File No. P175413

COMMENTS

of

WASHINGTON LEGAL FOUNDATION

to the

FEDERAL TRADE COMMISSION

Concerning

INFORMATIONAL INJURY WORKSHOP

Glenn G. Lammi
Cory L. Andrews
WASHINGTON LEGAL FOUNDATION
2009 Massachusetts Avenue, NW
Washington, DC 20036
(202) 588-0302

October 27, 2017

WASHINGTON LEGAL FOUNDATION
2009 Massachusetts Avenue, NW
Washington, DC 20036
(202) 588-0302

October 27, 2017

Submitted Electronically
Federal Trade Commission
Office of the Secretary
400 7th Street, SW
Fourth Floor, Suite 5610 (Annex A)
Washington, DC 20024

Re: Comments in Advance of FTC Public Workshop on Informational Injury

Dear Commissioners:

Washington Legal Foundation ("WLF") appreciates the opportunity to participate in the Federal Trade Commission's (the "FTC," the "Commission") public workshop on "informational injury." WLF has long encouraged the Commission to exercise its fact-finding and educational functions in the general area of consumer harm, specifically in the area of data security.

We are concerned, however, that the FTC is undertaking this worthwhile workshop under the rubric of assessing "informational injury," an amorphous and potentially new category of consumer harm. Our comments argue that the catch-all term conveys the impression that mere collection and availability of information, even public information, can constitute or cause an injury. In the course of conducting this workshop and related future activities, the FTC should specifically reject the concept of "informational injury" and focus instead on concrete consumer injuries that have some reasonable, non-speculative nexus with the defendant's conduct.

Next, we will suggest the legal framework the FTC should use to assess consumer privacy and data-security harms. We urge the Commission to respect Congress's intent that § 5 of the Federal Trade Commission Act ("FTC Act") be utilized only where *substantial* harm has occurred or is likely to occur (in unfair practices claims) or where the alleged consumer deception is material (in deception claims). We also explain why Commission staff should utilize a thorough, empirical assessment of consumer harm when determining whether any § 5 consumer-protection enforcement action is appropriate.

Finally, we argue that the FTC's enforcement activities must be conducted with the First Amendment rights of data producers and consumers squarely in mind.

I. Interests of WLF

Founded in 1977, WLF is a nonprofit, public-interest law firm and policy center based in Washington, DC, with supporters throughout the United States. WLF devotes a substantial portion of its resources to defending free enterprise, individual rights, limited government, and the rule of law. To that end, WLF regularly appears before federal administrative agencies, including the FTC, to ensure adherence to the rule of law.[1] Likewise, WLF has participated as *amicus curiae* in litigation challenging the scope of the FTC's regulatory authority under the FTC Act.[2] In addition, WLF's Legal Studies Division, the publishing arm of WLF, frequently produces articles and hosts discussions on a wide array of legal issues related to FTC activities.[3] WLF also encourages judicial and regulatory respect for the fundamental constitutional principle of "standing to sue," a key part of which is that the plaintiff suffered an "injury in fact."[4]

Finally, WLF is America's preeminent public-interest advocate for the commercial-speech rights of both businesses and consumers. Government regulators and other stakeholders in the debate over privacy and data-security have regrettably overlooked the First Amendment. In the past several years, WLF has worked to raise awareness in the courts and the public arena that because the sharing and dissemination of data constitutes speech, any government regulation of data's commercial uses must comport with the Constitution.[5]

---

[1] *See, e.g.*, Comments of Washington Legal Foundation, *In re: Proposed Consent Agreements and Request for Public Comments in Zero-VOC Paint Claims Cases*, File Nos. 1623079, 1623080, 1623081, & 1623082 (Sept. 11, 2017).

[2] *See, e.g., Ross v. FTC*, 135 S. Ct. 92 (2014) (challenging FTC's authority to obtain monetary restitution under § 13(b) of the FTC Act); *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015) (challenging the FTC's authority to regulate cybersecurity breaches under the "unfairness" prong of § 5 of the FTC Act).

[3] *See, e.g.*, Kurt Wimmer, *et al*., *Data Security Best Practices Derived from FTC § 5 Enforcement Actions*, WLF WORKING PAPER (Jan. 2017); John G. Greiner & Zoraida M. Vale, *FTC Intensifies Scrutiny of "Native Advertising,"* WLF LEGAL OPINION LETTER (Apr. 15, 2016); The Hon. Maureen K. Ohlhausen, John B. Morris, Jr., Katherine Armstrong, and Adam Thierer, *Online Privacy Regulation: The Challenge of Defining Harm*, WLF MEDIA BRIEFING, June 18, 2015.

[4] *See, e.g.*, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (challenging standing of a class of plaintiffs that had not suffered a concrete harm); Andrew C. Glass, Gregory N. Blase, Roger L. Smerage, and Hollee M. Watson, *In* Spokeo *Remand, Ninth Circuit Adopts Hybrid Approach to Statutory-Standing Analysis*, WLF LEGAL OPINION LETTER (Oct. 20, 2017).

[5] *See, e.g.*, *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011) (arguing that Vermont law which singled out commercial uses of prescription-drug-prescriber data as prohibited violated the First Amendment); Thomas R. Julin, *Confronting Online Privacy Regulation: Time to Defend the First Amendment*, WLF LEGAL BACKGROUNDER (May 27, 2016).

