, causing to be obtained, soliciting, or requiring the disclosure to an agency, third parties or the public of information by or for an agency … *whether such collection of information is mandatory, voluntary, or required to obtain or retain a benefit.*[185]

The burden-minimization goal of the PRA is evaluated by the OMB based on broad, unpredictable criteria, such as whether the "the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility."[186] The PRA has been enforced by the OMB with tunnel vision on reducing the burden of paperwork and compliance, measured quite simply on the metric of man hours spent processing the paperwork.[187] However, the more important question lies on balancing the potential burden of information collection with the value of added research and empirical data on FTC policymaking. The balance was correctly struck on the Green

---

[183] *See e.g.*, FTC To Study Credit Card Industry Data Security Auditing Commission Issues Orders to Nine Companies That Conduct Payment Card Industry Screening (March 2016) https://www.ftc.gov/news-events/press-releases/2016/03/ftc-study-credit-card-industry-data-security-auditing;
FTC To Study Mobile Device Industry's Security Update Practices (May 2016) https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices.

[184] Layne-Farrar, Anne, What Can the FTC's §6(B) PAE Study Teach Us? A Practical Review of the Study's Methodology (March 1, 2016). Available at SSRN: https://ssrn.com/abstract=2722057. or http://dx.doi.org/10.2139/ssrn.2722057.

[185] 5 C.F.R. § 1320.3(c).

[186] United States Office of Personnel Management, Paperwork Reduction Act (PRA) Guide Version 2.0 (April 2011), available at https://www.opm.gov/about-us/open-government/digital-government-strategy/fitara/paperwork-reduction-act-guide.pdf.

[187] *Id. See also* Sam Batkins, Evaluating the Paperwork Reduction Act: Are Burdens Being Reduced? AAF, https://www.americanactionforum.org/testimony/evaluating-paperwork-reduction-act-burdens-reduced/.

Guides, where the PRA analysis was satisfied upon a consideration of the benefits of consumer surveys which outweighed the minimal burdens to the respondents:

> Overall burden for the pretest and questionnaire would thus be 2,511 hours. The cost per respondent should be negligible. Participation is voluntary and will not require start-up, capital, or labor expenditures by respondents.[188]

Moreover, the FTC integrated various suggestions on the study methodology and data collection methods submitted in a public comment by the General Electric Company ("GE"), to ensure that the Commission surveyed "a proper universe of consumers" upon which to "obtain accurate projections of national sentiment."[189]

> With respect to GE's concern about identifying the ''proper universe of consumers,'' FTC staff has included in the questionnaire a brief section of questions that address participants' level of interest in environmental issues. For example, one question asks: ''In the past six months, have you chosen to purchase one product rather than another because the product is better for the environment?'' Through analyses of answers to such questions, staff can compare the study responses of participants who have a high degree of interest in environmental issues and who take these issues into account when making purchasing decisions with responses of participants who are not as concerned with environmental issues.
>
> GE also asserts that the FTC should ensure a ''proper sample size.'' The FTC staff determined the sample size of 3,700 consumers based on several considerations, including the funds available for the study, the cost of different sample size configurations, the number of environmental claims to be examined, and a power analysis. In this study, 150 participants will see each of the various environmental marketing claims to be compared. Staff believes that this will be adequate to allow comparisons across treatment cells.[190]

By contrast, the FTC study on PAEs, which also received PRA clearance, compiled "nonpublic data on licensing agreements, patent acquisition practices, and related costs and revenues"[191] to illuminate how PAEs operate in patent enforcement activity outside the confines

---

[188] Fed. Trade Comm'n, Agency Information Collection Activities; Submission for OMB Review; Comment Request (May 2009), Federal Register / VOL. 74, NO. 90, *available at* https://www.ftc.gov/sites/default/files/documents/federal_register_notices/green-marketing-consumer-perception-study-agency-information-collection-activities-submission-omb/090512greenmarketing.pdf.

