

Before the
Federal Trade Commission
Washington, DC

In re

Informational Injury Workshop

Project No. P175413

**COMMENTS OF
COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION**

Pursuant to the request for comments¹ issued by the Federal Trade Commission (FTC or the Commission), the Computer & Communications Industry Association (CCIA) submits the following comments on the subject of consumer injury in the context of privacy and security, in preparation for a public workshop on informational injury.

CCIA represents large, medium, and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications, and Internet products and services. Our members employ more than 750,000 workers and generate annual revenues in excess of \$540 billion.²

I. Introduction

CCIA commends the Commission for organizing the coming workshop to examine consumer injury in the context of privacy and security, and for its framing in this request for comments. Importantly, with respect to privacy harms, the Commission seeks input on the

¹ *Notice of Workshop and Request for Public Comments*, Project No. P175413, available at <https://ftcpublishcommentworks.com/ftc/informationalinjuryworkshop/>

² A list of CCIA members is available at <http://www.cciagnet.org/members>.

different types of injuries consumers may suffer from privacy and data security incidents, and how these injuries might be assessed by consumers, companies, and regulators.

The FTC should ensure that in the context of its enforcement that it focus on actual harms to consumers, rather than those that are speculative or theoretical. This means identifying injuries that are concrete, measurable, and related to the conduct at issue, so that the FTC's enforcement actions and remedies for harm are proportionate to the measured injury to consumers, deter harmful practices, and allow for innovative activities.

II. FTC regulatory and enforcement policy should focus on concrete consumer injury.

In Acting Chairman Ohlhausen's speech announcing the coming workshop on informational injury, she lays out a taxonomy of consumer informational injuries that the FTC has previously encountered in its history of privacy and data security cases.³ Chairman Ohlhausen lists five different types of injury: 1) deception injuries or subversion of consumer choice; 2) financial injuries; 3) health or safety injuries; 4) unwarranted intrusion injuries; and 5) reputational injuries.⁴

This non-exhaustive taxonomy of injuries is useful, but qualitative descriptions of injuries ought not be the FTC's primary focus in a privacy and data security enforcement context. Instead, the FTC should pay attention to outcomes—identifying and deterring the types of injuries that lead to actual privacy harms to consumers, rather than harms that are speculative. This does not mean a single-minded focus on injuries that lead to exclusively financial harms to consumers, but those that lead to harms that are concrete or tangible—an approach that is

³ Acting FTC Chairman Maureen K. Ohlhausen, *Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases*, Sep. 19, 2017, available at https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf.

⁴ *Id.* at 4-9.

consistent with the Supreme Court’s framework for evaluating standing in consumer digital privacy cases as established in *Spokeo v. Robins*.⁵

In *Spokeo v. Robins*, Spokeo, a data broker, generated an online profile of Robins that contained inaccurate information. The Supreme Court found that Robins had failed to adequately allege an injury in fact under Article III standing analysis because he did not demonstrate that he was actually harmed by Spokeo’s dissemination of inaccurate information online.⁶ To satisfy Constitutional standing requirements, such dissemination must at minimum cause harm or present a material risk of harm to the complainant.⁷

In the context of digital privacy harms, *Spokeo* stands for the principle that the mere technical violations without concrete injury are not per se harmful to consumers.⁸ An individual must have suffered some causally related adverse outcome to allege a privacy harm. This framework should inform the FTC’s approach. The FTC should avoid devoting regulatory and enforcement resources to instances where no concrete or tangible harm to the consumer has occurred. Rather, the FTC should work to deter practices that lead to actual, provable harm.

III. Consumer harms should be measurable and supported by data-driven analysis.

To further solidify the link between consumer injury and enforceable actual harms, the FTC should ensure that it focuses on measurable consumer injuries. More data driven analysis is the key to balanced and effective consumer protection, and will protect against the risk that FTC might “erroneously condemn” business practices that provide consumers net benefits.⁹

⁵ *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

⁶ *Id.* at 1549–50.

⁷ *Id.* at 1550.

⁸ Bijan Madhani, *The Supreme Court Clarifies Digital Privacy Harms in Spokeo v. Robins*, PROJECT DISCO (June 6, 2016), <http://www.project-disco.org/privacy/060616-the-supreme-court-clarifies-digital-privacy-harms-in-spokeo-v-robins/>.

⁹ FTC Commissioner Joshua D. Wright, *The Economics of Digital Consumer Protection: One Commissioner’s View*, July 31, 2014, at 6, available at https://www.ftc.gov/system/files/documents/public_statements/573061/010731techfreedom.pdf.