II. The Commission's Use of Its Fact-Finding Authority is Laudable

Public forums, workshops, and other events have long been an integral part of the FTC's "educate and inform" function. Such events educate not only the public, but also the Commission and its staff. The Commission has focused considerable resources and attention on data privacy, holding at least 16 public forums and workshops on the subject. It has not, however, focused such fact-finding on data security or on the threshold issue of how to measure consumer harm. For several years, WLF has been urging the FTC to pursue educational activities on data security,[6] as have other public-interest organizations.[7]

Ironically, the Commission's predominant approach when it comes to data security—arbitrary enforcement—undermines what minimal education and guidance work it has pursued. The FTC claims that the complaints, consent orders, and Commissioner statements arising from the Commission's dozens of unfairness actions comprise a body of data-security "common law" to which businesses must conform. Acting Chairman Ohlhausen reiterated this perspective in her September 19, 2017 speech announcing the "informational injury" workshop, in which she referenced the FTC's "body of decisions."[8]

WLF has argued previously that the FTC's approach to data-security enforcement is contrary to its statutory authority and the principle of constitutional due process.[9] FTC complaints and consent orders apply only to each targeted company and their unique situation, and they are not binding on third parties. The orders routinely point to a large number of factors which, taken together, are said to violate the FTC Act but which, taken individually or in some combination, may not. The orders leave third-party businesses in the dark as to which factors are most critical or which "failures" were fatal to the settling entity. Although the Third Circuit ultimately upheld the FTC's actions in *Wyndham Worldwide Corp.*, it recognized the significant shortcomings of a regulation-by-consent-decree approach to data security:

---

[6] *See, e.g.*, Glenn G. Lammi, *Education and Information Sharing: Underutilized Tools in FTC's Data Security Work*, WLF LEGAL PULSE, Sept. 16, 2014, https://wlflegalpulse.com/2014/09/16/education-and-information-sharing-underutilized-tools-in-ftcs-data-security-work/.

[7] Letter of Consumer Action, Consumer Federation of America, Privacy Rights Clearinghouse, and National Consumers League to FTC Chairwoman Ramirez, May 25, 2014, https://www.slideshare.net/nationalconsumersleague/data-security-letterftc.

[8] The Hon. Maureen K. Ohlhausen, *Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases*, before the Federal Communications Bar Association, Sept. 19, 2017, https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf.

[9] *See, e.g.*, Br. of *Amicus Curiae* Washington Legal Foundation, *FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. Oct. 14, 2014).

> 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.[10]

The FTC's decision to hold a workshop focusing on the threshold issue of injury in the data-security context is a promising step in the right direction.

III. "Informational Injury" Is an Inappropriate Focus for Workshop and Enforcement Activities

The concept of "informational injury" Acting Chairman Ohlhausen introduced in her September 19 Federal Communications Bar Association speech, however, somewhat tempers our enthusiasm for the December workshop. The Acting Chairman named five different kinds of "informational injuries": 1) deception; 2) financial injury; 3) health or safety injuries; 4) unwarranted intrusion; and 5) harm to reputation.

Each of these injuries requires more than just the existence or availability of "information." They all require intentional actions separate from the "information" that cause a particular type of injury long recognized in the common law. Therefore, the concept of "informational injury" as an umbrella term does not correctly capture the scope of the identified list of injuries that supposedly constitute "informational injuries." The Commission should be careful to avoid suggesting that the mere collection, use, and disclosure of "information" constitutes an injury in and of itself. If "information" is an injury, then a company could be responsible for any creation, use, disclosure, or availability of "information," with no consideration of whether the information caused a harm to consumers or whether the company's actions were intentional.

The FTC's cases addressing these five types of harms already frequently diverge from how courts treat similar causes of actions, particularly the requirements that plaintiffs prove causation and consumer injury. The use of the concept of "informational injury" would lead to further divergence. The common-law limitations of causation and consumer injury protect defendants from claims for which society has agreed defendants should not be held responsible. Absent such boundaries, the FTC's pursuit of "informational injury" cases is limited only by its prosecutorial discretion. Below, we discuss how the FTC has already diverged from how courts treat what the FTC suggested are "informational injuries."

---

[10] *Wyndham Worldwide Corp.*, 799 F.3d at 257, n.23.

Deception Injury. According to the FTC, deception injury occurs when a defendant has made a material statement that is false or misleading.[11] Even though deception is related to the common law of fraud, an FTC deception claim does not include several elements required under common law, including the need to prove reliance/causation and consumer harm. Some courts have identified nine independent elements to a fraud claim, which boil down to: there must be an intentional and material representation of fact that is false and is relied upon by a person in a way that injures that person.[12]

At common law, a plaintiff must allege more than simply a false statement to state a claim for fraud. The plaintiff also must allege reliance on the statement (*i.e.*, causation) and an injury (*e.g.*, typically economic injury such as overpaying for something). Under a fraud claim, if false statements are made but not heard by the consumer or they are not a factor in the consumer's decision to enter into a transaction with a company, there is no reliance, and thus no cognizable fraud claim.[13] Yet the FTC does not need to allege consumer reliance or injury when it brings complaints based on deceptive acts or practices. Under § 5, the courts have found that the FTC can bring a deception complaint when a statement is likely to mislead consumers acting reasonably under the circumstances in a way that is material.[14] According to the Ninth Circuit, the FTC is not even required to prove actual deception or reliance to find deception injuries from express statements, although actual evidence of deception and reliance supports a determination that a statement is likely to mislead consumers.[15]

---

[11] *See Uber Technologies, Inc.* 152 F.T.C. 3054 (2017); *Ashley Madison*, 152 F.T.C. 3284 (2016); *Snapchat, Inc.* 132 F.T.C. 3078 (2014).

[12] *See, e.g., Strategic Diversity, Inc. v. Alchemix Corp.*, 666 F.3d 1197, 1210 n.3 (9th Cir. 2012) ("The elements of common law fraud under Arizona law are: (1) A representation; (2) its falsity; (3) its materiality; (4) the speaker's knowledge of its falsity or ignorance of its truth; (5) his intent that it should be acted upon by the person and in the manner reasonably contemplated; (6) the hearer's ignorance of its falsity; (7) his reliance on its truth; (8) his right to rely thereon; (9) his consequent and proximate injury.").

