Before the
Federal Trade Commission
Washington, D.C. 20024

Comments of the
Software & Information Industry Association

Regarding

Informational Injury Workshop (P175413)

Ken Wasch
President
Software and Information Industry
Association
1090 Vermont Ave. NW Sixth Floor
Washington, D.C. 20005-4905
Phone: (202) 289-7442

October 27, 2017

I. Introduction

On behalf of the Software & Information Industry Association (SIIA), thank you for the opportunity to provide comments regarding the upcoming workshop on December 12, 2017, to examine consumer injury in the context of privacy and data security.

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.

SIIA supports the Federal Trade Commission's ("FTC" or "Commission") assessment of consumer injury in the context of privacy and data security. As the Commission has appropriately noted, information flows in general, and the transmission of consumer information in particular, are often critical to cutting edge products and services and essential new business models that drive the digital economy. The Commission must therefore tailor its approach to regulation and enforcement, realizing that an overbroad definition of informational injuries threatens the necessary data flows and data-driven innovation that power 21st Century economy.

With these comments, SIIA discusses the following key aspects of regulation and enforcement of informational injuries:

- The need to recognize evolving consumer privacy expectations when assessing harms;
- The increased importance of cost-benefit analysis to maintaining data-driven innovation;
- The need to prioritize enforcement around specific statutes where Congress has determined heightened risk to consumers;
- The need to rigorously assess materiality in deception cases;
- The value of maintaining a case-by-case approach to unfairness enforcement that relies heavily on the three-step test, rather than adopting a prescriptive ex-ante approach or assume harm based on the nature of the information involved.

II. Diverse and Evolving Consumer Privacy Expectations Are Critical to the Need for an Evolving Concept of Consumer Harm.

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.[1] This evolution has been quite rapid over the last decade, particularly as smartphones and apps have provided a range of personalized consumer experiences.

For many years, most consumers have understood and appreciated the value of online personalized advertising, based on their interests and experiences. Further, as they have become accustomed to smartphones and apps powered by data-driven innovation, consumer expectations have rapidly evolved. For instance, the broad utilization of concise notices before mobile apps are downloaded or used has led to consumers now commonly 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-

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

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, revealing that these expectations are increasingly converging. 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.[2] Consumer Protection Director Jessica Rich acknowledged that, "consumers expect some level of data collection when they use their computer." [3] This statement represents a fundamentally different environment than just 10 years ago, when consumers were not nearly as knowledgeable about interactive advertising.

As digital innovation continues to expand to more aspects of our lives, it would be unreasonable to predict that these expectations will not evolve in the very same way that they did with each new technological advancement, leading to an environment where consumers have increasingly sophisticated understandings of data uses and the benefits they provide. The dynamic, interactive connected device environment has led to an increased recognition about the need for policymakers and regulators to focus less on data collection and the attending notice and consent mechanisms, and focus more on a practical assessment of the risks of concrete harms (and benefits) associated with data uses.[4]

In further assessing what types of information it considers to be "sensitive," the Commission should refrain from drawing conclusions that are likely to become outdated and inconsistent in a matter of years. Rather, the Commission should continue to perform a case-by-case assessment of information collection and use, assessing the potential for consumer injury. Therefore, as the Commission assesses what constitutes informational injuries, it is critical to carefully apply regulation and enforcement actions to balance the potential for consumer harm against transformational benefits of data-driven innovation, such as opportunities to enhance public health, environmental protection and education, among others.

---

[2] FTC. Fall Technology Series: Smart TV. December 7, 2016.
[3] Schiff, Allison. The FTC Has Its Eye On What Smart TVs Mean For Consumer Privacy. AdExchanger. December 8, 2016.
[4] Mayer-Schönberger, Viktor; Cate, Fred; Cullen, Peter. Reinventing Privacy Principles for the Big Data Age. Oxford Internet Institute. December 6, 2013.

III. Cost benefit analysis has often been lacking in previous unfairness, and it should be fortified to account for data-driven innovation.