This analysis should rely on the expertise of the Bureau of Economics, and be informed by the technical experts in the Office of Technology Research and Investigation and the competition experts throughout the Commission, who can together help assess the harms and benefits of practices—along with the harms and benefits of regulation—in a data-driven way. Data-driven reasoning is particularly important in the context of unfairness actions in the digital privacy and security context, where cost-benefit analysis is a key part of determining whether an allegedly unfair business practice has actually led to substantial injury to consumers, or in fact yields overall benefits.¹⁰

IV. Harms should be tethered to the facts of a case and the FTC’s stated authority for enforcement.

The FTC’s primary privacy and data security tool is enforcement under its Section 5 authority to protect consumers from deceptive or unfair acts or practices.¹¹ Both deception and unfairness actions require demonstration of an injury to consumers. The Commission is most effective in its efforts to prevent and remedy actual harm to consumers when it links the facts of a particular case and the respective legal requirements of its deception and unfairness analyses to tie concrete injuries to actual harms.

Cases where the FTC has strayed from tying the materiality of a deceptive act,¹² or the costs and benefits of an allegedly unfair practice,¹³ to actual harms often create perverse incentives and fail to inform consumers and businesses of best practices. The same dangers apply

¹⁰ See FTC Policy Statement on Unfairness (Dec. 17, 1980) (appended to *International Harvester Co.*, 104 F.T.C. 949, 1070 (1984)) [hereinafter “FTC Policy Statement on Unfairness”], <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>.

¹¹ 15 U.S.C. § 45.

¹² See FTC Policy Statement on Deception (Oct. 14, 1984) (appended to *Cliffdale Assocs.*, 103 F.T.C. 110 (1984)) [hereinafter “FTC Policy Statement on Deception”], <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception>.

¹³ See FTC Policy Statement on Unfairness, *supra* note 10.

when certain types of data are considered per se sensitive and their disclosure per se harmful to consumers, without an assessment of the surrounding context or a specific articulation of the concrete harms that actually occurred.

One recent case where the link between a deceptive act and consumer harm was not well established was the FTC's settlement with Nomi Technologies.¹⁴ Nomi is a start-up that helps retail clients understand consumer behavior in stores. The facts underlying the Commission's complaint and consent order in its case against Nomi did not meet the legal and policy requirements for bringing an enforcement action for a deceptive practice. Nomi's failure to offer consumers a physical in-store opt-out from tracking, as stated in its privacy policy, likely harmed no one, given the effectiveness of its online opt-out system. Materiality, under the FTC's deception analysis, requires the consumer's decision-making to have been affected by an allegedly deceptive act or practice.¹⁵ Here, it is highly unlikely that any consumer based their decision to opt-out of Nomi's tracking service based on the availability of an in-store opt-out. In fact, Nomi's opt-out system, though imperfect, likely conferred more benefits to consumers than harms.

The consent order with Nomi did not serve to protect consumers from current injury in that case or prevent future harm. It merely enforced the letter of Nomi's privacy policy, rather than the spirit. Cases akin to the FTC's action against Nomi will ultimately result in adverse outcomes for consumer protection by leading to reduced transparency and fewer privacy-protective choices for consumers.

These sorts of analyses of deceptive acts or unfair practices that fail to comply with the statutory limits imposed by Congress do a disservice to consumers and businesses alike. If

¹⁴ *In the matter of Nomi Technologies, Inc.*, FTC File No. 132-3251, Decision and Order (Aug. 28, 2015).

¹⁵ See FTC Policy Statement on Deception, *supra* note 12.

harmless errors are enforceable, businesses will simply avoid the possibility they might commit them, rather than that risk in attempting to offer consumers a privacy choice or innovative service whose overall benefits to consumers could well outweigh its potential for injury. The nuance afforded to the FTC by its Section 5 authorities are its strengths, and the primary means through which the consumer can effectively balance robust consumer protection with the regulatory flexibility necessary to foster innovation online. Rigid, context-free enforcement actions and *per se* definitions rob the Commission of its ability to appropriately strike that balance.

V. Conclusion

CCIA appreciates the opportunity to submit these comments and participate in the coming workshop on informational injuries. As the Commission prepares for the workshop and future regulatory actions, CCIA urges it to identify injuries that are concrete, measurable, and related to improper acts or practices, so that FTC enforcement actions are linked to actual harms to consumers. This framework will allow the Commission to prevent and remedy truly irresponsible and harmful practices, while also providing clear guidance to consumers and businesses operating in the digital ecosystem.

October 27, 2017

Respectfully submitted,

Bijan Madhani
Senior Policy Counsel
Computer & Communications Industry
Association
655 15th Street NW, Suite 410
Washington, D.C. 20006
(202) 783-0070