[13] *See, e.g.*, *United States v. Luce*, No. 16-4093, 2017 WL 4768864, at *11 (7th Cir. 2017) (explaining fraudulent misrepresentation is a legal cause of loss due to reliance under the common law *only if* "the loss might reasonably be expected to result from the reliance.") (quoting RESTATEMENT (SECOND) OF TORTS § 548A (Am. Law. Inst. 1977)); *Sabrina Roppo v. Travelers Commercial Ins. Co.*, 869 F.3d 568, 591 (7th Cir. 2017) ("A plaintiff must believe the alleged misrepresentation to be true in order to state reliance.").

[14] *See, e.g., FTC v. Cyberspace.com LLC*, 453 F.3d 1196, 1199-1200 (9th Cir. 2006) (citing *FTC v. Gill*, 265 F.3d 944, 950 (9th Cir. 2001); *FTC v. Pantron I Corp.*, 33 F.3d 1088, 1095 (9th Cir. 1994)) ("As we have previously explained, a practice falls within this prohibition (1) if it is likely to mislead consumers acting reasonably under the circumstances (2) in a way that is material.").

[15] *Id*. at 1201 (citing *Trans World Accounts, Inc. v. FTC,* 594 F.2d 212, 214 (9th Cir.1979)) ("Although [p]roof of actual deception is unnecessary to establish a violation of Section 5, such proof is highly probative to show that a practice is likely to mislead consumers acting reasonably under the circumstances.") (internal quotes omitted).

Because the FTC need not prove reliance, it can and does review any statement by a company or its employees that may be a representation, whether found on a public website, in policies, or made during interviews. The Commission can then bring deception cases in which defendants cannot avoid liability by arguing lack of reliance/causation, perhaps the strongest defense they would normally have in a fraud case.

Financial, Health, or Safety Injury. Courts typically redress financial, health, and safety injuries if plaintiffs can show that the defendant proximately caused such injuries. The harm results from someone using information to steal money, steal a person's identity, or harass or abuse others. It is important to note that courts do not conclude that information itself is the cause of any loss or injury. Rather, plaintiffs must allege that the defendant's actions caused the alleged financial, health, or safety injury. As discussed above, the FTC's cases typically do not describe how the defendant's actions proximately caused consumer injury.

Unwarranted Intrusion Injury and Reputational Injury. Given the similarity in name to related privacy torts, one might think the FTC's approach in privacy and data-security cases mirrors the approach taken by courts when addressing privacy torts. Yet, not only does the FTC bring many privacy and data-security cases that have no relation to privacy torts, even when the FTC's case is similar to a privacy tort, the Commission does not conform to the elements of the privacy torts.

State statutes or common law generally categorize privacy-related violations into four distinct intentional torts: (1) intrusion into seclusion; (2) public disclosure of private facts; (3) false light; and (4) misappropriation of name or likeness. The unwarranted intrusion and reputational injuries identified by Acting Chairman Ohlhausen are similar to the torts of intrusion into seclusion and public disclosure of private facts, respectively. The tort of intrusion into seclusion is typically described as the intentional interference into the seclusion of another (or their private affairs or concerns) if that intrusion would be "highly offensive to a reasonable person."[16] The tort of intentional public disclosure of private facts involves a public disclosure of a private fact, not of legitimate concern to the public, which would be highly offensive to a reasonable person and result in harm from a damaged reputation.[17]

A primary difference between the FTC cases and court cases with similar facts is that the privacy torts are intentional torts, requiring a showing by the plaintiff of some volition by the defendant to violate the plaintiff's privacy interests. In contrast, the FTC

[16] RESTATEMENT (SECOND) OF TORTS § 652B.

[17] RESTATEMENT (SECOND) OF TORTS § 652D; *see also Cox Broadcasting Co. v. Cohn*, 420 U.S. 469 (1975).

does not look at intent. According to the FTC, an accidental exposure of information alone can be a violation of § 5.[18]

A second difference is that the privacy torts require a "private" element. Intrusion into seclusion requires the intrusion into "private" affairs or concerns. The tort of public disclosure of private facts requires that the information disclosed be "private." The FTC recognizes no such constraint. The Commission has brought § 5 cases when it finds that any type of personal information, even already public information, is vulnerable to exposure.[19] The FTC does not analyze whether the information involved is public or private information.

Therefore, when it brings enforcement actions, the FTC does not incorporate into its analysis key factors that plaintiffs would need to prove for a successful privacy-tort action. The factors the FTC does not consider are important, because they help prevent an abundance of questionable and vexing privacy-tort claims.

Even if the FTC is simply couching the five injuries under the catch-all, awkward rubric of "information injuries" with no aim to create a new category of harm, semantics matter when discussing and debating legal and policy issues. TechFreedom President Berin Szóka quite aptly expressed concern with "informational injury" in recent testimony before a U.S. Senate committee: "[I]t's … a dangerous term—one that could, like 'net neutrality,' take on a life of its own, and serve to obscure and frustrate analysis rather than inform it."[20] In her speech, Acting Chairman Ohlhausen stated that harms ranging from physical harm to reputational harm fall within the rubric of her catch-phrase, "informational injury." That is an astonishingly broad spectrum of injuries and, as will be discussed below, the legal framework the FTC should use to identify "substantial harm" would not view each of them as being equally significant or worthy of Commission enforcement resources.

