



**Comments of the
Software & Information Industry Association (SIIA)
on the
Federal Trade Commission Hearings on Competition and
Consumer Protection in the 21st Century
August 20, 2018**

Topic #5: The Commission’s remedial authority to deter unfair and deceptive conduct in privacy and data security matters

About SIIA

With nearly 700 member companies, SIIA is the principal trade association of the software and digital content industries. Our members are global industry leaders in the development and marketing of software and electronic content for business, education, government and consumer markets. They range from start-up firms to some of the largest and most recognizable corporations in the world. SIIA member companies are leading providers of, among other things:

- Data analytics and artificial intelligence,
- business, enterprise and networking software,
- publishing, graphics, and photo editing tools,
- corporate database and data processing software,
- financial trading and investing services, news, and commodities,
- online legal information and legal research tools,
- education software, digital content and online education services,
- specialized business media,
- open source software, and
- many other products and services in the digital content industries.

Introduction

In 2017, the Commission undertook a valuable exercise in assessing its deception and unfairness authority under Section 5, appropriately described in this context by Acting Chairman Maureen Ohlhausen as an exploration of “informational injuries.” The Commission’s authority in this area has proven to be quite broad, albeit challenging to apply in some cases where injuries are hard to identify. Based on a range of comments and discussion at the informational injury workshop, there appears to be broad agreement that privacy and data security incidents (involving various types of sensitive data) can and have caused injuries that do not involve solely financial loss. There was also substantial agreement that government intervention ought to be tied to injury, whatever the definition, and that countervailing benefits must be evaluated as well.¹

¹ Ohlhausen, Maureen. [Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases](#) (September 19, 2017).

Given the various elements that contribute to the effort to measure injury, e.g. the type of injury, the sensitivity of the data, the magnitude, the frequency, and the causal link to a particular firm or practice, SIIA urges the Commission to continue assessing these on a case-by-case basis, with a thorough economic assessment of both risks and benefits to consumers and businesses. SIIA recommends that the Commission continue its focus on refining and clarifying the notion of informational injury as a guide to its enforcement actions.

We urge the Commission to consider the following elements when applying its broad Section 5 authority with respect to these informational injuries.

The Commission should recognize that consumer privacy expectations evolve with changes in technology and business practice.

As technologies evolve to become more personalized and instrumental in all facets of our lives, our preferences and expectations of privacy also evolve. In our 2014 white paper, SIIA explained how the rise off big data and data-driven innovation have led to evolving consumer expectations about data collection and use.² This evolution has been quite rapid over the last decade, particularly as smartphones and apps have provided a range of personalized consumer experiences.

For instance, growing experience with apps and the broad utilization of concise notices before mobile apps are downloaded or used have led to widespread consumer understanding that apps often incorporate various different types of data from their devices to provide new and innovative services. Although the Internet of Things is still in its very early stages, consumer understanding and expectations are already beginning to change, as more and more consumers recognize the opportunities for data-driven innovation that has moved from the devices in the palms of their hands, to devices all around us.

The Commission examined consumer expectations across platforms during its 2016 review of Smart TVs. Key conclusions established at its December workshop were that context is a critical element of data collection, and that consumer understanding and expectations about data practices change over time.³ Consumer Protection Director Jessica Rich acknowledged that, “consumers expect some level of data collection when they use their computer.”⁴ As digital innovation continues to expand to more aspects of our lives, it is reasonable for the Commission to anticipate that consumer privacy expectations will continue to evolve. Consumers will have increasingly sophisticated understandings of data uses and the benefits they provide.

The Commission must determine materiality in deception cases.

Section 5 of the FTC Act prohibits deceptive or misleading acts or practices. The injury to a misled consumer is that they took an action that, in the absence of deception, they might not have taken. The act or practice involves the withholding of information that would have had a material impact on the consumer’s choice.

² SIIA, [Data-Driven Innovation, A Guide for Policymakers: Understanding and Enabling the Economic and Social Value of Data](#) (2015).

³ FTC, [Fall Technology Series: Smart TV](#) (December 7, 2016).

⁴ Schiff, Allison, [The FTC Has Its Eye On What Smart TVs Mean For Consumer Privacy](#), AdExchanger (December 8, 2016).

In deception cases involving privacy, the Commission must assess whether consumers might have made a different decision if not for a false or misleading statement or lack of disclosure in a privacy policy or other public statement about data practices. Enforcement actions in cases where the lack of disclosure or false or misleading statements seem incidental to any possible change in consumer behavior raise concerns as they may impose burdens on companies without actually remedying a consumer injury.