[189] *Id* at 22398.

[190] *Id*.

[191] *See* What Can the FTC's §6(B) PAE Study Teach Us? A Practical Review of the Study's Methodology (March 1, 2016); "Supporting Statement for a Paperwork Reduction Act: Part B" *available at* http://www.reginfo.gov/public/do/DownloadDocument?objectID=47563401.

of litigation records. But even when the OMB cleared the PAE study, the FTC chose a limited sample size of "25 PAEs, 9 wireless chipset manufacturers that hold patents, and 6 non-practicing wireless chipset patent holders."[192] This restrictive sample size significantly limited the applicability of the Commission's conclusions. More broadly, it suggests a shift towards a general reluctance to design and implement systemic research even when the required administrative blessing is obtained under the PRA.

The PRA Guide of 2011 outlines information collection policies and procedures, albeit with only a superficial explanation of statistical methodologies, and zero mention of survey design and quantitative research methods. [193] It is a cause for concern that the OMB's task of cutting down on the amount of paperwork is framed so parochially, for the short term goal of reducing participation hours, without perhaps considering cases where the quality and usability of the research itself depends on obtaining a larger sample. The mandate to limit the sample size of survey respondents ironically defeats the "practical utility" of the research, which is one of the main cornerstones of the PRA.

On the other hand, the PRA does not apply to *all* voluntary collection — only when the FTC sends "identical" questions to ten or more companies (whether their answer is voluntary or compulsory). The PRA would *not* apply to the FTC requesting public comment, such as it has done through the Green Guides process. This point is critical: while targeting specific companies with the same questions might well prove useful in informing the FTC's understanding of informational injuries, the FTC's failure to collect more such data thus far, to analyze it, and to publish it in useful guidance can in no way be blamed on the requirements of the PRA. Nor can it excuse the FTC staff for relying on an expert witness in the LabMD case whose recommendations about "reasonable" data security referred exclusively to the practices of Fortune 500 companies, without referencing *any* small businesses comparable in size and technical sophistication to LabMD.[194]

Indeed, the PRA Guide exempts from the definition of "information," and thus eliminates the need for clearance on, the collection of "facts or opinions submitted in response to general solicitations of comments from the general public"[195] and "examinations designed to test the

---

[192] *Id.*

[193] *See generally* Paperwork Reduction Act (PRA) Guide Version 2.0.

[194] Gus Hurwitz, *The FTC's Data Security Error: Treating Small Businesses Like the Fortune 1000* (Feb. 20, 2017), *available at* https://www.forbes.com/sites/washingtonbytes/2017/02/20/the-ftcs-data-security-error-treating-small-businesses-like-the-fortune-1000/#58d2b735a825.

[195] United States Office of Personnel Management, Paperwork Reduction Act (PRA), Version 2.0, OPM at 6 (April 2011), *available at* https://www.opm.gov/about-us/open-government/digital-government-strategy/fitara/paperwork-reduction-act-guide.pdf.

aptitude, abilities, or knowledge of the person tested for a collection."[196] The PRA poses no impediment to the FTC taking a proactive approach on conducting empirical research on data privacy by calling for consumer survey participants, holding public workshops, or from analyzing public data such as companies' privacy policies as a means to test privacy risk perception and consumer expectations. The Green Guides illustrate just how much data collection the FTC can do to substantiate its policymaking with empirical and economic research, based on real consumer studies.

## VIII. Pleading, Settlement and Merits Standards under Section 5

In general, the FTC Act currently sets a very low bar for bringing complaints: "reason to believe that [a violation may have occurred]" and that "it shall appear to the Commission that [an enforcement action] would be to the interest of the public."[197] In practice, this has become the standard for *settlements*, since the Act does not provide such a standard, and the FTC commonly issues both together. This raises three questions:

1. What should the standard be for issuing complaints?
2. Closely related, what should the standard be for courts weighing a defendant's motions to dismiss?
3. What should the standard be for settling cases?