To her credit, Acting Chairwoman Ohlhausen was careful in her speech to note such injuries had to be "measurable" and that "not all of these types of injuries, standing

---

[18] Many of the FTC's data-security cases are based on a defendant's failure to implement certain data security measures. There is typically no allegation that a defendant intentionally failed to implement such measure. *See e.g.*, Complaint, *FTC v. Wyndham Worldwide Corporation*, No. 2:12-cv-01365 (June 26, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/06/120626wyndamhotelscmpt.pdf ("As a result of the failures [to provide appropriate data security measures] intruders were able to gain unauthorized access to Hotels and Resorts' computer network…").

[19] *See e.g.*, Complaint, *In re Fandango*, Dkt. No. C-4481 (Mar. 28, 2014), https://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf (basing action on the potential for attackers to misuse of credit card information and authentication credentials).

[20] Testimony of TechFreedom, *FTC Stakeholder Perspectives: Reform Proposals to Improve Fairness, Innovation, and Consumer Welfare*, U.S. Senate Committee on Commerce, Science, and Transportation, Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, Sept. 26, 2017 at 8 (citation omitted).

alone, would be sufficient to trigger liability under the FTC Act."[21] But such cautionary language will not be carried forward with the "informational injury" catch-phrase. The FTC's continued use of the term could have a negative influence on other policy makers as they address data privacy and security. Class-action lawyers have been flooding federal and state courts with lawsuits seeking redress for perceived harm from privacy invasions and data breaches. They would certainly advance the broad concept of "informational injury" and cite to the FTC's use of it.

IV. The Legal Framework for Data-Security and Privacy Actions

A. "Unfair Acts and Practices" Claims

1. Critiquing the FTC's Interpretation of "Substantial Injury"

Section 5 of the FTC Act prohibits as "unfair" acts that "cause or are likely to cause substantial injury to consumers which is not unreasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition." The Commission has used this authority to bring claims against businesses that have been victimized by third parties such as hackers and foreign nation states.[22] The alleged unfair act is the business's failure to maintain what the Commission considers to be "reasonable" data protection, or the exposure of personal data.

The FTC's interpretation of when an injury is "likely" and "substantial," what amount of proof is needed to show causation, and how a cost-benefit analysis should be done are not entirely clear because the vast majority of data-breach unfairness claims have been resolved through consent decrees. Only three targets of such unfairness claims have forced the Commission to make its case in federal court. The two suits that are ongoing, *LabMD, Inc. v. FTC* and *FTC v. D-Link Systems, Inc.*, turn largely on whether substantial injury occurred. The most recent court decisions arising from these suits merit discussion as part of the "Informational Injury" workshop.

In the case against LabMD, Inc., the FTC claimed that peer-to-peer software on the company's computer shared records containing sensitive personal information. The FTC alleged, "A number of the SSNs [Social Security Numbers] in the Day Sheets are being, or have been, used by people with different names, which may indicate that the

---

[21] *Painting the Privacy Landscape*, *supra* note 8.

[22] *See, e.g.*, Eric Lipton, David E. Sanger & Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, NY TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html (discussing the alleged Russian hack of DNC servers); Patrick Thibodeau, *The Sony Breach May Be Start of New Nation-State Cyberattack*, COMPUTERWORLD (Dec. 18, 2014), https://www.computerworld.com/article/2860745/it-security-in-2015-were-now-at-war.html (discussing the possibility of North Korea's involvement in the Sony data breach).

SSNs have been used by identity thieves."[23] There was no allegation that any identity theft had actually occurred or that there was any actual injury to consumers. The only entity to obtain a copy of the LabMD file containing personal data was a data-security company, Tiversa, which used its successful breach of security as a tactic to pursue LabMD's business. When LabMD refused to hire Tiversa, Tiversa contacted the FTC, which filed a § 5 action.

An FTC Administrative Law Judge (ALJ) dismissed the FTC's case for failing to meet the standards of § 5. The FTC staff appealed to the Commissioners, who overturned the ALJ's decision. LabMD in turn appealed to the Eleventh Circuit which, on November 1, 2016, granted the company's motion to stay enforcement of the FTC's final order.[24]

The court held that the FTC's interpretation of § 5's "substantial injury" requirement as including intangible harms such as risk of reputational damage or emotional impact was unreasonable. It also found unreasonable the Commission's argument that it deserves broad discretion in determining whether harm was "likely." The FTC, in other words, did not allege any consumer injury other than the bare disclosure. In essence, the act, injury, and causation were all the same—the exposure of information.

The FTC's attempt to present mere information disclosure as a substantial injury in another recent data-breach case has met a similar fate in federal court. Router and Internet-protocol camera maker D-Link Systems refused to settle the Commission's charges that it had deceived consumers and committed unfair acts. On September 19, 2017, the U.S. District Court for the Northern District of California dismissed the FTC's unfairness charges for failing to satisfy the pleading requirements of Federal Rule of Civil Procedure 8.[25]

The court chided the FTC for failing to "allege any actual consumer injury in the form of a monetary loss or an actual incident where sensitive personal data was accessed or exposed."[26] The Commission could only allege that D-Link likely put consumers at risk. "The lack of facts indicating a likelihood of harm," the court added, "is all the more

---

[23] Complaint, *In re LabMD, Inc.*, Dkt. No. 9357 (Aug. 29, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf ("[R]espondent's failure to employ reasonable and appropriate measures to prevent unauthorized access to personal information, including dates of birth, SSNs, medical test codes, and health information, caused, or is likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.")

[24] 678 Fed. Appx. 816 (11th Cir. 2016).

[25] *FTC v. D-Link Systems, Inc.*, No. 3:17-cv-00039-JD (N.D. Ca. Sept. 19, 2017).

