THE
NATIONAL LAW REVIEW

FTC Hosts Workshop Highlighting Consumer, Industry, and Law Enforcement Perspectives on Informational Injury

Monday, December 18, 2017

On December 12, 2017, the Federal Trade Commission ("FTC") hosted a workshop examining "informational injury," defined by Acting Chairman Maureen Ohlhausen in her opening remarks as the harm consumers suffer due to privacy and data security breaches.

Chairman Ohlhausen emphasized three main purposes for the workshop: First, to better identify qualitatively different injuries; second, to explore different frameworks for quantifying informational injury and estimating the overall impact of informational injury; and third, to better understand how businesses and consumers weigh the risks around informational injury. Noting the FTC's role in enforcing consumer protections, Chairman Ohlhausen envisioned the workshop as part of an ongoing conversation on consumer injury.

COVINGTON

Article By Covington & Burling LLP
Calvin CohenInside Privacy

Communications, Media & Internet
Consumer Protection
Global
All Federal

The workshop highlighted the tension between the benefits consumers receive when they engage with products that collect their personal information and the potential risks to consumers that data breaches and disclosures of personal information pose. While panelists disagreed on how to define injury and how much risk of injury is acceptable, there was a clear consensus that better definitions for injury and risk are needed to guide consumers, industry, and law enforcement moving forward.

Panel 1: Injuries 101

The first panel brought together a range of experts from different backgrounds to survey the array of injuries and impacts on consumers that may result from privacy and data security breaches. Most people are likely familiar with traditional identity theft schemes and their financial impact. The panelists focused on several emerging types of informational injury as well as unique risks associated with unauthorized disclosures of information:

- **Medical Identity Theft:** Medical identity theft is the unauthorized use of medical information to obtain health care benefits. In addition to the financial consequences that result from theft of an individual's medical identity, a disease or condition may be added to his or her medical file which may have collateral consequences for insurance coverage and future medical treatment.
- **Biometric Identify Theft:** The manipulation of biometric identification systems is becoming more common through technologies such as photo morphing software.
- **Doxing:** Doxing is the researching and releasing of private documents on individuals, typically for the purpose of encouraging harassment of the individual.
- **Algorithmic Decision-Making:** As the volume of consumer data grows, automatic decisions made based on that data become more common. Examples include credit card approvals and predictive policing. There is a growing body of literature examining the intersection of civil rights issues and algorithmic decision-making.
- **Domestic Violence and Stalking:** Victims of domestic violence and stalking face significant risks if their information is disclosed, as disclosures may enable abusers to locate them.

Panel 2: Potential Factors in Assessing Injury

The second panel discussed different policy approaches to identifying informational injury. The panelists represented public policy and legal academia, as well as economic and data privacy research and advocacy organizations. The moderators posed a series of hypothetical privacy and data security disclosures to the panelists and asked them to identify whether these disclosures of consumer information constituted injury. The panelists took a wide range of views when defining and explaining injury.

The panelists disagreed about whether the aggregation of consumer information mitigates potential consumer injury or increases the risk of injury. James C. Cooper, Associate Professor of Law and Director of the Program on Economics & Privacy at the Antonin Scalia Law School, George Mason University, took the position that when data is aggregated, nothing meaningful is disclosed about the individual consumer. Michelle De Mooy, Director of the Privacy & Data Project at the Center for Democracy & Technology, disagreed, arguing that aggregation is meaningless when the aggregated data may be easily re-identified. Georgetown Law Professor Paul Ohm pointed out that if information is so aggregated that it is truly unidentifiable, then it loses its commercial value.

Another area of sharp disagreement between the panelists was whether risk of future injury from disclosure constitutes an injury in and of itself. Professor Ohm explained that in certain areas of the law this theory is already recognized, such as medical malpractice, and they highlighted that consumers experience emotional distress and anxiety when they discover that their private information is vulnerable to disclosure. Ms. De Mooy took the view that all instances of consumer data collection create a risk that the information may ultimately be disclosed, and therefore consumers could be injured every time they are subject to tracking and data collection practices. Geoffrey Manne, Executive Director of the International Center for Law & Economics, pushed back on these points, arguing that there cannot be an injury to consumers just because the risk of disclosure has been increased because defining injury in this way would prevent businesses from taking any risks.

Several panelists focused on the role of consumer agency in assessing whether an injury had occurred. Ms. De Mooy and Professor of Information Technology and Public Policy at Carnegie Mellon University Heinz College Alessandro Acquisti explained that it is integral to ask whether consumers were aware that their data was being tracked, whether they consented to the collection of their information, and whether they understood how their information was being used. Ms. De Mooy expressed a particular concern for the need to increase transparency in data collection practices in order to level the playing field for consumers. Professor Cooper and Mr. Manne both emphasized the benefit to consumers from data collection practices, such as broader information sharing and insights that may be derived from data aggregation.