Perhaps no case highlights this point more than *Nomi Technologies*. In 2015, a split Commission charged that the startup company tracked consumers in retail stores through mobile device information and offered retail merchants the ability to analyze aggregate data about their consumer traffic. The company promised to provide an opt-out for consumer both in stores and online but did not follow through with the in-store opt-out. The Commission said that this failure to provide the promised in-store opt-out was deceptive.⁵

SIIA shares the concerns expressed by the dissenting Commissioners. Commissioner Wright pointed out that the Commission’s complaint lacked the evidence that Nomi’s representation about an opportunity to opt-out of their service at the retail level was material to consumers.⁶ Then-Commissioner Ohlhausen warned, “...we should not apply a de facto strict liability approach to a young company that attempted to go above and beyond its legal obligation to protect consumers but, in so doing, erred without benefiting itself.”⁷

Going forward, the Commission should carefully analyze deception cases to ensure that there is evidence of materiality and that consumers really might have made different decisions had the information available to them been different.

The Commission should utilize unfairness authority cautiously to protect consumers from concrete informational harms.

Under Section 5 of the FTC Act, an “unfair” act or practice is one that “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”⁸ SIIA agrees that unfairness authority can be an important and useful tool, enabling the Commission to address concrete harms that occur outside of deception. However, unfairness is also a narrow tool, that can be applied only on the basis of a specific statutory three-step analysis of consumer injury.⁹

This three-step test analysis requires that to justify a finding of unfairness the injury must satisfy three tests: It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided.¹⁰

Monetary, health and safety risks are common injuries considered “substantial,” but as the Commission defined in its policy statement, “[e]motional impact and other more subjective types of harm, on the

⁵ FTC, [Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices](#) (April 23, 2015).

⁶ [Dissenting Statement of Commissioner Joshua D. Wright In the Matter of Nomi Technologies, Inc.](#) (April 23, 2015).

⁷ [Dissenting Statement of Commissioner Maureen K. Ohlhausen in the Matter of Nomi Technologies, Inc.](#) (April 23, 2015).

⁸ 15 U.S.C. Sec 45(n)

⁹ Beales, Howard, [The FTC’s Use of Unfairness Authority: Its Rise, Fall, and Resurrection](#) (May 30, 2003).

¹⁰ [FTC Policy Statement on Unfairness](#).

other hand, will not ordinarily make a practice unfair. Thus, for example, the Commission will not seek to ban an advertisement merely because it offends the tastes or social beliefs of some viewers....”¹¹

The Commission should continue to examine practices involving sensitive information with special care in assessing unfairness. The Commission defines sensitive information to include financial information, health information, Social Security Numbers, and information about children.¹² In addition it is sensible to pay attention to the reasonable expectations people have developed about the collection and use of information in particular contexts.¹³

But neither of these considerations should take the place of a specific demonstration of consumer injury that satisfies the three-step test for a finding of unfairness. The FTC’s recent action against Vizio is illustrative of the difficulties in this area. SIIA shares the concerns that Acting Chairman Ohlhausen raised about this case.

In *Vizio*, the Commission alleged that the company collected “the sensitive television viewing activity of consumers.” This was done in “a medium that consumers would not expect to be used for tracking” and “without consumers’ consent.” The Commission ultimately concluded that consumers do not expect tracking and might choose a different television if they knew of it, they the Commission determined that such information would be material to consumers and the failure to disclose it was deceptive.

But the Commission also concluded that this collection and sharing of sensitive data without consumers’ consent was unfair tracking.¹⁴ Acting Chairman Ohlhausen pointed out that the Commission had not previously determined television viewing data to be sensitive and raised a question whether there it had really established substantial consumer injury. In fact, it was this case that led to the Commission inquiry into the nature of “substantial injury” in the context of information about consumers.¹⁵

Going forward, SIIA recommends that the Commission rigorously apply the three-step test for substantial consumer injury in unfairness cases and determine whether informational injury rises to the level of an unfair practice.

Cost benefit analysis should play an important role in unfairness cases.

The OECD has concluded that data-driven innovation forms a key pillar in 21st century sources of growth, concluding that “big data” has become a core asset in the economy, fostering new industries, processes and products and creating significant competitive advantages.¹⁶ Data-driven innovation has also been credited with spurring new industries, processes, and products; and creating significant competitive advantages. In this sense, data-driven innovation has become a key pillar of 21st-century growth, with the potential to significantly enhance productivity, resource efficiency, economic

¹¹ Ibid.

¹² FTC, [Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers](#) at 59 (March 2012).

¹³ Mayer-Schönberger, Viktor; Cate, Fred; Cullen, Peter, [Reinventing Privacy Principles for the Big Data Age](#). Oxford Internet Institute (December 6, 2013).

¹⁴ FTC. [Complaint for Permanent Injunction and Other Equitable and Monetary Relief](#) (February 6, 2017).

¹⁵ [Concurring Statement of Acting Chairman Maureen K. Ohlhausen in the Matter of Vizio, Inc.](#) (February 6, 2017).