Raising all three bars would do much to improve the quality of the agency's "common law" in several respects:

1. It would provide greater rigor for FTC staff throughout the course of the investigation;
2. Companies would be less likely to settle, and more likely to litigate, if they had a better chance of prevailing at the motion to dismiss stage; and
3. Complaints that settle before trial (after the FTC has survived a motion to dismiss) would, or complaints that the FTC has withdrawn (after the FTC has lost a motion to dismiss) would provide more guidance standing on their own as the final, principle record of each case.

We take the questions raised above in reverse order, beginning with the standard by which a court will assess a motion to dismiss and concluding with the standard by which Commissioners will decide whether to issue a complaint (and thus, in nearly every case, also a settlement):

[196] *Id*.

[197] 15 U.S.C. 45(b).

## A. Pleading & Complaint Standards

Fortunately, the courts are already moving towards requiring the FTC to do a better job of writing its pleadings (complaints) or face dismissal of its complaints — at least with respect to deception. Congress should take note of the current case law on this issue and consider codifying a heightened pleading requirement for any use of Section 5.

Heightened pleading standards can be fatal to normal plaintiffs, who need to survive a motion to dismiss in order to obtain the discovery they need to actually prevail on the merits. But the FTC has uniquely broad investigative powers. It is difficult to see why they would *ever* need court-ordered discovery — in other words, why would it be a problem for the Commission to have to do more to ground their complaints in the requirements of Section 5, as made clear in the FTC's Deception and Unfairness policy statements, and Section 5(n). Today, the FTC wants the best of both worlds: vast pre-trial discovery power *and* the low bar for pleadings claimed by normal plaintiffs who lack that power.

At a minimum, the FTC should be required to plead its Section 5 claims with specificity. Ideally, this standard would closely mirror a "preponderance of the evidence," as explained in the attached white paper.[198]

### 1. Deception Cases

TechFreedom has long argued that the FTC's deception complaints should have to satisfy the heightened pleading standards of Fed. R. Civ. Pro. 9(b).[199] Under that rule, "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake."[200] In other words, such claims must be accompanied by the "who, what, when, where, and how" of the conduct charged.[201] Rule 9(b) gives defendants "notice of the claims against them, provide[ ] an increased measure of protection for their reputations, and reduce[ ] the number of frivolous suits brought solely to extract settlements."[202]

Several district courts have concluded that 9(b) applies to FTC deception allegations.[203] Most recently, the Northern District of California dismissed two of the FTC's five deception counts

---

[198] *See* White Paper, *supra* note 51, at 18-21 (unfairness) and 28 (deception).

[199] *See* Brief of Amicus Curiae TechFreedom, International Center for Law and Economics, & Consumer Protection Scholars in Support of Defendants, *FTC. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-1887), 2013 WL 3739729, *available at* https://goo.gl/JGUE9e.

[200] Fed. R. Civ. P. 9(b).

[201] *Vess v. Ciba–Geigy Corp., USA*, 317 F.3d 1097, 1106 (9th Cir. 2003).

[202] In re Burlington Coat Factory Sec. Litig., 114 F.3d 1410, 1418 (3d Cir. 1997).

[203] *See, e.g.,* FTC v. Lights of Am., Inc., 760 F. Supp. 2d 848 (C.D. Cal. 2010); FTC v. Ivy Capital, Inc., 2011 WL 2118626 (D. Nev. May 25, 2011); FTC v. ELH Consulting, LLC, No. CV 12-02246-PHX-FJM, 2013 WL 4759267,

in its data security complaint against D-Link[204] for failure to satisfy the heightened pleading standard of Rule 9(b).[205] The district court noted that the Ninth Circuit has yet to address the question, but nonetheless found controlling the appeals court's decision holding that California's Unfair Competition Law — the state's "Baby FTC Act," which, "like Section 5 outlaws deceptive practices without requiring fraud as an essential element" — is subject to Rule 9(b).[206]

