TECHNOLOGY
POLICY
INSTITUTE

October 26, 2017

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Washington, DC 20580

RE: Informational Injury Workshop P175413

I am submitting these comments to the Federal Trade Commission (FTC) in connection with its Workshop on Informational Injury to be held December 12, 2017. The workshop is intended "to examine questions about the injury consumers suffer when information about them is misused, … how to best characterize these injuries, how to accurately measure such injuries and their prevalence, and what factors businesses and consumers consider when evaluating the tradeoffs involved in collecting, using, or providing information while also potentially increasing their exposure to injuries."[1]

Introduction

The Commission is correct to focus on consumer injury because it is central to a rational privacy regime based on actual harms. Such a regime is most likely to help consumers.

The alternative, favored by many privacy advocates, is to prophylactically limit the collection, use, sharing, and retention of data in an attempt to protect consumers from hypothetical concerns about data being used in harmful ways. This is the approach taken by the Fair Information Practice Principles (FIPPs) dating back to the 1970s, the Organization for Economic Cooperation and Development's (OECD's) Privacy Principles of 1980, and the FTC's own 2012 privacy

[1] "FTC Announces Workshop on Informational Injury", Press Release, September 29, 2017. Retrieved from https://www.ftc.gov/news-events/press-releases/2017/09/ftc-announces-workshop-informational-injury.

report. In a world of big data, however, where innovative new uses of data are unpredictable, the focus on data minimization has come to be seen as increasingly costly.[2]

The existence of actual harms is necessary for any meaningful cost-benefit analysis, whether in the context of privacy liability litigation, FTC enforcement, or regulatory policy. By definition, privacy benefits consist of reducing harms from the misuse of information. Without harms, restricting data use has only costs and no benefits. Thus, regulatory agencies should limit enforcement actions and regulatory prescriptions to cases where there is evidence of harm to consumers.

These comments focus on three issues the FTC's announcement raises:

- The different types of injuries from privacy and data security incidents;
- Consumer decision-making concerning the sharing of information; and
- Business decision-making concerning the collection and use of information.

Injuries from Privacy and Data Security Incidents

A common view is that Internet users don't understand the extent of data collected and how the data are used. If consumers had a better understanding, they would be less willing to share their information. In the next section I discuss why this might not be so and why it might not make sense for rational consumers to spend the additional time and effort required to be better informed about how their data are used.

Privacy advocates enumerate a long list of injuries they believe consumers incur from the use of their information online.[3] Some believe the detailed profiling of individuals violates fundamental rights. Relatedly, some claim that predictive models are harmful because they can be used to make decisions about individuals based on inferences and correlations rather than facts. This claim, if valid, would apply to quantitative analysis used for decision-making throughout the economy. The concern seems to be that these models are not totally accurate. However, more

[2] Executive Office of the President, President's Council of Advisors on Science and Technology, "Big Data and Privacy: A Technological Perspective" May 2014. Hereafter PCAST Report.
[3] For a review of some of these arguments, see Thomas M. Lenard and Paul H. Rubin, "In Defense of Data: Information and the Costs of Privacy," Policy & Internet, vol. 2: iss.1, Article 7 (2010), 166-174. See also Thomas M. Lenard and Paul H. Rubin, "Big Data, Privacy, and the Familiar Solutions," The Journal of Law, Economics & Policy, Vol. 11, No. 1, Spring 2015.

data should make them more accurate and make it more likely that a correct decision will be reached. Then, the relevant question is whether the models reach "better" outcomes than would be achieved otherwise.

Other advocates suggest that personalized advertising manipulates consumers and induces them to purchase items they don't really want or need. This is inconsistent with the modern theory of advertising,[4] which indicates that advertising provides valuable information on prices and product availability. More accurate targeting of advertising should increase the value of the information to the consumer. Moreover, the proposition that advertising manipulates consumers does not seem to be testable, since consumers' preferences are not directly observable except through their behavior. It seems more likely that firms use data to identify and locate consumers who want their products, benefitting both parties.

