FTC INFORMATIONAL INJURY WORKSHOP

BE AND BCP STAFF PERSPECTIVE | OCTOBER 2018

Introduction

On December 12, 2017, the FTC hosted a workshop in Washington, DC to discuss "informational injuries," which are injuries – both market-based and non-market[1] – that consumers may suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data. There were two main reasons the FTC convened this workshop. First, as then-Acting Chairman Maureen Ohlhausen noted, "in making policy determinations, injury matters…we need to understand consumer injury to weigh effectively the benefits of [government] intervention against its inevitable costs."[2] Second, in order to take law enforcement action against "unfair" acts or practices under the FTC Act, the FTC must demonstrate that the acts or practices "cause or are likely to cause substantial injury."[3] The workshop asked participants to discuss and develop analytical frameworks to help guide future application of the "substantial injury" prong in cases involving informational injury.

Key Takeaways

Several important points emerged from the workshop. First, participants gave several examples of market and non-market informational injuries.

- **Medical Identity Theft.** Medical identity theft occurs when a criminal uses a consumer's identity to access health care services.[4] As one participant noted, in addition to financial injuries that occur when consumers are billed for medical services obtained by a thief,

[1] "Market-based" injuries can be objectively measured—for example, credit card fraud and medical identity theft affect consumers' finances in a directly measurable way. Alternatively, a "non-market" injury, such the embarrassment that comes from a breach of sensitive health information, cannot be objectively measured using available tools because there is no functioning market for it.

[2] *See Informational Injury Workshop Transcript, Remarks of then-Acting Chairman Maureen Ohlhausen, Federal Trade Commission*, at 9-10, *available at* https://www.ftc.gov/system/files/documents/public_events/1256463/informational_injury_workshop_transcript_with_index_12-2017.pdf.

[3] 15 U.S.C. § 45(n).

[4] *See Comment of World Privacy Forum*, at 6, *available at* https://www.ftc.gov/policy/public-comments/2018/01/26/comment-00037.

medical identity theft can also result in inaccurate information in a consumer's medical file, which can have serious consequences to the consumer's safety and treatment.[5]

- **Doxing.** Doxing is the deliberate and targeted release of private information about an individual, often with the intent of harassing or injuring the individual.[6] One participant explained that doxers may release an individual's name, online alias, age, date of birth, address, phone number, medical information, and other sensitive personal information.[7] They may purchase such information online or use online guides on how to use a single piece of an individual's personal information to gather more of that individual's information.[8] They may also use phishing and other social engineering techniques to trick victims into installing malware on their devices.[9] According to this participant, such malware can give the attacker access to the device's files, cameras, and microphones, enabling the theft of information and images, including intimate images that can be used to extort the victim.[10] He noted that young people are particularly susceptible to doxing attacks, which can result in violence, physical threats, emotional harm, and social isolation.[11]

- **Disclosure of Private Information.** Some participants noted that exposure of personal information that a consumer wishes to keep private, such as sensitive medical information, sexual orientation, or gender identity, may cause both market and non-market harm to the consumer.[12] For example, one participant noted that exposure of such information may affect a consumer's ability to obtain or keep employment. Another stated that it may negatively affect the consumer's relationships with family, friends, and coworkers.[13]

---

[5] *See Informational Injury Workshop Transcript, Remarks of Pam Dixon, World Privacy Forum,* at 17-20.

[6] *See Informational Injury Workshop Transcript, Remarks of Prof. Damon McCoy, New York University Tandon School of Engineering,* at 25-26.

[7] *Id.* at 25-26.

[8] *Id.* at 29.

[9] *Id.* at 29.

[10] *Id.* at 30.

[11] *Id.* at 25-30.

