Before the
Federal Trade Commission
Washington, DC 20580

In the matter of Competition and Consumer Protection in the 21st Century Hearings	Project Number P181201

COMMENTS OF PUBLIC KNOWLEDGE

5. The Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters. [1]

Consumer protection, fairness, and competition policy in today's digital economy require substantially stronger enforcement of antitrust law, more aggressive use of existing regulatory powers and new laws to fill in important policy gaps. Public Knowledge commends the FTC for launching this proceeding and a series of public hearings to examine competition and consumer protection in the 21st century, and today offers some initial observations and ideas to consider on the topics the Commission has identified as central to its inquiry. We will augment these ideas through our participation in Commission workshops and through follow up filings as the Commission refines the focus of its efforts.

The recent explosion in internet distribution of goods and services, growing dependence of democratic processes on nondiscriminatory and open digital communications platforms, and ongoing market dominance of entrenched media and communications companies makes it imperative for the FTC to become more vigilant and assertive to protect incipient and potential competition, to apply all qualitatively relevant elements to its consumer welfare analysis, and to update its consumer protection enforcement to reflect the complexities of the digital marketplace. As an expert agency with a specific mandate from Congress, it is also important for the FTC to inform lawmakers and the public of market imperfections and problems it lacks the tools and resources to address

[1] Public Knowledge staff John Bergmayer, Allie Bohm, Ryan Clough, Harold Feld, Meredith Rose, Kory Gaines, Dylan Gilbert, and Gus Rossi contributed to the comments filed in this proceeding.

and to propose policy adjustments that would more effectively address inequities in the oversight of today's economy.

Today, we are highlighting a number of the complexities and issues regarding application of FTC authority to the digital economy and the exploding internet economy in response to the Commission's request for comment. Rather than delineate precisely what deserves treatment under antitrust, consumer protection or some new legal authority, we instead highlight many of the problems that deserve careful attention, definition, further analysis and refinement before precise policy action should be considered. We offer this as a first step because we believe:

- the explosion of the digital market calls first for understanding precisely what is going wrong and therefore deserves fixing;
- identifying what are the best policy tools available to fix the problems;
- evaluating how best to apply existing policy tools; and
- proposing new policy tools to address problems that fall between the gaps under existing law.

This document contains our comments relating to the Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters.

We look forward to working with the FTC and all other stakeholders to flesh out the details of the concerns raised in our comments and propose meaningful policy adjustments and enforcement practices to help the Commission fully protect competition and consumers in the digital marketplace.

* * *

Since 2005, the FTC has brought administrative actions under its unfair and deceptive practices authority to protect privacy and address data security.[2] Many of these actions were brought under the deceptiveness prong of the Commission's authority, and the vast majority, under either authority, have resulted in settlements.[3]

The FTC's deceptiveness authority is fairly straightforward. An entity's privacy or data security practice is deceptive if "'first, there is a representation, omission, or practice

---

[2] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015).
[3] *Id.*

that, second, is likely to mislead consumers acting reasonably under the circumstances, and third, the representation, omission, or practice is material.'"[4] This authority has proved useful in drawing attention to and, in many cases, ameliorating companies' privacy violative practices in the digital age.[5]

The FTC's unfairness authority is more complicated. Rather than enumerate particular unfair practices, Congress envisioned unfairness keeping pace with technology and "designed the term as a 'flexible concept with evolving content.'"[6] In order to qualify as "unfair," the injury the practice causes must be "[1] substantial; [2] it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and [3] it must be an injury that consumers themselves could not reasonably have avoided."[7] This is a fairly high bar in and of itself. It requires a cost-benefit analysis.[8] And, in many cases, even if the FTC is able to demonstrate a legally cognizable harm, the consumer may benefit from the practice, because, for example, pervasive data collection may reduce her search time and enable businesses to show her more relevant advertisements. Or, competition may benefit, because, for example, it may be less expensive for a new entrant to enter the market if it does not have to pay the money necessary to adhere to the latest security standards. Finally, in some cases, the consumer

---

[4] *FTC v. AMG Servs.*, 29 F. Supp. 3d 1338, 1364 (quoting F.T.C. v. Gill, 265 F.3d 944, 950 (9th Cir. 2001)).