A recent concern is that data, particularly "big data", can be used in discriminatory ways against income and/or ethnic groups. A 2014 White House Big Data Report argued that "big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace."[5] The evidence supporting the assertion that data are used for discrimination is weak, and the examples are typically hypothetical rather than actual.[6] The argument also ignores the fact that big data can also be used to uncover discrimination that otherwise might not be detected.

Injuries related to security (as distinct from privacy) are more concrete.[7] People may be comfortable with the intended uses of data collected or even new uses that yield better products and services, but worry about unintended uses of information (such as blackmail, extortion, or embarrassment). In other words, they want their data to be secure. Identity theft—which involves

[4] See Paul H. Rubin, "Economics and the Regulation of Deception," Cato Journal, 1991, 667-690; and John E. Calfee, "Fear of Persuasion: A New Perspective on Advertising and Regulation," American Enterprise Institute, Washington, 1997.
[5] Executive Office of the President, President's Council of Advisors on Science and Technology, "Big Data: Seizing Opportunities, Preserving Values," May 2014. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf
[6] See Comments of Thomas M. Lenard to Federal Trade Commission, "Effects of Big Data on Low Income and Underserved Consumers," July 28, 2014.
[7] See Lenard & Rubin (2010), 169-174.

the loss of personal data that poses a financial threat (such as a credit card number)—is perhaps the major privacy concern of individuals.[8]

There are two categories of identity theft. Misuse of an existing credit card or other account—i.e., charging items on someone else's account—constitutes the great majority of the total number of incidents.[9] The costs to consumers of this type of fraud are minimal—a maximum of $50 and frequently only the inconvenience of replacing the card.

The other category consists of opening new accounts in another person's name and related frauds. This latter category—which corresponds more closely to true identity theft—is substantially more costly to businesses and individuals. Victims of this type of identity theft can incur substantial monetary and time costs clearing their damaged credit records.

Javelin Strategy and Research has conducted an annual identity fraud survey since 2003. The most recent report shows fraud losses of $16 billion for 2016, a slight uptick from 2015, but still below each year from 2011 to 2014.[10] The number of fraud victims, however, increased to 15.4 million, a substantial increase over the previous years. The costs of the Equifax breach remain to be seen.

Notwithstanding these data, a recent paper by Wolff and Lehr bemoans the lack of accurate data on the costs of data breaches.[11] For example, they report that estimates of total losses from the 2013 Target breach range from $11 million to $4.9 billion. The lack of good cost data can be an impediment to informed decision making, particularly for firms concerning how much to invest in information security, but also for government policy makers. The authors acknowledge, however, that it is likely that those who need it in the private sector, such as information security and cybersecurity insurance providers, will have more accurate data, but those data are often proprietary.

---

[8] Hal Varian, Google's chief economist, observed that the most common privacy concern expressed by consumers in a focus group was that "someone might steal my credit card number."

[9] See Thomas M. Lenard and Paul H. Rubin, "Much Ado About Notification," Regulation, Spring 2006, 44-50.

[10] "Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study." Press Release, February 1, 2017. Retrieved from https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new.

[11] Josephine Wolff & William Lehr, "Degrees of Ignorance about the Costs of Data Breaches: What Policymakers Can and Can't Do about the Lack of Good Empirical Data." Forthcoming.

The relationship between identity theft and online privacy remains tenuous. Regulating the collection and use of information by legitimate firms does not appear to make it more difficult for criminals to access information such as credit card numbers, and therefore does little or nothing to deter identity theft. Excessive control of information can even have the opposite effect—increasing the risk of identity theft by making it more difficult for sellers to determine if a potential buyer is fraudulent or not.

Evaluating Consumer Benefits and Costs

The Commission asks how "consumers perceive and evaluate the benefits, costs, and risks of sharing information in light of potential injuries…the obstacles they face in conducting such an evaluation [and] how they evaluate the tradeoffs."

The market provides information on how consumers evaluate these tradeoffs and how much consumers are willing to pay for more privacy. Economists usually prefer basing consumers' willingness to pay on observed market behavior, since how people behave when confronted with actual market choices better reflects their real preferences than responses to survey questionnaires or even behavior observed in experiments. The widespread use of free, advertising supported services, such as search, email and online news subscriptions, suggests that people routinely give up some information about themselves in return for access to content, more useful advertising, and other services, although the transaction is indirect. That is, consumers often are willing to exchange less privacy for the resulting benefits.

