Comments to the Federal Trade Commission from Consumer Federation of American, Consumer Action, the Center for Digital Democracy, and U.S. PIRG on the December 12, 2017 Workshop on "Informational Injury"

January 26, 2018

We[1] write to provide comments following the December 12, 2017 workshop that the Federal Trade Commission (FTC) held on Informational Injury. The FTC asked "how to best characterize" consumer privacy injuries.

Most of the discussion at the workshop focused on the injury that consumers suffer as a result of data breaches and identity theft. While the information that panelists provided about the dangers and impact of data breaches and identity theft helped to illustrate some of the informational injuries that consumers may experience, the workshop failed to explore these crucial questions:

- Why do the levels of data breach, identity theft, and financial fraud continue to rise in the United States? How does this compare with other countries, and if there are differences, why?

- What is being done to reduce the number of data breaches and the extent of damage they cause? What more should be done?

- Who should be held responsible when individuals' data are not adequately safeguarded and what remedial action and penalties are appropriate?

Not all panelists agreed that consumers whose personal data have been subject to a data breach have been "harmed"[2] but those injuries are obvious – a 2015 report from the Department of Justice found that 86% of identity theft victims experienced the fraudulent use of existing account information.[3] The same report estimated the cost of identity theft to the U.S. economy at $15.4 billion.[4] The FTC reported 399,225 cases of identity theft in 2016 alone.[5] In the first panel, Pam Dixon, Executive Director of the World Privacy Forum, highlighted the serious consequences of medical identity theft and, even more alarming, warned that new techniques

1 Consumer Federation of America, Consumer Action, and U.S. PIRG are nonprofit consumer organizations that conduct research, educational activities, and advocacy to further consumers' interests. More information is available at www.consumerfed.org, www.consumer-action.org, www.democraticmedia.org, and www.uspirg.org.
2 Remarks of Geoffrey Manne, International Center for Law & Economics, FTC Workshop on Informational Injury (December 12, 2017) Panel 2, https://www.ftc.gov/news-events/audio-video/video/informational-injury-panel-2-potential-factors-assessing-injury
3 Erika Harrell, Bureau of Justice Statistics, *Victims of Identity Theft, 2014* (Sept. 27, 2015), https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408.
4 *Id*.
5 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.

such as biometric "morphing" will present serious challenges to efforts to prevent the fraudulent use of consumers' personal data.[6]

And as Laura Moy at the Georgetown University Law Center's Center on Privacy and Technology noted in testimony[7] before Congress last year concerning "trigger standards" for data breach notification:

> "In addition, trigger standards narrowly focused on financial harm ignore the many non-financial harms that can result from a data breach. For example, an individual could suffer harm to dignity if he stored embarrassing photos in the cloud and those photos were compromised. If an individual's personal email were compromised and private emails made public, she could suffer harm to her reputation. And in some circumstances, breach could even lead to physical harm. For example, that fact that a domestic violence victim had called a support hotline or attorney, if it fell into the wrong hands, could endanger her life."

Edmund Mierzwinski, U.S. PIRG Program Director, testified[8] in another House hearing that harms resulting from data breaches also include "the cost and time cleaning the problems up, additional problems caused by an empty checking account or a missing tax refund and being denied or paying more for credit or instance or rejected for jobs due to the digital carnage caused by the thief." He further noted that breach victims may face additional problems such as the stigma of being considered a "deadbeat" and dealing with the emotional and worry that brings.

Consumers have no control over the security of the information that businesses hold about them, and as Katie McInnis from Consumers Union pointed out in the workshop, the number and severity of breaches indicates that businesses do not appear to have sufficient incentive to adequately secure that data.[9] Furthermore, as the Equifax data breach makes clear, it is totally insufficient to frame the problem of data security as one of how consumers perceive and evaluate the benefits, costs, and risks of sharing information in light of potential injuries, and what obstacles they face in conducting such an evaluation. Consumers never provided their personal information directly to Equifax, yet the company had acquired detailed profiles on them.

Much of the modern information economy reflects this reality – in many cases consumers do not choose to disclose their 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

---

6 Remarks of Pam Dixon, World Privacy Forum, FTC Workshop on Informational Injury (December 12, 2017), Panel 1, https://www.ftc.gov/news-events/audio-video/video/informational-injury-panel-1-injuries-101

7 Testimony of Laura Moy before the House Financial Services Committee (October 25, 2017), available at https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-lmoy-20171025.pdf

8 Testimony of Edmund Mierzwinski before the House Financial Services Committee Subcommittee on Financial Institutions and Consumer Credit (November 1, 2017), available at https://financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-emierzwinski-20171101.pdf

9 Remarks of Katie McInnis, Consumers Union, FTC Workshop on Informational Injury (December 12, 2017), Panel 3, https://www.ftc.gov/news-events/audio-video/video/informational-injury-panel-3-business-consumer-perspectives

them that have a profound impact on their lives.[10] 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."[11]

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.[12] The same study reported that 64% of Americans supported greater regulation over how advertisers handle their personal data. Unfortunately, the workshop revealed the limitations of the FTC's privacy framework and its legal capabilities to address these issues and demonstrated why Americans need both comprehensive privacy rights and an independent data protection authority that can enforce them.