[5] *E.g.* Lesley Fair, What Vizio was Doing Behind the TV screen, FED. TRADE COMM'N, (Feb. 6, 2017, 11:05 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what- vizio-was-doing-behind-tv-screen; Tech Company Settles FTC Charges it Unfairly Installed Apps on Android Mobile Devices Without Users' Permission, FED. TRADE COMM'N (Feb. 5, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/tech-company-settles-ftc-charges-it-unfairly-installed-apps; HTC America Settles FTC Charges it Failed to Secure Millions of Mobile Devices Shipped to Consumers, FED. TRADE COMM'N (Feb. 22, 2013), https://www.ftc.gov/news-events/press-releases/2013/02/htc-america-settles-ftc-charges-it-failed-secure-millions-mobile; Grant Gross, FTC Warns App Developers Against Using Audio Monitoring Software, CIO (Mar. 18, 2016), http://www.cio.in/news/ftc-warns-app-developers-against-using-audio-monitoring-software; Aaron's Rent-To-Own Chain Settles FTC Charges that it Enabled Computer Spying by Franchises, FED. TRADE COMM'N (Oct. 22, 2013), https://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer; Spyware Seller Settles FTC Charges; Order Bars Marketing of Keylogger Software for Illegal Uses, FED. TRADE COMM'N (June 2, 2010), https://www.ftc.gov/news-events/press-releases/2010/06/spyware-seller-settles-ftc-charges-order-bars-marketing-keylogger.

[6] *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236, 243 (3d Cir. 2015) (quoting *FTC v. Bunte Bros*, 312 U.S. 349, 353 (1941)).

[7] *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir. June 6, 2018), at *12 (internal citations omitted).

[8] *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236, 255 (3d Cir. 2015).

could have avoided the harm by declining to sign up for the particular service or buy the particular product.

In addition to the high bar set by the unfairness factors themselves, the Eleventh Circuit in *LabMB* recently concluded that an unfair act or practice must be "clear and well-established," that is, "expressed in the Constitution, statutes, or the common law."[9] The court did signal that this requirement does not dictate that the FTC spell out precisely what portion of Constitution, statute, or the common law it is relying upon. Rather, the Eleventh Circuit noted that the source of the clear and well-established principle could be "apparent"[10] Still, this would seem to confine the FTC to serving – in some cases, such as when the clearly established law is the common law of torts – as a second enforcement mechanism for existing laws, rather than allowing the concept of unfairness to evolve as Congress intended.[11]

LabMB creates something of a circuit split with the Third Circuit, which held in FTC v. Wyndham Worldwide Corp that an entity subject to the FTC's unfairness authority need only have "fair notice that its conduct could fall within the meaning of the" FTC Act; it is not entitled to "to know with ascertainable certainty the FTC's interpretation of what . . . practices are required by" the act.[12] The Third Circuit reasoned that Wyndham had reason to know that "cybersecurity practices can, as a general matter, form the basis of an unfair practice."[13] It did not peg its reasoning to the idea that unfair cybersecurity practices violate clear and well-established law. Indeed, even the Eleventh Circuit in *LabMB* acknowledged that "Congress 'intentionally left development of the term 'unfair' to the Commission' through case-by-case litigation."[14] Still, *LabMB* likely makes the already hard-to-satisfy standard for "unfairness" harder to satisfy.

---

[9] *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir. June 6, 2018), at *16.

[10] *Id.*, at *16-17 ("The Commission's decision in this case does not explicitly cite the source of the standard of unfairness it used . . . It is apparent to us, though, that the source is the common law of negligence.")

[11] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3d Cir. 2015) (quoting FTC v. Bunte Bros, 312 U.S. 349, 353 (1941)).

[12] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d at 255.

[13] *Id*.

[14] *LabMD, Inc. v. FTC,* No. 16-16270 (11th Cir. June 6, 2018), at *10 (internal citations omitted).

Moreover, even where the FTC is able to prove unfairness or deception, it is only able to impose financial penalties on an entity once that entity has entered into a consent agreement with the Commission and violated that consent agreement. And, it may only impose financial penalties by bringing suit in district court. In addition, the Eleventh Circuit's decision in *LabMB* also requires that "prohibitions contained in cease and desist orders and injunctions must be specific," enjoining particular acts or practices, rather than requiring an entity to simply engage in reasonable practices.[15] This mandate may inhibit the FTC from imposing flexible requirements that keep pace with technology.

In sum, while there is no doubt that the FTC has, can, and should continue to do substantial good to protect consumers' privacy and data security in the digital age under its Section 5 authority, "the Commission's existing authority may not be sufficient to effectively protect consumers with regard to all data privacy issues of potential concern."[16] The FTC should advocate with Congress for increased authority in this area and to clean up the mess the Eleventh Circuit created with *LabMB*.

Respectfully submitted,
Public Knowledge
August 20, 2018

[15] *Id.* at *27, *30.
[16] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 249 (3d Cir. 2015) (quoting Order Denying Respondent LabMD's Motion to Dismiss, No. 9357, 2014 FTC LEXIS 2 at *51 (Jan. 16, 2014) (emphasis original)).