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.[5] 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 competitiveness, and social well-being.[6] 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.[7] 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.[8] 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

[5] Data-Driven Innovation: Big Data for Growth and Well-Being. OECD. September 5, 2017.
[6] Ibid.
[7] Siwek, Stephen. Measuring the U.S. Internet Sector, Internet Association. 2015.
[8] Beals, Howard. The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection. 2003.

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.[9] For instance, the value 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.[10]

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.[11] 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."[12]

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.

IV. Congress has created multiple statutory frameworks to specifically address circumstances that require increased privacy protections, the Commission should prioritize these areas for enforcement.

At the direction of Congress, the FTC is responsible for enforcing a wide range of privacy and data security statutes—at least in part. That is, specific consumer protection statutes, such as the Equal Credit Opportunity Act, Truth-in-Lending Act, Fair Credit Reporting Act, the Do-Not-Call

[9] Acquisti, Alessandro; Taylor, Curtis; Wagman, Liad. The Economics of Privacy; March 27, 2015.
[10] Ibid.
[11] Wright, Joshua. The FTC and Privacy Regulation: The Missing Role of Economics. November 12, 2015.
[12] Cooper, James; Wright, Joshua. The Missing Role of Economics in FTC Privacy Policy. January 5, 2017.

Implementation Act of 2003, the Children's Online Privacy Protection Act, Fair and Accurate Credit Transactions Act of 2003 and others that prohibit specifically-defined practices and generally specify that violations are to be treated as if they are unfair or deceptive acts or practices under Section 5.

These statutes, taken together, reveal that Congress has repeatedly identified the need for increased privacy protections where information is collected by certain types of entities, such as health care providers, and for certain types of sensitive information, such as children's information. While the bulk of these statutes seek to protect against the risk pertaining to eligibility determinations and the financial, health and safety of consumers, COPPA and the Do-Not-Call Act identify that Congress has provided the Commission with specific regulatory and enforcement authority to ameliorate these risks. In light of this targeted sectoral privacy framework established by Congress, the Commission should prioritize enforcing informational injuries within these areas.

V. When considering informational injury in the deception context, the Commission should be sure to determine materiality, not merely incidental discrepancies in privacy policies.

Substantial injury is not a prong of the deception legal analysis, which focuses instead on materiality. The injury to a misled consumer is that they took an action that, in the absence of deception, they might not have taken. Thus, this materiality requirement is a proxy for harm to consumers, which follows from the requirement in the FTC Act that consumer injury be apparent in conduct that violates the statute. After all, per the FTC Act, "…the term 'unfair or deceptive acts or practices' includes such acts or practices involving foreign commerce that… cause or are likely to cause reasonably foreseeable injury within the United States."[13]

Given the broad and rapidly evolving technological landscape, as well as the continually evolving set of consumer expectations regarding privacy, the Commission's assessment of information injury is critical. As Acting Chairman Ohlhausen recently stated, "regardless of the legal authority being used, the Commission, as a matter of good governance, should always consider consumer injury in determining what cases to pursue."[14]

[13] 15 U.S.C. Sec. 45(a)(4)(A)
[14] Ohlhausen, Maureen. Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases. September 19, 2017.

Therefore, when looking at deception cases and assessing the potential for informational injury, the Commission's determination of a "material" misrepresentation or practice must assess whether it is likely to affect a consumer's choice of or conduct regarding a product or service—that is, to consider whether there is injury to the consumer because they might have made a different decision if not for a false or misleading statement in a privacy policy or other public statement about data practices. This analysis should take into account whether the "reasonable consumer" is actually reading and relying on the alleged misstatement, which often is not the case with privacy policies. Thus, any representations ought to be found to have a substantial impact on the consumer and rigor should be applied by the Commission in deception cases to establish that privacy policy statements are proven (and not presumed) to be material to consumers.