[26] *Id.*, Slip op. at 8.

striking in that the FTC says that it undertook a thorough investigation before filing the complaint."[27]

Another set of unfairness cases—from the data-privacy, not data-security, space—which relied upon a questionable interpretation of "substantial injury" arose from an FTC investigation into various companies' mobile-app sales practices. Parents had complained that because the companies' failed to require that passwords be re-entered when in-app purchases were made, their children engaged in "unauthorized" transactions on the adults' accounts. Google and Apple entered into consent decrees with the FTC, while Amazon opposed the Commission in court. The court granted the FTC's summary judgment motion, rubber-stamping the Commission's theory of harm against Amazon.[28]

Commissioner Joshua Wright forcefully dissented from the FTC consent decree with Apple.[29] He argued that the harm was not substantial when taking into account the economic context and the offsetting benefits to consumers and competition. By 2013, Commissioner Wright explained, Apple had 50 billion apps downloaded from its App Store. Even if, as the FTC's complaint alleged, Apple received "at least tens of thousands of complaints related to unauthorized in-app purchases," Wright argued that amount was extremely small when placed into the context of total app purchases.

Commissioner Wright also argued that the when examining harm, the FTC must consider countervailing benefits. Apple decided not to implement frequent pop-ups asking for password entry, he explained, with consumer preferences and the larger consumer experience in mind. Commissioner Wright's dissent engaged in the type of rigorous, economics-based cost-benefit analysis that neither the FTC staff nor the majority of Commissioners performed prior to bringing an unfairness action. Such rigorous analysis, Commissioner Wright noted, "ensure[s] that government action does more good than harm."[30]

2. The FTC Should Interpret "Substantial Injury" in the Context of Constitutional Standing

The principle of standing to sue arises from Article III, § 2 of the U.S. Constitution, which empowers U.S. courts to hear "cases" and "controversies." The standing doctrine preserves the judiciary's limited role by requiring that a plaintiff

---

[27] *Id.*, slip op. at 9.

[28] *See* Glenn G. Lammi, *Court's* FTC v. Amazon *Decision Endorses Agency's Disregard for Economic Analysis*, WLF LEGAL PULSE, June 1, 2016, https://wlflegalpulse.com/2016/06/01/courts-ftc-v-amazon-decision-endorses-agencys-disregard-for-economic-analysis/.

[29] *In re Apple, Inc.*, Dissenting Statement of Commissioner Joshua D. Wright, Jan. 15, 2014, https://www.ftc.gov/sites/default/files/documents/public_statements/dissenting-statement-commissioner-joshua-d.wright/140115applestatementwright.pdf.

[30] *Id*. at 5.

suffered an "injury in fact" that is fairly traceable to the defendant's conduct and which can be redressed by the relief sought. Although the FTC as a sovereign entity need not establish constitutional standing when it pursues unfairness or deception claims, it should adhere to those principles when assessing whether harm occurred.

Enforcement actions such as *LabMD* and *D-Link* demonstrate that the Commission is significantly out of step with current constitutional-standing jurisprudence. The courts reviewing the FTC's unfairness claims in those cases found the harms alleged to be "speculative" or unsupported by "any concrete facts." The most recent U.S. Supreme Court precedents on Article III standing dictate that federal civil claims must allege "particularized" and "concrete" harm.[31] Plaintiffs can overcome the standing hurdle if they plausibly allege that the harm is "likely" or that an act increased the risk of harm, but only if they can demonstrate that the "threatened injury is certainly impending" and not merely speculative.[32]

Numerous federal courts of appeals have applied those standing principles in the context of consumer class actions alleging injuries from data breaches. In *In re: SuperValu, Inc., Customer Data Security Breach Litigation*, the Eighth Circuit held that risk of identity theft or other harms arising from the theft of credit-card information, without concrete instances of fraudulent charges or opened accounts, was entirely "speculative."[33] In *Beck v. McDonald*, the Fourth Circuit found that even though the threat of future identity theft after a data breach could be "reasonably likely to occur," the threat was still "insufficiently 'imminent' to constitute injury-in-fact."[34] Neither the defendant's offer of free credit monitoring nor the plaintiffs' personally incurred costs to mitigate the risk of identity theft altered the court's conclusion. The Second Circuit reached the same conclusion when reviewing claims that alleged only future risk of harm and lost time and money from investigating possible fraudulent credit-card charges.[35]

B. Deception Claims

Section 5 of the FTC Act also prohibits business conduct that deceives consumers. In 1983, the Commission published a Policy Statement on Deception which limited its § 5 deception jurisdiction to statements that are "material," *i.e.* "likely to affect that consumer's conduct or decision with regard to the product or service."[36] The FTC

[31] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

[32] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147-48 (2013).

[33] 870 F.3d 763, 770 (8th Cir. 2017).

[34] 848 F.3d. 262, 276 (4th Cir. 2017).

[35] *Whalen v. Michaels Stores, Inc.*, No. 16-260 (L), 2017 WL 1556116, at *1–2 (2d Cir. May 2, 2017) (Summ. Order).

[36] Fed. Trade Comm'n, Policy Statement on Deception (1983), appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 175, 182 (1984), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

has brought claims against businesses victimized by a data breach for making allegedly deceptive statements about the quality of their data security. It has also filed suit when businesses have made allegedly deceptive claims about the privacy of customers' data. Such cases customarily have involved published (but rarely read) privacy policies.

1. Materiality must be Proven, Not Presumed

Unlike § 5 unfairness cases, substantial injury is not an element of an FTC deception claim. Materiality acts as an evidentiary proxy for injury, as explained in the Policy Statement on Deception: "[i]njury exists if consumers would have chosen differently but for the deception. If different choices are likely, the claim is material, and injury is likely as well."[37] Without the need to prove materiality, the FTC could pursue § 5 deception as a strict-liability claim—an especially harsh and troubling standard given that the government is examining speech, not conduct.