Panelists Alessandro Acquisti from Carnegie Mellon University Heinz College,[13] Michelle De Mooy from the Center for Democracy & Technology,[14] and Paul Ohm from Georgetown University Law Center[15] all noted that consumers have intrinsic interests in the collection and use of their personal data and should have some say in that regard. Yet as the recent paper[16] by Harold Feld at Public Knowledge describes in great detail, the basic rights of Americans to own and control their personal information are increasingly being ignored with the deployment of computer networks and the rise of data processing, and the FTC lacks the legal authority to adequately protect their privacy and security. We would also point out that where the FTC does have authority, such as with the Children's Online Privacy Protection Act and the Cable Communications Policy Act, the agency is failing to use it in some cases where we believe that it can and should act to prevent consumer injury.[17]

---

10 Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (2015); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014)

11 Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change* 60 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

12 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/

13 Remarks of Alessandro Acquisti, Carnegie Mellon University Heinz College, FTC Workshop on Informational Injury (December 12, 2017) Panel 2, https://www.ftc.gov/news-events/audio-video/video/informational-injury-panel-2-potential-factors-assessing-injury

14 Remarks of Michelle De Mooy, Center for Democracy & Technology, FTC Workshop on Informational Injury (December 12, 2017) Panel 2, https://www.ftc.gov/news-events/audio-video/video/informational-injury-panel-2-potential-factors-assessing-injury

15 Remarks of Paul Ohm, Georgetown University Law Center, FTC Workshop on Informational Injury (December 12, 2017) Panel 2, https://www.ftc.gov/news-events/audio-video/video/informational-injury-panel-2-potential-factors-assessing-injury

16 Harold Feld, Public Knowledge, *Principles for Privacy Legislation: Putting People Back in Control of Their Information* (December 2017), https://www.publicknowledge.org/documents/principles-for-privacy-legislation

17 See complaint to the FTC by the Electronic Privacy Information Center, the Campaign for a Commercial Free Childhood, the Center for Digital Democracy, and Consumers Union in the Matter of Genesis Toys and Nuance Communications (December 6, 2016), https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf and complaint to the FTC by Public Knowledge, the Center for Digital Democracy, TURN – The Utility Reform Network, Consumers Union, Consumer Action, and Consumer Federation of America in the Matter of Comcast Corp., Cablevision Systems Corp., AT&T, Inc. (June 9, 2016), https://consumerfed.org/wp-content/uploads/2016/06/6-9-16-FTC-Privacy-Complaint_Petition.pdf

As one of the workshop panelists noted, there are instances in which we as a society may believe that parameters should be set for the collection and use of personal information even where there may be an economic or other benefit – for instance, an insurance company's access to information about a consumer's HIV status.[18] Setting such parameters requires enacting legislation and providing for robust rulemaking and enforcement. Instead of going forward, however, we seem to be going backward; for instance, with the Congressional repeal of the Federal Communications Commission (FCC) broadband privacy rules and with the FCC's decision to jettison the rules on net neutrality and reclassify internet service providers, essentially abdicating its responsibility to protect internet users from unfair and abusive practices.

We therefore believe that it is imperative for public policies to be adopted to protect our core values of privacy, human dignity, personal autonomy, security, and fair treatment. These polices should:

- Ensure that the use of individuals' data does not detrimentally affect the services or the terms of service that consumers receive;

- Provide individuals with meaningful control over whether and how their finances, health, race or ethnicity and geo-location is used to target them for advertising or other purposes;

- Mandate that individuals are provided with clear, complete and accurate information about data collection and use;

- Place reasonable limits on the collection and/or use of individuals' data;

- Prohibit "pay for privacy" offers in which individuals are provided greater control over their personal data if they agree to pay a higher price than those who forgo such control;

- Require adequate security of individuals' data and hold those who fail to exercise it accountable through strict liability, meaningful penalties, and requirements to provide compensation to individuals who are affected by such failure;

- Bar forced arbitration provisions in any contracts or terms of service for consumer goods or services; and

- Not interfere with the rights of states to enact their own laws and regulations to protect individuals' privacy and security, or with individuals' rights to bring private actions.

The FTC, with its harm-based approach, jurisdictional constraints, lack of rulemaking authority, inability to assess civil penalties, and pressing responsibilities in other areas such as combatting fraud and policing competition, is not ideally positioned to effectively protect individuals' privacy and security.

---

18 Remarks of James C. Cooper, George Mason University, FTC Workshop on Informational Injury (December 12, 2017), Panel 2, https://www.ftc.gov/news-events/audio-video/video/informational-injury-panel-2-potential-factors-assessing-injury

The United States should establish an independent data protection authority, as exists in most other advanced countries, with the power to examine marketplace practices, promulgate necessary rules, act on complaints, enforce consumers' rights, and ensure compliance with settlements and orders.

In conclusion, we need a legal framework that is based on individuals' rights to own and control their personal information and an agency that can effectively ensure that those rights are respected. Without these measures, public workshops such as this one, while interesting and informative, cannot produce the privacy and security protections that Americans need and deserve.