As former Commissioner Wright consistently pointed out, it is critical that the Commission exercise prosecutorial discretion, urging the Commission not to expend finite resources exercising Section 5 deception authority when discrepancies between privacy policies and actions are incidental, and not material. Acting Chairman Ohlhausen has also underscored this line of thinking, very effectively articulating the critical need for the Commission to prioritize action to resolve areas of *real* consumer harm that the market and private arrangements cannot address well on their own now. [15] This approach is consistent with the FTC Act's focus on actual harm for both deceptive and unfair enforcement.

Perhaps no case highlights this point more than *Nomi Technologies*. In 2015, a split Commission charged that the startup company offering retail merchants the ability to analyze aggregate data about consumer traffic, was deceptive for promising to provide an opt-out for consumer both in stores and online, and not following through with the in-store opt-out.[16] On behalf of its clients, Nomi passed smartphone MAC addresses through a cryptographic hash function before collection and created a persistent unique identifier for the mobile device. Nomi did not "unhash" this identifier to retrieve the MAC addresses and Nomi did not store the MAC addresses of the mobile devices. Therefore, Nomi was not collecting any personally identifiable information and had no obligation to offer consumers *any* opt-out. This promise for an in-store opt-out was a well-intended

[15] Ohlhausen, Maureen. Regulatory Humility in Practice. April 1, 2015.
[16] FTC. Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices. April 23, 2015.

addition to the opt-out that was provided for on its website, but Nomi's retail partners did not ultimately provide for this opt-out to become a reality.

In a dissenting opinion, 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.[17] In addition to the lack of materiality, Section 5(b) of the FTC Act requires the Commission, before even issuing any complaint, to establish a reason to believe that a violation has occurred and that an enforcement action would "be to the interest of the public."[18] 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."[19]

SIIA concurs with the dissent of Commissioners Wright and Ohlhausen in *Nomi*, on the grounds that because there was no evidence of materiality, there was no real harm to consumers, and therefore the Commission should have not issued an order in this case. In addition to expending its limited resources on a case where consumer harm is not present, *Nomi* does a disservice to consumers by creating a disincentive for companies set a high bar for consumer notice and choice. Further, given that this case deals with anonymized data, there is no privacy violation.

VI. The Commission should utilize unfairness authority cautiously to protect consumers from concrete harms, without adopting an overly-broad interpretation of what constitutes an informational injury.

As noted above, a wide range of existing statutory frameworks provide substantial opportunity for the FTC to protect against informational injuries. Therefore, the Commission should not seek to expand its unfairness enforcement based on an overly-broad interpretation of what constitutes an informational injury. To be sure, the Commission's unfairness jurisdiction was defined by statute to be exercised only where there is actual, provable consumer harm. As defined by the FTC Act, an "unfair" trade practice is one that "causes or is likely to cause substantial injury to consumers which

[17] Dissenting Statement of Commissioner Joshua D. Wright In the Matter of Nomi Technologies, Inc. April 23, 2015.
[18] 15 U.S.C. Sec 45(b)
[19] Dissenting Statement of Commissioner Maureen K. Ohlhausen in the Matter of Nomi Technologies, Inc. April 23, 2015.

is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[20] 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 can also be misused, particularly if the Commission strays from a principled basis for applying it.[21]

The three-step test remains as the essential starting point for the Commission to ensure that it does not misuse its authority in this area. Directed by the FTC Act, the Commission outlined in its unfairness policy statement that in order 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.[22]

While this test presents clear-cut guidelines for the Commission's enforcement, it also poses significant questions that the Commission must assess on a case-by-case basis, such as determining what constitutes substantial injury, the cost-benefit analysis and the avoidability of the injury. 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 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…." [23]

Another key element in the assessment of informational injury in the unfairness context is evaluating the sensitivity of the information and therefore the potential risk. Of course, this approach does not lend itself to a clear formula for determining unfair practices, as the costs and benefits of the use of that information varies significantly on a case-by-case basis. The Commission has long defined sensitive information to include financial information, health information, Social

[20] 15 U.S.C. Sec 45(n)
[21] Beales, Howard. The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection. May 30, 2003.
[22] FTC Policy Statement on Unfairness.
[23] Ibid.

