Before the Federal Trade Commission

In re: Competition and Consumer Protection in the 21st Century Hearings Topic 5: The Commission's Remedial Authority to Deter Unfair and Deceptive Conduct in Privacy and Data Security Matters	Project No. P181201 Docket No. FTC-2018-0052

Comments of the R Street Institute

In response to the Federal Trade Commission's request for comments dated June 20, 2018, the R Street Institute respectfully submits the following comments. Submitted in advance of the hearings planned to be held, these are intended to identify topics for those hearings, and will likely be supplemented by more detailed analysis afterward.

This comment is one of several that R Street is submitting, pursuant to the Commission's request of a separate comment per topic. This comment relates to Topic 5 on the Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters.

Privacy and data security are increasingly vital to the American public.[1] The Commission has done an admirable job in these areas by offering recommendations for business and policymakers,[2] as well as by pursuing legal actions where appropriate,[3] but not all these efforts have been successful. Indeed, the recent setback in its case against LabMD suggests that significant changes may need to be made in how the Commission pursues privacy and data security cases going forward.[4]

In the upcoming hearings, we therefore encourage the Commission to consider at least the following topics.

Lessons Learned from *Wyndham* and *LabMD*. On privacy and data security matters, the Commission has hosted workshops,[5] issued reports[6] and entered into multiple consent decrees. But for all this informal guidance, there is still a dearth of formal guidance on how Section 5

[1] See, e.g., Tom Struble, "Resolving Cybersecurity Jurisdiction Between the FTC and FCC," *R Street Policy Study* No. 116, October 2017. https://goo.gl/yku1YH.
[2] See, e.g., Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," March 2012. https://goo.gl/M02JF3.
[3] See, e.g., Federal Trade Commission, "Privacy and Data Security Update: 2017," January 2017–December 2017. https://goo.gl/EJzRvx.
[4] See *LabMD, Inc. v. FTC*, No. 16-16270, slip op. (11th Cir. June 6, 2018). https://goo.gl/e5PZGC.
[5] See, e.g., Federal Trade Commission, "Informational Injury Workshop," Dec. 12, 2017. https://goo.gl/SjFxKz.
[6] See, e.g., "2012 Privacy Report."

applies to privacy and data security.[7] Indeed, despite having brought over 60 data security cases since 2002,[8] the Commission has only ever litigated three: *Wyndham*,[9] *LabMD*[10] and *D-Link*.[11] The first of these cases went in favor of the Commission,[12] but the second did not.

What should the Commission take away from these cases? The holding in *Wyndham* and dicta in *LabMD* suggest that privacy and data security are within the scope of Section 5 and that even in the absence of formal rules, the Commission can pursue these areas via case-by-case adjudication. However, the court in *LabMD* demanded more from the Commission's proposed remedy.[13] How will the Commission address the Eleventh Circuit's concerns going forward? Should the Commission's complaints and proposed remedies be more specific?[14] Should the Commission eschew behavioral remedies and pursue only monetary penalties?

Informational Injuries and Civil Penalty Authority. Last December, in an effort to better understand the various non-financial harms consumers can suffer when information about them is misused, the Commission hosted a workshop on informational injuries.[15] The intangible nature of these harms makes them difficult to detect and quantify, so it is understandable that the Commission has been struggling to deal with them. For example, the 2015 enforcement against Nomi Technologies strained the bounds of the Commission's Deception Policy Statement.[16] Instead of proving that Nomi's false promise of in-store opt-out mechanisms harmed consumers — because consumers would have chosen differently but for that deception — the Commission simply relied on the presumption that all express statements are material.[17] Such broad use of its deception authority is a poor way to pursue informational injuries, but there are also difficulties in using the Commission's unfairness authority.

---

[7] See, e.g., Justin (Gus) Hurwitz, "Data Security and the FTC's UnCommon Law," *Iowa Law Review* 101:3 (2016). https://goo.gl/pP6tAf; and Tom Struble, "Reforming the Federal Trade Commission Through Better Process," *R Street Policy Study No. 122*, December 2017. https://goo.gl/tEtBMN.

[8] 2017 Privacy and Data Security Update, p. 4.

[9] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[10] See *LabMD, Inc. v. FTC.* https://goo.gl/e5PZGC.

[11] See Federal Trade Commission, "FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of its Computer Routers and Cameras," Jan. 5, 2017. https://goo.gl/17qvYY.

[12] *Wyndham*, 799 F.3d at 249–59 (rejecting Wyndham's arguments that informal guidance alone cannot provide fair notice of what Section 5 requires in terms of data security).

[13] *LabMD*, at 25–31.

[14] See, e.g., Daniel Castro, "LabMD Ruling Gives FTC Chance for Course Correction on Cybersecurity," *Morning Consult*, June 13, 2018. https://goo.gl/2PHN5J.

[15] "Informational Injury Workshop." https://goo.gl/SjFxKz.

[16] Federal Trade Commission, "Complaint," In the Matter of NOMI TECHNOLOGIES, INC., Docket No. C-4538, Aug. 28, 2017. https://goo.gl/HbFLRf.

[17] See Federal Trade Commission, "Dissenting Statement of Joshua D. Wright, Commissioner," In the Matter of NOMI TECHNOLOGIES, INC., Docket No. C-4538, April 23, 2015. pp. 2–3. https://goo.gl/9hOxfy.

Indeed, in his recent testimony before the Senate, Chairman Simons admitted as much.[18] But the Commission's task is difficult, not impossible. The mere fact that "Section 5 does not provide for civil penalties,"[19] in some instances, does not leave the Commission helpless to pursue informational injuries. Section 5 does provide civil penalty authority for "knowing violations of rules and cease and desist orders respecting unfair or deceptive acts or practices[.]"[20] Thus, either a rulemaking under Section 18[21] or a fulsome body of case law would enable the Commission to file complaints and seek civil penalties even in cases where the degree of harm is difficult to quantify, as it often is with informational injuries.

Has the Commission considered undertaking a Mag-Moss rulemaking in this area? For example, could the Commission specify that maintaining inadequate data security, failing to post a privacy policy, or failing to notify affected users after a data breach are categorically unfair or deceptive practices? Are data breaches and other privacy incidents "prevalent" enough to satisfy the requirements of Section 18?[22] Could such a rulemaking provide the uniform national framework needed to preempt a patchwork of state privacy laws? Does the Commission have adequate resources on staff to manage such an undertaking? Should the Commission instead simply continue using its unfairness and deception authority to pursue informational injuries case by case?

* * *

R Street thanks the Federal Trade Commission for the opportunity to submit these comments, and recommends that the Commission pursue the above-identified areas in its ongoing work on promoting competition and innovation.

Respectfully submitted,

/s/

Tom Struble
Tech Policy Manager

R Street Institute
1212 New York Ave, NW
Suite 900
Washington, DC 20005
tstruble@rstreet.org

August 14, 2018

---

[18] Testimony of Joseph Simons, Chairman, Federal Trade Commission, House Subcommittee on Digital Commerce and Consumer Protection, "Prepared Statement of the Federal Trade Commission 'Oversight of the Federal Trade Commission,'" 115th Congress. July 18, 2018. https://goo.gl/abZVYp.
[19] Ibid., p. 6.
[20] 15 U.S.C. § 45(m).
[21] 15 U.S.C. § 57a.
[22] 15 U.S.C. § 57a(b)(3).