[12] *See Informational Injury Workshop Transcript, Remarks of Cindy Southworth, National Network to End Domestic Violence,* at 40-42; *Informational Injury Workshop Transcript, Remarks of Heather Wydra, Whitman-Walker Health,* at 44-49; *see also Comment of Consumer Federation of America, Consumer Action, the Center for Digital Democracy, and U.S. PIRG,* at 2, *available at* https://www.ftc.gov/policy/public-comments/2018/01/26/comment-00036; *see also Comment of Center for Democracy & Technology,* at 2-5, *available at* https://www.ftc.gov/policy/public-comments/2017/10/27/comment-00027.

[13] *See Informational Injury Workshop Transcript, Remarks of Heather Wydra, Whitman-Walker Health*, at 46-47.

- **Erosion of Trust.** According to some participants, privacy and data security incidents may erode consumers' trust in the ability of businesses to protect their data.[14] Without this trust, many consumers may be less willing to share their data or even to engage in e-commerce, depriving them of the benefits provided by the full range of goods and services available.[15] This disengagement can have negative impacts on individual businesses and competition.

Second, participants noted that these injuries, and the risk of these injuries, must be balanced against the value of information collection. One key benefit of information collection is that it supports an ad-funded internet.[16] One participant discussed a survey in which 85% of consumers said they preferred an ad-supported internet model where users do not pay a fee for costs and services.[17] This participant noted the benefits of an ad-supported internet model, not only for large, well-known sites, but also for the ability of small, niche sites to be available to consumers because they are funded by advertising.[18] Another participant discussed the value of being able to use personal data to prevent fraud and verify identities.[19] Yet another participant cited the benefit of services made possible entirely by data, such as Google Maps[20], while another cited to the benefit of personalization.[21]

Third, although no participants disputed that the potential for injuries described above are real, there was robust debate over whether and when governments should intervene to address these injuries, particularly in light of the benefits.[22] Participants noted that flexibility and

---

[14] *See Informational Injury Workshop Transcript, Remarks of Bob Gourley, Cognitio,* at 149; *Informational Injury Workshop Transcript, Remarks of Katie McInnis, Consumers Union*, at 162-163; *see also Comment of Developers Alliance*, at 2-3, *available at* https://www.ftc.gov/policy/public-comments/2017/10/27/comment-00029.

[15] See *Informational Injury Workshop Transcript, Remarks of Heather Wydra, Whitman-Walker Health*, at 46, 52; *Informational Injury Workshop Transcript, Remarks of Cindy Southworth, National Network to End Domestic Violence*, at 54; *Informational Injury Workshop Transcript, Remarks of Pam Dixon, World Privacy Forum*, at 54-55.

[16] *See Comment of American Advertising Federation, American Association of Advertising Agencies, Association of National Advertisers, Data & Marketing Association, Interactive Advertising Bureau, and Network Advertising Initiative*, at 1-2, *available at* https://www.ftc.gov/policy/public-comments/2017/10/27/comment-00022.

[17] *See Informational Injury Workshop Transcript, Remarks of Leigh Freund, Network Advertising Initiative*, at 144.

[18] *Id.* at 145.

[19] *See Informational Injury Workshop Transcript, Remarks of Jennifer Glasgow, Privacy Expert*, at 161-162.

[20] *See Informational Injury Workshop Transcript, Remarks of Bob Gourley, Cognitio,* at 159.

[21] *See Informational Injury Workshop Transcript, Remarks of Prof. Omri Ben-Shahar, University of Chicago Law School*, at 168.

[22] *See Informational Injury Workshop Transcript, Remarks of Prof. Paul Ohm, Georgetown University Law Center*, at 92-95; *Informational Injury Workshop Transcript, Remarks of Geoffrey Manne, International Center for Law & Economics*, at 96-99; *Informational Injury Workshop Transcript, Prof. Alessandro Acquisti, Carnegie Mellon*

innovation are vital to the economy, particularly in emerging technologies.[23] As a result, governments should be judicious in deciding whether to intervene, in order to avoid unintended consequences.[24] Although participants did not agree on the point at which governments should intervene, they appeared to coalesce around several factors that governments should consider:

- First, how sensitive is the data at issue? Sensitive personal information such as Social Security numbers, health information, and financial information will weigh in favor of more protection than less sensitive information.[25]
- Second, how will the information be used? Internal, expected uses would not generate the same level of concern as unexpected uses for some other purpose.[26]
- Third, is the information anonymized or identifiable? Companies may be able to perform analytics and share data for research purposes, for example, which governments may want to encourage, particularly for anonymized information.[27]

Fourth, there was some discussion of whether the definition of injury should include risk of injury. One participant argued that, while it may seem intuitive to measure harm as the negative consequences that result from identity theft or a fraudulent transaction, stakeholders should also consider increased risks of harm caused by certain practices.[28] This participant analogized to a polluter that exposes households to an increased risk of cancer, noting that the polluter should be held responsible for its conduct.[29] In contrast, another participant suggested that risk of injury should not be considered injury, noting that, "[i]f risk of injury were enough to

---

University, at 107-108; *see also Comment of NetChoice,* at 6-7, *available at* https://www.ftc.gov/policy/public-comments/2017/10/27/comment-00020.

[23] *See Informational Injury Workshop Transcript, Remarks of Geoffrey Manne, International Center for Law & Economics*, at 97; *see also Comment of U.S. Chamber Institute for Legal Reform,* at 2-4, *available at* https://www.ftc.gov/policy/public-comments/2017/10/27/comment-00023.

[24] *See Informational Injury Workshop Transcript, Remarks of Geoffrey Manne, International Center for Law & Economics*, at 97.

[25] *See Informational Injury Workshop Transcript, Remarks of Leigh Freund, Network Advertising Initiative,* at 151; *Remarks of Michelle De Mooy, Center for Democracy & Technology,* at 82; *Remarks of Prof. Paul Ohm, Georgetown University Law Center*, at 95; *see also Comment of Information Technology & Innovation Foundation*, at 1-2, *available at* https://www.ftc.gov/policy/public-comments/2017/10/27/comment-00013.

[26] *See Informational Injury Workshop Transcript, Remarks of Katie McInnis, Consumers Union,* at 162-163.

[27] *See Informational Injury Workshop Transcript, Remarks of Prof. James Cooper, George Mason University*, at 102.

[28] *See Informational Injury Workshop Transcript, Remarks of Prof. Ginger Jin, University of Maryland*, at 212.

[29] *Id.* at 213-14.

constitute injury, literally everything, literally the existence of these businesses, would increase the risk of injury and therefore be actionable."[30]

Fifth, there was a great deal of discussion of "the privacy paradox," in which survey evidence indicates that consumers state that they care about privacy, but their behavior is inconsistent with that stated preference.[31] Participants cited to several studies:

- One research project showed that, initially, people took steps to avoid giving their friends' contact information, but once they were offered a slice of pizza, even those people who said they cared deeply about privacy started giving away this data.[32]
- In the same study, respondents were given a variety of wallets in which to store Bitcoin, some of which protected their privacy and some of which did not. The biggest predictor of the wallet they chose was the location of the wallet on the page containing the different choices. When they were given additional information about privacy practices, about half of the respondents changed their behavior.[33]
- Another project showed that 10% of survey respondents stated that they would never choose a streaming video service that collects information about them. Each of these respondents, however, did use a streaming video service that collected information about them.[34]
- In another study, an artist gave away cookies on a sidewalk in New York City in exchange for a piece of personal information. About half of the people who interacted with the artist were willing to let their photograph be taken, about half were willing to give the last four digits of their Social Security number, and one third were willing to give their fingerprints.[35]

Participants discussed several explanations for the privacy paradox. One explanation is that when consumers choose to give away their personal information, they may not understand the risk.[36] As one commenter recognized, "individuals face pervasive asymmetries online" and

---

[30] *See Informational Injury Workshop Transcript, Remarks of Geoffrey Manne, International Center for Law & Economics*, at 85.

[31] *See Informational Injury Workshop Transcript, Remarks of Prof. Catherine Tucker, Massachusetts Institute of Technology Sloan School of Management*, at 229; *see also Comment of Developers Alliance*, at 3, *available at* https://www.ftc.gov/policy/public-comments/2017/10/27/comment-00029.