¹⁶ [Data-Driven Innovation: Big Data for Growth and Well-Being](#). OECD (September 5, 2017).

competitiveness, and social well-being.¹⁷ While not all of the data powering data-driven innovation is consumer information, it is a key component of the digital economy, which accounts for an estimated six percent of GDP annually.¹⁸ Indeed, consumer data is also vital in powering socially beneficial programs, such as building smart cities, addressing health crises, and advancing scientific research.

The Commission's enforcement actions should involve rigorous economic and empirical analyses that assess whether the injuries are "material" or "substantial," in deception and unfairness cases respectively. Measuring either benefits or costs may be difficult in particular situations, especially because they are often measured in different terms, e.g. safety risks versus dollar costs. Nonetheless, such tradeoffs are real. As Howard Beales has long opined, these benefits should be thoroughly evaluated, not swept under the rug.¹⁹ This was true in 2003 when Mr. Beales served as the Director for the Consumer Protection Bureau and is even more so now that data-driven innovation has further altered the difficult equation.

By providing the ability to substantially enhance consumers' quality of life, such as through critical health and education outcomes, data-driven innovation has made it more essential than ever to weigh the benefits against the costs on a case-by-case basis. Indeed, theoretical and empirical research reveals that characterizing a single unifying economic theory of privacy is hard, because privacy issues of economic relevance arise in widely diverse contexts, and in situations where the protection of privacy can both enhance, and detract from, individual and societal welfare.²⁰ For instance, personal data has driven revolutionary new services (such as search engines and recommender systems), new companies (such as social networking sites and blogging platforms), and even new markets have emerged, such as emerged crowdsourcing.²¹

As former Commissioner Josh Wright has explained, "[a]n economic approach to privacy regulation is guided by the tradeoff between the consumer welfare benefits of these new and enhanced products and services against the potential harm to consumers, both of which arise from the same free flow and exchange of data.²² He has also described the Commission's recent environment as having a "generalized apprehension about the collection and use of data – whether or not the data is actually personally identifiable or sensitive – along with a corresponding, and arguably crippling, fear about the possible misuse of such data."²³

The necessary cost benefit balance is therefore not just about weighing risks against economic benefits, but rather measuring risks of harm against broader consumer and societal benefits from new innovative uses of data. The Commission must recognize these opportunities and place a greater emphasis on enforcement actions only in cases where there is actual, concrete harm. Bringing enforcement actions where the consumer harm is merely speculative or presumed, or without a full assessment of the benefits provided by the use of data, risks crippling data-driven innovation and its transformative economic and societal benefits throughout the United States.

¹⁷ Ibid.

¹⁸ Siwek, Stephen, [Measuring the U.S. Internet Sector](#), Internet Association (2015).

¹⁹ Beals, Howard, [The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection](#) (2003).

²⁰ Acquisti, Alessandro; Taylor, Curtis; Wagman, Liad, [The Economics of Privacy](#) (March 27, 2015).

²¹ Ibid.

²² Wright, Joshua, [The FTC and Privacy Regulation: The Missing Role of Economics](#) (November 12, 2015).

²³ Cooper, James; Wright, Joshua, [The Missing Role of Economics in FTC Privacy Policy](#) (January 5, 2017).

The Commission should take steps to preserve its role in enforcing reasonable security requirements.

Since 2002, the FTC has brought over 60 cases against companies that have engaged in unfair or deceptive practices that failed to adequately protect consumers' personal data.²⁴ The pattern is for the Commission to find that a company failed to establish and maintain reasonable security practices and then to impose on the company a security program that mirrors many of the requirements of the FTC's Safeguard Rule.²⁵

In 2015, the Third Circuit upheld the Commission's authority to regulate information security practices.²⁶ In 2018, however, the Eleventh Circuit vacated the Commission's LabMD enforcement order, thereby creating confusion about the FTC's information security enforcement authority going forward.²⁷

The Eleventh Circuit reasoned that the Commission's LabMD security order is unenforceable because it is "devoid of any meaningful standard informing the court of what constitutes a 'reasonably-designed' data-security program." In the event of an enforcement action, the court would have to evaluate dueling opinions from the Commission and the defendant on whether the company's security practices were reasonable without any clear standard to guide it.

SIIA supports continued FTC authority and enforcement action in this area. It is an important element in moving the country to a higher level of information security. It will be especially important to have a strong cop on the beat as connected devices are deployed throughout society, and keeping the information gathered from distant sensors becomes increasingly urgent.

SIIA urges the Commission to craft its future orders on privacy and data security in a way that meets the concerns of the LabMD decision and provides clearer guidance for companies seeking to put in place and maintain reasonable security measures.

²⁴ FTC, [Privacy and Security Update: 2017](#)

²⁵ 16 CFR Part 314

²⁶ *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

²⁷ *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir. 2018)