In discussing the role of government intervention in assessing injury, the panelists took a number of positions. Professor Ohm emphasized the importance of tying government intervention to the level of sensitivity of the information at issue, explaining that government should only intervene to either prevent collection and disclosure practices or respond to a breach where the information at issue is particularly sensitive. Mr. Manne warned against deterring experimentation and the development of new technologies through over-regulation. All the panelists agreed that not all injuries necessitate government intervention and that a clearer definition of injury is needed to guide the FTC in bringing enforcement actions.

Panel 3: Business and Consumer Perspectives

The third panel focused on how businesses and consumers perceive and evaluate benefits, costs, and risks of collecting and sharing information in light of potential benefits and injuries. The panelists represented the business community, legal academia, and advertising, consumer advocacy, and data security organizations.

Regarding the business perspective on informational injury, the panelists agreed that businesses of all sizes account for the risks to consumers in their overall calculus of the benefits of informational injury, but industries vary as to how much risk is too much. Bob Gourley, Partner at Cognitio, stated that the banking industry is largely founded upon consumer trust, so businesses there assess the risks posed by informational injury more heavily than an industry that uses largely publicly available information. Leigh Freund, President & CEO of the Network Advertising Initiative, and Jennifer Glasglow, a Privacy Expert, agreed that that businesses most effectively consider the direct injury to consumers when they obtain the least amount of data necessary to accomplish their organization’s objectives in marketing, analytics, or otherwise.

Other panelists disputed the idea that businesses adequately consider risks to consumers in their actions. Katie McInnis, Policy Counsel at Consumers Union, asserted the many high profile data breaches over the last five years demonstrate how companies’ data practices are misaligned from consumer priorities regarding informational injury. However, some panelists questioned how informed consumers are regarding the risk of informational injury; technology can outpace consumers’ ability to understand its real risks, and academic studies demonstrate that corporate transparency is not totally effective at explaining risks to consumers. Nonetheless, a Omri Ben-Shahar, Professor of Law at the University of Chicago Law School, suggested that the social benefits which emerge when consumers share their information, like personalized services, may influence organizational

weighting of informational injury.

When the discussion shifted to the consumer perspective, the panelists disagreed over how consumers actually view informational injury. Some argued that injury can be highly contextual, particularly with data breaches, as consumers will have different levels of exposure and different understandings of the risks. Others argued that consumers must vary their views because industries are fragmented, and data policies in one industry differ from those in another. But all agreed that the relative immaturity of the big data market and its complexity are obstacles to accurately assessing the costs and benefits of information sharing.

The panelists had a lively discussion about the market for privacy products and services. Ms. McInnis argued that there is a desire for consumer-based privacy solutions, but that consumers do not feel there is a way to effectuate their concerns either in the marketplace or through regulatory action. Other panelists agreed with this sentiment, stating that emerging privacy products and services are predominantly private sector-oriented. But Mr. Ben-Shahar questioned whether consumers really desire increased privacy given their actual behavior, such as continuing to use online services with unclear data security. Ms. Freund analogized consumer behavior regarding informational injury to air travel: consumers fly on airplanes all the time, but they do not know the mechanical manuals, specifications, or what they say regarding the plane; rather, they trust that the mechanics know what they are doing, and they similar trust in businesses.

The panelists suggested varied approaches going forward. To ensure consumer protection, Ms. McInnis suggested that the FTC's rulemaking powers should be enlarged to act before informational injuries occur. Mr. Gourley believed that current law, such as tort law, sufficiently protects consumers and keeps businesses accountable. And many panelists claimed that businesses were appropriately self-regulating to safeguard consumer information.

Panel 4: Measuring Injury

The fourth panel examined different methods for and challenges in assessing and quantifying informational injury. The panelists represented the private sector, legal academia, and the government, and each currently conducts research into methods for measuring informational injury.

First, the panelists discussed the ways to measure consumer statements and value regarding informational injury. Most of the panelists stated that survey-based data is currently the most widely recognized method, but all acknowledged its shortcomings. Chief among these is the "privacy paradox": consumers rate as highest their data privacy concerns, but their actual behavior regarding data privacy is inconsistent with such a high preference. Ginger Jin, Professor of Economics at the University of Maryland, suggested that the measurement of informational injury should account for both survey-based data and consumers' "stated" versus "revealed" preferences like the "privacy paradox."

Similarly, the panelists discussed the challenges inherent to measuring the outcomes from informational injury. Part of the difficulty stemmed from what types of informational injuries had occurred. Instances where a company had deprived a consumer of the "benefit of the bargain," such as promising but failing to provide data security, were easier to quantify than uncertain outcomes. Garrett Glasgow, Senior Consultant at NERA Economic Consulting, gave as an example of an uncertain outcome a company promising not to transfer a consumer's data but then suffering a data breach in which a hacker gains the consumer's information. In such an instance, the consumer clearly suffered an injury, but measuring the harm is difficult because multiple factors (e.g., the black market price of that consumer's information, any remedial data security measures taken, and the amount of time taken to fix the problem) are potentially in play.