As part of its fact-finding on consumer injury, the FTC should thus closely reexamine its highly controversial 2015 deception case against Nomi Technologies.[38] The Commission accused Nomi of deceptively stating in its privacy policy that consumers could, at brick-and-mortar retail locations, opt out of Nomi's collection of anonymized data from Wi-Fi-enabled devices. Nomi did not in fact offer this extra level of consumer choice at the retail locations. Even though Nomi eliminated the opt-out choice from its privacy policy once learning of the FTC's investigation, the Commission persisted in its claim, and Nomi ultimately agreed to a settlement in 2015.

Commissioner Wright and then-Commissioner Ohlhausen dissented from the consent order. Both were troubled that the Commission did not establish in its complaint that Nomi's alleged deception was material to consumers. It offered no evidence that consumers "would have chosen differently but for" the alleged deception. Instead, the FTC presumed materiality.

Commissioner Wright discussed the evidence of materiality available to the Commission in his dissent, and concluded that "[It] strongly implies that the specific representation [that consumers could opt out] was not material and therefore not deceptive."[39] Both he and Commissioner Ohlhausen emphasized that Nomi was under no legal duty to offer the additional consumer choice, and imposing *de facto* strict liability will "chill business conduct that makes consumers better off."[40]

---

[37] *Id*. at 183.

[38] *In re Nomi Technologies, Inc*. FTC File No. 132-3251 (Sept. 3, 2015) https://www.ftc.gov/enforcement/cases-proceedings/132-3251/nomi-technologies-inc-matter.

[39] *In re Nomi Technologies, Inc*., Dissenting Statement of Commissioner Joshua D. Wright, Apr. 23, 2015 at 3, https://www.ftc.gov/public-statements/2015/04/dissenting-statement-commissioner-joshua-d-wright-matter-nomi-technologies.

[40] *Id*. at p. 2.

2. The FTC Should Consider Injury in Deception Cases Prior to Issuing a Complaint

In his *Nomi* dissent, Commissioner Wright asserted that the FTC had also failed to establish, as § 5 requires, a "'reason to believe that [a violation has occurred]' and that an enforcement action would 'be to the interest of the public.'"[41]

Not every possible consumer deception is harmful in and of itself, and even those that might be harmful may not impose *substantial* injury. The FTC should, as a matter of prosecutorial discretion, apply the "substantial injury" requirement it utilizes in unfairness cases as a pre-filing inquiry for deception claims. The Commission's claim against D-Link provides a useful example. In addition to the unfairness charge discussed above, the FTC charged D-Link with deceiving consumers by misrepresenting the effectiveness of its data security. The federal district court ruled against D-Link's motion to dismiss the FTC's deception claims, even though it found no substantial injury occurred in analyzing the Commission's unfairness claim. Had the FTC performed a fair assessment of whether D-Link's failure to prevent a breach caused substantial harm prior to issuing a complaint, it should have concluded that litigating was not in the public interest.

3. The FTC Should Explain Why Certain Data is "Sensitive"

In the course of pursuing privacy and data-security claims, the Commission has labeled certain information as "sensitive data." Financial information, Social Security Numbers, health information, and information about children are some examples of data that the FTC finds "sensitive." The special sensitivity of each type of data has a firm foundation in either federal law or long-standing public policy.

On two occasions in the past several years, the Commission has created new categories of sensitive data with no explanation for why it did so. In a 2014 complaint against the developer of a smartphone flashlight app, the FTC for the first time considered geolocation data as "sensitive."[42] In a 2017 complaint against television manufacturer Vizio, the FTC alleged § 5 violations for the manner in which "sensitive television viewing activity" was monitored and collected.[43] The FTC filed the complaint along with a consent order imposing an injunction and monetary damages.

Then-Commissioner Ohlhausen issued a concurring statement in which she noted concerns with the Commission's unsubstantiated decision to label TV viewing activity as "sensitive." She wrote, "There may be good policy reasons to consider such information sensitive. … But under our statute, we cannot find a practice unfair based primarily on

---

[41] *Ibid*.

[42] *In re Goldenshores Tech., LLC*, FTC Docket No. C-4446 (Mar. 31, 2014), Complaint at 2.

[43] *In re Vizio, Inc.*, FTC Docket No. 1623024 (Feb. 6, 2017), Complaint at 8.

public policy."[44] With that statement, Commissioner Ohlhausen tied the determination of data as "sensitive" directly to whether an injury is "substantial."

Because the nature of data is, at least in Acting Chairman Ohlhausen's opinion, directly tied to the level of consumer injury, any future Commission determinations that data is "sensitive" should only be made after rigorous analysis. In addition, if information is being newly minted "sensitive" in an FTC complaint, the Commission should include a thorough explanation of the its rational for adopting that label.

V. The FTC Must Consider the First Amendment when Taking Privacy and Data-Security Actions

The First Amendment provides strong limitations on prohibiting and constraining the collection, use, and disclosure of information, including electronic data.[45] The FTC performed a rather cursory First Amendment analysis of its authority under § 5 to pursue deception claims in 2002, concluding that Commission actions comported with the First Amendment.[46] The FTC cannot, however, rely on this 15-year old analysis when bringing deception actions, given the significant developments in the commercial-speech doctrine since 2002. Further, the FTC has to our knowledge neither performed a similar, general First Amendment analysis of its unfair-practices authority nor considered speech rights in the specific area of privacy and data-security regulation and enforcement.

---

[44] *In re Vizio, Inc.*, Concurring Statement of Commissioner Maureen K. Ohlhausen, Feb. 6, 2017, https://www.ftc.gov/public-statements/2017/02/concurring-statement-acting-chairman-maureen-k-ohlhausen-matter-vizio-inc.