The *D-Link* court's analysis of each of the FTC's five deception counts illustrates that, while a heightened pleading standard *would* require more work from Commission staff to establish their cases, this burden would be relatively small and would in no way hamstring the Commission from bringing legitimate cases. The court upheld the principal deception count (Count II: "that DLS has misrepresented the data security and protections its devices provide") and two others, dismissing only two peripheral claims. If anything, merely applying Section 9(b) to the Commission's complaints would likely not be enough, on its own, to provide adequate discipline to the Commission's use of its investigation and enforcement powers — but it would certainly be a start.

The district court's discussion of Count II illustrates what specificity in pleading deception claims would look like. The FTC's allegations identified "specific statements DLS made at specific times between December 2013 and September 2015," and that the allegations "also specify why the statements are deceptive."[207] The court goes on to say that "Count II identifies the time period during which DLS made the statements and provides specific reasons why the statements were false—for example, that the routers and IP cameras could be hacked through hard-coded user credentials or command injection flaws," and that "this is all Rule 9(b) demands."[208]

---

at *1 (D. Ariz. Sept. 4, 2013) (same); *see also* FTC v. Swish Marketing, No. C-09- 03814-RS, 2010 WL 653486, at *2-4 (N.D. Cal. Feb. 22, 2010) (finding "a real prospect" that Rule 9(b) applies but not deciding the issue).

[204] *See* Complaint for Permanent Injunction and Other Equitable Relief, *Fed. Trade Comm'n v. D-Link Sys., Inc.*, No. 3:17-CV-00039-JD, 2017 (N.D. Cal. Sept. 19, 2017), 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.

[205] *See* Order Re Motion to Dismiss, *Fed. Trade Comm'n v. D-Link Sys.,* No. 3:17-CV-00039-JD, 2017 (N.D. Cal. Sept. 19, 2017), *at* 2-3, https://consumermediallc.files.wordpress.com/2017/09/dlinkdismissal.pdf.

[206] *Id.* at 2-3 (discussing Vess v. Ciba-Geigy Corp. USA, 317 F.3d 1097, 1103-04 (9th Cir. 2003)).

[207] *Id.* at 4.

[208] *Id.* at 4-5.

### 2. Unfairness Cases

The *D-Link* court noted that "[w]hether the FTC must also plead its unfairness claim under Rule 9(b) is more debatable," finding "little flavor of fraud in the[] elements [of unfairness under Section 5(n)]." But, the court continued:

> the FTC has expressly stated that the unfairness claim against DLS is not tied to an alleged misrepresentation. See Section III, below. At the same time, however, the FTC has said that for all of its claims "the core facts overlap, absolutely," and there is no doubt that the overall theme of the complaint is that DLS misled consumers about the data security its products provide. The FTC also acknowledges that DLS's misrepresentations are relevant to the unfairness claim because consumers could not have reasonably avoided injury in light of them.
>
> Consequently, there is a distinct possibility that Rule 9(b) might apply to the unfairness claim. But the question presently is not ripe for resolution. As discussed below, the unfairness claim is dismissed under Rule 8. Whether it will need to satisfy Rule 9(b) will depend on how the unfairness claim is stated, if the FTC chooses to amend.[209]

Whatever the courts actually conclude about the applicability of Rule 9(b) to unfairness claims, we see no reason why the Commission should not be subject to the same heightened pleading requirements under unfairness.