A recent paper by Athey, Catalani and Tucker[12] supports this observation. Their work highlights the "privacy paradox: Whereas people say they care about privacy, they are willing to relinquish private data quite easily when incentivized to do." Their results suggest, "When expressing a preference for privacy is essentially costless as it is in surveys, consumers are eager to express such a preference, but when faced with small costs this taste for privacy quickly dissipates."

The authors offer a caveat to their finding: "On the one hand it might lead policy makers to question the value of stated preferences when determining privacy policy. On the other hand, it might suggest the need for more extensive privacy protections, from the standpoint that people

[12] Susan Athey, Christian Catalini, and Catherine Tucker, The Digital Privacy Paradox: Small Money, Small Costs, Small Talk, *NBER Working Paper Series.* September 27, 2017.

need to be protected from their willingness to share data in exchange for relatively small monetary incentives."

Closely connected to consumer decision making is the notice and consent framework and whether consumers read privacy notices and are informed about the information practices of the sites with which they share their information. The fact that consumers routinely exchange their information for a variety of benefits, without reading and understanding privacy notices, suggests that most consumers do not find it rational to spend the time and effort to do so. Former FTC officials Howard Beales and Timothy Muris observe that "the reality [is] that decisions about information sharing are not worth thinking about for the vast majority of consumers…"[13]

The recent PCAST report also addresses this issue, observing, "Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent."[14] The report casts doubt on notice and consent as a useful policy tool, noting it "is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data. It is simply too complicated for the individual to make fine-grained choices for every new situation or app."[15]

Business Evaluation of Benefits and Costs

The Commission also asks how businesses evaluate the benefits, costs and tradeoffs involved in collecting and using information and what incentives they face.

Firms have a strong incentive to avoid data security breaches because markets penalize them if breaches occur. Costs include direct costs of addressing the breaches as well as potentially substantial reputational effects, as companies from Target to Equifax quickly learn.

These costs are reflected in stock prices. Spanos and Angelis reviewed the literature on the impact of information security events on stock prices.[16] Of the 28 studies that analyzed the impact of security breaches on the breached firm, 25 (89 percent) found a negative impact. In 20

[13] J. Howard Beales and Timothy J. Muris, "Choice or Consequences: Protecting Consumer Privacy in Commercial Information," *University of Chicago Law Review*: Vol. 75: Iss. 1, Article 6.
[14] PCAST Report, pp. xi.
[15] Ibid, pp. 38.
[16] George Spanos and Lefteris Angelis, "The impact of information security events to the stock market: A systematic literature review," *Computers & Security,* 58 (2016), 2016-229.

of those studies (80 percent), the negative impact was statistically significant. Equifax, for example, lost about $6 billion in market capitalization after its breach, some expect losses to exceed $20 billion, and the firm itself may be in existential danger.[17]

The incentive to reduce costs associated with identity theft is particularly strong for credit card companies, which bear most of the costs. These companies continue to devise new and better security systems as they compete to sign up merchants. While the primary purpose of increasing security is to reduce the costs of fraud to businesses, the costs to consumers are also reduced. The guarantee that consumers are liable for no more than $50 (and often for nothing) if a credit card is misused is essentially a form of insurance provided by issuers and merchants to credit card holders. In a competitive economy, the costs of this insurance are ultimately passed on to consumers in the form of higher prices for goods and services. Thus, the expenditures that businesses make to enhance security (and reduce the costs of fraud) produce benefits in the form of lower prices for consumers.

I hope the Commission finds these comments useful.

Respectfully submitted,

Thomas M. Lenard, Ph.D.
Senior Fellow and President Emeritus
Technology Policy Institute

[17] Michelle Fox, "Equifax will not survive fallout from massive breach, says technology attorney," *CNBC,* September 14, 2017, Retrieved from https://www.cnbc.com/2017/09/14/equifax-will-not-survive-fallout-from-massive-breach-says-technology-attorney.html.