Security Numbers, information about children.[24] It is reasonable to recognize the potential sensitivity of data that, if misused, has a reasonable expectation of leading to monetary, health or physical safety risks. However, the Commission should be careful to ensure that actual, concrete harm has occurred before asserting that a practice is unfair. That is, it should look not only at the potential sensitivity of the data, but whether such data was actually used in a way that would lead to substantial consumer injury. The FTC should not presume consumer harm due to the sensitivity of the information involved, but instead must analyze the totality of the circumstances as required under the three-part unfairness test.

Some have suggested that the Commission's unfairness authority is applicable in any case where an information collection practice or use is "unreasonable" for not being consistent with consumers' expectations. The challenges with this approach are two-fold. First, it does not comport with the requirement to assess the likelihood of concrete, substantial injuries; and second, consumers don't maintain uniform expectations around various data collection and use practices, to the extent that they constitute a consistent reasonable expectation of privacy—again, these expectations are evolving rapidly along with technology. Related to this, it has been suggested that the Commission could map the Fair Information Practice Principles (FIPPs) to its unfairness test, but FIPPs represent only conceptual, broad statements about privacy values, and their precise formulation and meaning have frequently been disputed and debated.[25]

The FTC's recent action against Vizio highlights the importance of a clear articulation of actual, tangible consumer harms caused by an allegedly unfair practice, and the confusion that arises when the Commission strays beyond the statutory limits of Section 5. The mere fact that personal information was collected without a consumer's knowledge does not lead to an unfair practice. In *Vizio*, the Commission recently alleged that the company omitted information about its data collection and sharing program; that consumers do not expect televisions to collect and share information about what they watch; and therefore that this omission is deceptive because it is

[24] FTC. Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers. March 2012. at 59.
[25] Mayer-Schönberger, Viktor; Cate, Fred; Cullen, Peter. Reinventing Privacy Principles for the Big Data Age. Oxford Internet Institute. December 6, 2013.

material to consumers who might have otherwise chosen an alternative television.[26] However, as Acting Chairman Ohlhausen pointed out, her concerns with any unfairness claim, given that the information collected was viewing activity, and the Commission has not previously determined television viewing data to be "sensitive information," she found that the Commission had not established a substantial risk of injury.[27] The Commission failed to articulate any actual, tangible harm to consumers and instead presumed injury based solely on the nature of the information involved.

Additionally, compared to the other types of data that have been determined sensitive by the Commission, television viewing data does not pose an increased potential for monetary, health or safety risks. *Vizio* presents an example for future cases where the Commission must always perform a thorough cost-benefit analysis of the potential benefit of the collection and sharing, and articulate with specificity the tangible harm causing substantial injury to consumers.

In summary, a prescriptive ex-ante approach to unfairness enforcement, particularly one based on an ambiguous notion of "unreasonableness" or the FIPPs, is less desirable than a case-by-case approach that relies heavily on the three-step test. SIIA encourages the Commission to continue rejecting calls to develop such a prescriptive framework based on an ever-evolving notion of a reasonable expectation of privacy. The Commission must instead rigorously apply the three-step test, and ultimately determine whether informational injury rises to the level of an unfair practice. In these cases, the Commission should be careful about creating new categories of "sensitive" information, or presuming harm based on the nature of the information involved, and also be mindful of evolving privacy ideals and expectations by consumers.

[26] FTC. Complaint for Permanent Injunction and Other Equitable and Monetary Relief (368.79 KB). February 6, 2017.
[27] Concurring Statement of Acting Chairman Maureen K. Ohlhausen in the Matter of Vizio, Inc. February 6, 2017.

VII. Conclusion

Again, thank you for the opportunity to provide written comments in advance of the workshop on December 12, 2017, to examine consumer injury in the context of privacy and data security. With these comments, SIIA also requests the opportunity to participate in the workshop.