## B. Preponderance of the Evidence Standard

Applying Section 9(b) to all Section 5 pleadings would help greatly. But the more fundamental problem in unfairness cases is the low bar set by Section 5(b) for bringing a complaint — and the lack of *any* standard for settling it. We believe the answer is to require the Commission staff to demonstrate that it would prevail by a preponderance of the evidence. It may, at first, seem strange to apply this standard — the general standard for resolving civil litigation — at the early stages of litigation, but it must be remembered that this is not normal litigation. As noted above, the FTC has unique pre-trial discovery powers, and so is very likely to have accumulated all the evidence it will need at trial before the complaint is ever issued. Second, in nearly every "informational injury" case, the Commission's decision over whether to issue a complaint *is* the final decision over the case — because the cause will simply settle at that point. Congress should consider applying this standard either to the issuance of unfairness complaints, or to the issuance of settlements. If the standard is applied only to the issuance of settlements, Congress should consider some other heightened standard for

[209] *Fed. Trade Comm'n v. D-Link Sys.,* at *2 (N.D. Cal. Sept. 19, 2017).

bringing unfairness complaints, above that required by Section 9(b). In any event, the purpose of any standard imposed at this stage would not be to change how litigation would work — which would still be resolved under separate standards for motions to dismiss, motions for summary judgment and final resolution of litigation on the merits — but rather to spur Commissioners to demand more analytical work of the staff. Some such change is likely the only way to create sustainable analytical discipline inside the Commission.

## IX. Conclusion

There is little reason to expect that the FTC will not continue to more and more closely resemble the Federal Technology Commission with each passing year: the Commission will continue to grapple with new issues. This is just as Congress intended. But if the agency is to be trusted with such broad power, Congress should expect — and indeed take steps to ensure — that the FTC does more to justify how it wields that power. As Sens. Barry Goldwater (R-AZ) & Harrison Schmitt (D-AZ) said in 1980:

> Considering that rules of the Commission may apply to any act or practice "affecting commerce", and that the only statutory restraint is that it be unfair, the apparent power of the Commission with respect to commercial law is virtually as broad as the Congress itself. In fact, the Federal Trade Commission may be the second most powerful legislature in the country…. All 50 State legislatures and State Supreme Courts can agree that a particular act is fair and lawful, but the five-man appointed FTC can overrule them all. The Congress has little control over the far-flung activities of this agency short of passing entirely new legislation.[210]

This testimony, and the attached documents, lay out some of the ideas that Congress should consider in assessing how to reform the FTC's processes and standards. But these questions are sufficiently complex, and have been simmering for long enough, that the Committee would benefit from finding ways to maximize the input of outside experts.

One model for that would be the House Energy & Commerce Committee's ongoing #CommActUpdate effort.[211] The Committee has issued six white papers, each time taking public comment and refining its proposals. Given the complex interrelationships among the pieces of FTC reform, this would be a more constructive approach than having a flurry of separate bills, as Energy & Commerce did with FTC reform.

---

[210] S. Rep. No. 96-184, at 18 (1980), available at http://digitalcollections.library.cmu.edu/awweb/awarchive?type=file&item=417102.

[211] The Energy and Commerce Committee, #COMMSUPDATE (last visited Sept. 25, 11:00 AM), https://energycommerce.house.gov/commactupdate/.

The Committee could also consider establishing a blue-ribbon Commission modeled on the Antitrust Modernization Commission — as TechFreedom and the International Center for Law & Economics proposed in 2014:

> A Privacy Law Modernization Commission could do what Commerce on its own cannot, and what the FTC could probably do but has refused to do: carefully study where new legislation is needed and how best to write it. It can also do what no Executive or independent agency can: establish a consensus among a diverse array of experts that can be presented to Congress as, not merely yet another in a series of failed proposals, but one that has a unique degree of analytical rigor behind it and bipartisan endorsement. If any significant reform is ever going to be enacted by Congress, it is most likely to come as the result of such a commission's recommendations.[212]

We stand ready to assist the Committee in whatever approach it takes.

[212] Comments of TechFreedom & International Center for Law and Economics, In the Matter of Big Data and Consumer Privacy in the Internet Economy, Docket No. 140514424–4424–01, at 4 (Aug. 5, 2014), available at http://www.laweconcenter.org/images/articles/tf-icle_ntia_big_data_comments.pdf