[32] *See Informational Injury Workshop Transcript, Remarks of Prof. Catherine Tucker, Massachusetts Institute of Technology Sloan School of Management*, at 230.

[33] *Id.* at 240-41.

[34] *See Informational Injury Workshop Transcript, Remarks of Garrett Glasgow, NERA Economic Consulting*, at 236-38.

[35] *Id.* at 238.

[36] *See Informational Injury Workshop Transcript, Remarks of Prof. Ginger Jin, University of Maryland*, at 231.

this "opacity in online data flows further hampers individual's ability to meaningfully evaluate privacy risks and potential benefits."[37] As the participant who discussed the streaming video study pointed out, consumers may alternatively have figured out that a survey is about privacy and understand that their information is being collected, but want to send a signal that they value their privacy.[38] Yet another explanation is that whether consumers care about their privacy depends largely on context. For example, as one participant noted about the study involving cookies, consumers might have concluded that an artist would not be likely to take their fingerprints and rob a bank.[39] Another participant posited alternate explanations. As an example, she stated that, although you could assume that consumers do not care about privacy based on the fact that they do not pursue lawsuits from data breaches, it could be that people who value their privacy do not want to make their name public as part of a lawsuit.[40]

Finally, participants agreed that more research on a broad range of privacy and data security issues would help guide government policy makers and law enforcers in their efforts to prevent and remedy informational injuries, without stifling innovation. Among the specific research ideas raised and discussed were the following:

- Participants suggested conducting surveys of what consumers value in privacy and the protection of data. One participant discussed two potential methods of research. The first is conjoint analysis, where consumers are asked to value two or more products or services with different privacy or security features in order to discover the difference in how much consumers are willing to pay for those services. The second is contingent valuation, where consumers are asked how much more they would pay for a good or service to avoid a bad outcome, such as a data breach.[41]
- One participant suggested using emerging technologies, such as blockchain, to attempt to track how data changes hands to assist in linking data breaches to specific injuries such as identity theft.[42]
- This participant also suggested applying the lessons learned from food and drug safety, product liability, and tort law to privacy markets and data security.[43]

---

[37] *See Comment of Center for Democracy & Technology*, at 11, *available at* https://www.ftc.gov/policy/public-comments/2017/10/27/comment-00027.

[38] *See Informational Injury Workshop Transcript, Remarks of Garrett Glasgow, NERA Economic Consulting*, at 237-38.

[39] *Id.* at 238-39.

[40] *See Informational Injury Workshop Transcript, Remarks of Prof. Josephine Wolff, Rochester Institute of Technology*, at 233-35.

[41] *See Informational Injury Workshop Transcript, Remarks of Garrett Glasgow, NERA Economic Consulting*, at 222-28.

[42] *See Informational Injury Workshop Transcript, Remarks of Prof. Ginger Jin, University of Maryland*, at 252.

- Another participant suggested empirical studies on the efficacy of data protection measures, such as credit card chips and multi-factor authentication. Such studies could help to identify the measures that are most effective at preventing data breaches or mitigating the resulting harm.[44]

FTC staff agrees that further research on these and other privacy and security related topics would be useful. For this reason, the FTC hosts an annual PrivacyCon conference, in which it solicits academic research on the types of issues discussed above, among others. The FTC's next PrivacyCon conference will take place in May 2019. In addition, in June 2018, the FTC announced a series of Hearings on Competition and Consumer Protection in the 21st Century. The hearings include topics related to the work of the Informational Injury Workshop, such as hearings on the intersection between privacy, big data, and competition, and on the Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters. Through these and other vehicles, staff will keep abreast of research and developments in this area, to inform its policy and enforcement efforts.

---

[43] *Id.* at 267.

[44] *See Informational Injury Workshop Transcript, Remarks of Prof. Josephine Wolff, Rochester Institute of Technology,* at 254-56.