[45] *See, e.g.*, *Sorrell v. IMS Health, Inc.*, 131 S. Ct. 2653, 2672 (2011) ("Vermont law restricts the sale, disclosure, and use of pharmacy records that reveal the prescribing practices of individual doctors. ... Subject to certain exceptions, the information may not be sold, disclosed by pharmacies for marketing purposes, or used for marketing by pharmaceutical manufacturers. ... The State has burdened a form of protected expression that it found too persuasive. At the same time, the State has left unburdened those speakers whose messages are in accord with its own views. This the State cannot do."); *U.S. West, Inc. v. Fed. Communications Comm'n*, 182 F.3d 1224, 1240 (10th Cir. 1999) ("The FCC failed to adequately consider the constitutional implications of its CPNI regulations. Even if we accept the government's proffered interests and assume those interests are substantial, the FCC still insufficiently justified its choice to adopt an opt-in regime. Consequently, its CPNI regulations must fall under the First Amendment. At the very least, the foregoing analysis shows that the CPNI regulations clearly raise a serious constitutional question, invoking the rule of constitutional doubt.").

[46] Fed. Trade Comm'n, Press Release, *FTC Staff Provides the FDA with Comments on First Amendment Commercial Speech Doctrine* (Sep. 20, 2002), https://www.ftc.gov/news-events/press-releases/2002/09/ftc-staff-provides-fda-comments-first-amendment-commercial-speech ("In executing [the FTC's] mission, we have found that the First Amendment commercial speech doctrine is fully compatible with our vigorous consumer protection program. The FTC requires that all claims be true, non-misleading, and substantiated at the time they are made. The FTC's post-market review of advertising claims and application of tailored remedies in advertising cases curb deception without overly restricting truthful commercial speech, thus promoting the goals embodied in the First Amendment.").

A. First Amendment Review is Appropriate

Courts have concluded that a First Amendment review is appropriate when the government restricts the collection, use, and disclosure of information. For example, in *Sorrell*, the U.S. Supreme Court held unconstitutional a Vermont law that the purportedly protected the privacy interests of doctors by prohibiting business entities from using and/or disclosing prescriber-identifying data for marketing purposes.[47] In *U.S. West*, the Tenth Circuit held that FCC rules limiting the use and disclosure of personal information restricted the company's speech and therefore were subject to First Amendment review.[48]

The FTC has formed what it calls a "privacy common law" (the collection of the FTC's consent orders in privacy and data security cases).[49] Commission staff and some commentators treat this "privacy common law" as a set of legal requirements that restrict how companies may collect, use, disclose, and secure information.[50] In addition, individual FTC consent orders impose on companies subject to the orders certain privacy and data-security obligations that are treated as legal judgments and enforced through court orders. Violations of court orders can result in millions of dollars in monetary penalties.[51]

---

[47] *Sorrell*, 131 S. Ct. at 2672.

[48] *U.S. West, Inc. v. Fed. Communications Comm'n*, 182 F.3d 1224 (10th Cir. 1999).

[49] *See* Public Statement, FTC Commissioner Julie Brill, "Privacy, Consumer Protection, and Competition" (Apr. 27, 2012) ("Of course, our enforcement work is primarily designed to address the practices at issue in the specific matter. Yet our privacy cases are also more generally informative about data collection and use practices that are acceptable, and those that cross the line, under Section 5 of the Federal Trade Commission Act creating what some have referred to as a common law of privacy in this country."), https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-consumer-protection-and-competition/120427loyolasymposium.pdf; Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 586 (2014) ("We contend that the FTC's privacy jurisprudence is functionally equivalent to a body of common law").

[50] Solove and Hartzog, *supra* note 26 at 620 ("Practitioners look to FTC settlements as though they have precedential weight. The result is that lawyers consult and analyze these settlements in much the same way as they do judicial decisions."). Washington Legal Foundation has argued that due-process considerations dictate against the creation or application of "common law" through individual consent decrees. *See, e.g.*, Br. of *Amicus Curiae* Washington Legal Foundation, *supra* note 9.

[51] *FTC v. Lifelock, Inc., Stipulated Order Resolving FTC's Allegations of Contempt and Modifying Stipulated Final Judgment and Order for Permanent Injunction* (Dec. 17, 2015), https://www.ftc.gov/system/files/documents/cases/151217lifelockstip.pdf (ordering $100 million civil penalty); *U.S. v. Google, Inc. Order Approving Stipulated Order for Permanent Injunction and Civil Penalty Judgment* (Nov. 20, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/11/121120googleorder.pdf (ordering $22.5 million civil penalty).

B. The FTC Must Identify a Substantial State Interest

Under the test which the U.S. Supreme Court has set out for reviewing commercial-speech restrictions, the government defendant bears the burden of first identifying a substantial state interest that it seeks to advance.[52] Courts generally do not apply this part of the commercial-speech test with much rigor, but in the *U.S. West* case, the Tenth Circuit would not accept the Federal Communications Commission's general interest in privacy protection as sufficiently specific to be "substantial."[53] The court stated:

> Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of substantial state interest under [the First Amendment's commercial speech test] for it is not based on an identified harm.[54]

The concept of privacy, especially with regards to personal data and its online availability, has broadened substantially since the Tenth Circuit decided *U.S. West* in 1999. If an FTC privacy or data-security action were to face a First Amendment challenge, and the court were to apply the Tenth Circuit's demands for specificity, the Commission would have to provide a far more detailed explanation of the privacy interest it sought to advance through its action than it generally has in past and current agency statements.

C. The FTC's Actions Must Directly and Materially Advance the State Interest

The FTC's actions must also directly and materially advance its stated privacy or data-security interest. The FTC must show that the harms are real and that the restriction will alleviate them to a material degree.[55] The Commission would need to show that the privacy or data-security requirements sought in enforcement actions or imposed through

---

[52] *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 566-71 (1980).

