epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

October 31, 2017

Chairman Maureen K. Ohlhausen
Commissioner Terrell McSweeny
The Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

RE: December Workshop on "Informational Injury"

Dear Chairman Ohlhausen and Commissioner McSweeny:

We write to you to express concerns regarding the upcoming FTC workshop on Informational Injury, scheduled for December 12, 2017. The FTC asks "how to best characterize" consumer privacy injuries. But the injuries consumers face are obvious – identity theft, data breach, ubiquitous data gathering, consumer profiling, and a growing lack of trust in the information economy.

The Equifax data breach helps make clear the various problems with the FTC's framing of the December workshop. In the proposed agenda, the FTC asks "how do consumers perceive and evaluate the benefits, costs, and risks of sharing information in light of potential injuries? What obstacles do they face in conducting such an evaluation?" But most consumers never interacted with Equifax, yet the company had acquired detailed profiles on Americans. Much of the modern information economy reflects this reality – consumers do not choose to disclose personal data to firms. Companies simply acquire the information and use it without the consumers knowledge or control. Increasingly, consumers confront a "black box society" in which companies engage in secret profiling to make judgments about them that have a profound impact on their lives.[1] Even when consumers interact directly with firms, privacy policies provide little value. As the FTC itself found, a "notice-and-choice" approach to privacy does not work. The Commission concluded in 2012 that notice-and-choice "led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand."[2]

On the other hand, the risk to consumers of the current self-regulatory approach to privacy is clear. The FTC reported 399,225 cases of identity theft in 2016 alone.[3] A 2015 report from the Department of Justice found that 86% of identity theft victims experienced the

[1] FRANK PASQUALE, THE BLACK BOX SOCIETY 8 (2015); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).
[2] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change* 60 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[3] Fed. Trade Comm'n, *FTC Releases Annual Summary of Consumer Complaints* (March 3, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints.

fraudulent use of existing account information.[4] The same report estimated the cost of identity theft to the U.S. economy at $15.4 billion.[5]

According to the Pew Research Center, 91% of consumers say that they have lost control over how personal information is collected and used by companies.[6] The same study reported that 64% of Americans supported greater regulation over how advertisers handle their personal data. Even leading CEOs now support stronger privacy protections in the United States.

Given the urgency of these problems, we recommend that the FTC refocus the December workshop, focusing less on how to define the problem of "informational injury" and more on how to address the problem. The FTC currently proposes these topics for discussion:

- What are the qualitatively different types of injuries from privacy and data security incidents?
- What frameworks might we use to assess these different injuries?
- How do businesses evaluate the benefits, costs, and risks of collecting and using information in light of potential injuries?
- How do consumers perceive and evaluate the benefits, costs, and risks of sharing information in light of potential injuries? What obstacles do they face in conducting such an evaluation?

We propose instead that the FTC address these questions:

- Why do the levels of data breach, identity theft, and financial fraud continue to rise in the United States? And how does the U.S. experience compare with that of other countries?
- What is the Federal Trade Commission currently doing to minimize the risk of data breach and identity theft? What more could the FTC do?
- What are businesses currently doing to minimize the risk of data breach and identity theft? What more could businesses do?
- Do consumers have adequate legal remedies to protect against informational injuries? What more could be done to extend protections for consumers?
- How does the use of a consumer data affect the services consumers receive? How is information about a person's finances, health, race or ethnicity and geo-location used to target consumers? And what do consumers know about such practices?

[4] Erika Harrell, Bureau of Justice Statistics, *Victims of Identity Theft, 2014* (Sept. 27, 2015), https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408.
[5] *Id*.
[6] George Gao, Mary Madden, *Privacy and Cybersecurity: Key Findings From Pew Research*, Pew Research Center, (Jan. 16, 2015), http://www.pewresearch.org/fact-tank/2015/01/16/privacy/.

- Should new limits be established on data collection to address the national security risks of informational injury?

Thank you for your consideration.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Alan Butler*
Alan Butler
EPIC Senior Counsel

/s/ *Christine Bannan*
Christine Bannan
EPIC Policy Fellow

/s/ *Sam Lester*
Sam Lester
EPIC Consumer Privacy Fellow