[53] *U.S. West, Inc.*, 182 F.3d at 1234-35 ("The breadth of the concept of privacy requires us to pay particular attention to attempts by the government to assert privacy as a substantial state interest. When faced with a constitutional challenge, the government bears the responsibility of building a record adequate to clearly articulate and justify the state interest. The government cannot satisfy the second prong of the *Central Hudson* test by merely asserting a broad interest in privacy. It must specify the particular notion of privacy and interest served.").

[54] *Id*. at 1235.

[55] *See Edenfield v. Fane*, 507 U.S. 761, 770 (1993).

its settlements would alleviate the identified threats to privacy or data-security interests. The FTC may not be able to meet this part of the *Central Hudson* test in some cases. In cases where no consumer injury can be shown, the FTC obviously cannot show that the harms are real or that they will occur. In addition, the FTC may not be able to show that the privacy and data-security obligations imposed on a company will alleviate the risks to a material degree. Companies constantly face cyber-attacks, and no security measures have proven fully effective. For companies that already have implemented data-security measures, the FTC may not be able to show that the measures it requires will make a material difference, especially if the specific vulnerability identified by the Commission has already been remediated by the company.

D. The FTC's Actions Must Be No More Extensive than Necessary

Finally, the FTC's actions must be no more extensive than necessary to serve the privacy or data-security interests it is advancing. The actions must be in reasonable proportion to the interest served using a careful calculation of the costs and benefits associated with the burden imposed by the FTC.[56]

The generic, one-size-fits-all privacy and data-security obligations currently pursued in enforcement actions or imposed through FTC consent orders are by their nature not reasonably tailored to the state interest. The Commission must take into consideration the size and type of company, the type of data involved, and the data-breach threats it faces. Failure to do that will impose far more restrictions on the collection or use of speech in the form of data than necessary.

Small companies are not able to implement the same data-security measures the FTC imposes upon a Fortune 500 company through a consent order. So, rather than collect and use the information they otherwise might, such companies may choose to not collect the information at all, chilling their First Amendment rights.

Also, in some cases, a data breach may involve data that is already public, and the privacy and data-security burdens imposed by the FTC may very well dwarf the benefit to the protected interest, particularly if the alleged vulnerability has been addressed.

Moreover, the FTC's typical consent order and the privacy and data-security requirements it imposes can remain in place for up to 20 years, which may be dramatically disproportionate to the harm being redressed. FTC consent decrees do not explain why 10, 15 or 20 years is the appropriate amount of time that settling parties must comply.

---

[56] *See Board of Trustees of the State Univ. of N.Y. v. Fox*, 492 U.S. 469, 480 (1989) ("a fit that is not necessarily perfect, but reasonable; that represents not necessarily the single best disposition but one whose scope is "in proportion to the interest served,"); *Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 417 (1993) ("[the city] has not 'carefully calculated' the costs and benefits associated with the burden on speech imposed by its prohibition.").

E. The FTC Can Better Tailor its Enforcement Activity to its Data-Privacy Interest

The FTC can take enforcement approaches that would be more closely tailored to the governmental interest in privacy and data-security. Narrowing its enforcement focus would also reduce the burden on protected speech. The choice for companies may change from deciding whether to collect, use, and disclose any personal or device information at all, to a choice of selecting which data it will collect, use, and disclose knowing that certain choices may raise its data-security bar.

The FTC could also develop guidance for the staff's case selection or issue an enforcement policy which acknowledges that data-based expressive activity is constitutionally protected. The FTC, for instance, could tailor its enforcement activity by focusing on instances where

- the defendant made an improper use or disclosure;
- consumer injuries are substantial and there is a reasonable, non-speculative nexus between the defendant's conduct and the consumer injury in unfairness cases;
- statements related to privacy and data security are material and there is evidence to suggest they were relied upon;
- sensitive information is involved; or
- "private" information is involved, which considers whether information is already public.

V. Conclusion

Data is the oil that fuels today's economy. Economic growth is thus quite dependent on the ability of that fuel to flow freely. Data, and businesses' creative, respectful collection of use of it, is integral to keeping the cost of access to the World Wide Web either extremely low or, in most cases, entirely without cost.

The Federal Trade Commission can facilitate that the free flow of data by tethering its privacy and data-security regulatory and enforcement activities to such reliable legal principles as actual, substantial harm, materiality, and freedom of speech. Those basic limitations will help cabin the agency's natural tendency to expand its authority and desire to solve problems.

The workshop that these comments inform can be a positive beginning to a more humble path for FTC in the privacy and security spaces. It should not be used to create a knowledge-base to justify and support a new category of harms to prevent—

"informational injuries." Refocusing FTC resources on the most substantial harms and the most material deceptions would not only preserve increasingly limited budgetary resources, it could also open up new possibilities for safeguarding sensitive data.

The past two Presidents have urged companies to engage in cybersecurity-threat information sharing.[57] However, researchers have found that companies are not sharing threat information because they are concerned that doing so will provide a roadmap for regulators (and plaintiffs) in date-security lawsuits.[58] If a company knows that disclosing a vulnerability will expose it to increased risk of a 20-year FTC order, it is unlikely to participate in the information-sharing process.

Washington Legal Foundation appreciates the opportunity to inform the December 12 workshop with these comments.

Respectfully submitted,

/s/Glenn G. Lammi

Cory L. Andrews

WASHINGTON LEGAL FOUNDATION

October 27, 2017

[57] President Obama, Executive Order, IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity; President Trump, Executive Order, STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE, *available at* https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

[58] George V. Hulme, *Tackling Cybersecurity Threat Information Sharing Challenges*, CSO ONLINE, (Jan. 17, 2017), https://www.csoonline.com/article/3157540/security/tackling-cybersecurity-threat-information-sharing-challenges.html.