

December 21, 2018

VIA ELECTRONIC FILING

Mr. Donald S. Clark
Federal Trade Commission Office of the Secretary
Constitution Center 400 7th Street, SW
5th Floor, Suite 5610 (Annex A)
Washington, DC 20024

**Re: Hearings on Competition and Consumer Protection in the 21st Century
(P181201)**

Mr. Clark:

Please accept the attached comments on behalf of the U.S. Chamber Institute for Legal Reform.

Respectfully Submitted,

Harold Kim
Executive Vice President
U.S. Chamber Institute for Legal Reform

cc: Timothy J. Muris
Alan Charles Raul
Kate Heinzelman
Gabrielle Whitehall
Sidley Austin LLP

Howard Beales
George Washington School of Business

**Comments Submitted to the Federal Trade Commission in Connection with Hearings on
Competition and Consumer Protection in the 21st Century**

*Considerations for Framing, Assessing, and Balancing Actionable Injury and Intangible Harm
Relating to Privacy and Data Protection*

Timothy J. Muris
Alan Charles Raul
Kate Heinzelman
Gabrielle Whitehall
Sidley Austin LLP
1501 K Street N.W.
Washington, DC 20005

Harold Kim
U.S. Chamber Institute for Legal Reform
1615 H Street N.W.
Washington, DC 20062

Howard Beales
George Washington School of Business
2201 G Street N.W.
Washington, DC 20052

The U.S. Chamber Institute for Legal Reform (“ILR”) is pleased to submit this response to the Federal Trade Commission’s (“FTC” or “the Commission”) public notice seeking comments regarding its hearings concerning Competition and Consumer Protection in the 21st Century (P181201).

ILR is an affiliate of the U.S. Chamber of Commerce, which is the world’s largest business federation, representing the interests of more than three million companies across different sectors and regions, as well as state and local chambers and industry associations. ILR is dedicated to making our nation’s civil legal system simpler, faster, and fairer for all participants.

ILR applauds the FTC for engaging in a substantial examination of whether changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection law, enforcement priorities, and policy. We respectfully submit that the FTC’s paradigm for protecting consumers with respect to privacy, data protection, and information practices would benefit greatly from such an in-depth examination.

ILR encourages the FTC and interested parties to focus on the question of what commercial data-related acts or practices can qualify as actionable injuries for purposes of section 5 of the Federal Trade Commission Act (“FTC Act”). In the following comment, ILR draws upon the FTC’s 2017 Workshop on Informational Injury to propose a framework to inform the FTC’s enforcement efforts related to privacy and data-related intangible injuries.

INTRODUCTION

Uses of data and new technologies are transforming the U.S. economy. The vast majority of Americans are online;¹ approximately 8 out of 10 of them also shop online.² Roughly 75% of all U.S. adults report owning a smartphone,³ and the number of connected devices in our economy is only growing.⁴ Data generates a tremendous amount of economic value. A 2018 U.S. Bureau of Economic Analysis report, for instance, estimates that from 2006 to 2016, the “digital economy real value added grew at an average annual rate of 5.6 percent, outpacing the average annual rate of growth for the overall economy of 1.5 percent.”⁵ A 2013 McKinsey report estimates that improved use of data in education, transportation, consumer products, electric power, oil and gas, health care, and consumer finance alone could generate \$1.1 trillion in additional value each year

¹ Kevin Barefoot et al., *Defining and Measuring the Digital Economy*, U.S. Bureau of Economic Analysis at 3 (Mar. 15, 2018), <https://www.bea.gov/system/files/papers/WP2018-4.pdf>.

² Aaron Smith & Monica Anderson, *Online Shopping and E-Commerce*, Pew Research Ctr. at 2 (Dec. 19, 2016), http://assets.pewresearch.org/wp-content/uploads/sites/14/2016/12/16113209/PI_2016.12.19_Online-Shopping_FINAL.pdf.

³ Lee Rainie & Andrew Perrin, *10 Facts About Smartphones as the iPhone Turns 10*, Pew Research Ctr. (June. 28, 2017), <http://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones/>.

⁴ See Dep’t of Commerce, Internet Policy Task Force & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things*, 4 (Jan. 2017), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

⁵ Barefoot et al., *supra* at 2.

in the United States.⁶ In short, data is driving innovation, unleashing economic growth, improving decision-making, and leading to rapid advances across a range of applications and industries.⁷

As the data-driven economy takes off, the question of how to regulate businesses' collection and use of consumer-related data becomes ever more consequential. In what circumstances do business' practices regarding such data cause consumer injury under existing legal frameworks regarding "unfair" and "deceptive" trade acts and practices? As ILR has previously stated, if the U.S. digital economy is to achieve its potential, "organizations must be able to collect, share, and use information, subject to contractual limits and reasonable consumer protections to prevent fraud and deception, on the one hand, and without the threat of overburdensome and disproportionate liability" on the other.⁸

Earlier this year, the U.S. Department of Commerce's National Telecommunications and Information Administration released a request for comments on an approach to modernize U.S. data privacy policy. The request emphasized "risk-based approaches" to privacy issues that would "allow organizations the flexibility to balance business needs, consumer expectations, legal obligations, and potential privacy harms, among other inputs, when making decisions about how to adopt various privacy practices."⁹ The "[r]isk-based flexibility . . . at the heart of the approach the Administration"¹⁰ is exploring will require a careful assessment of the costs and benefits of privacy-related practices and requirements, as well as quantitative data to ensure those assessments are sound.¹¹

The FTC has long recognized that its authority under section 5 of the FTC Act to prohibit "unfair" and "deceptive" trade practices must be wielded responsibly, consistent with the Commission's statutory mandate and its broader purpose: the protection of consumer welfare and choice.¹²

⁶ James Manyika et al., *Open Data: Unlocking Innovation and Performance with Liquid Information*, McKinsey Global Institute, 6 (Oct. 2013), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Open%20data%20Unlocking%20innovation%20and%20performance%20with%20liquid%20information/MGI_Open_data_FullReport_Oct2013.ashx.

⁷ U.S. Chamber of Commerce Foundation, *The Future of Data-Driven Innovation* at 1 (Oct. 2014), <https://www.uschamberfoundation.org/sites/default/files/The%20Future%20of%20Data-Driven%20Innovation.pdf>.

⁸ U.S. Chamber Inst. for Legal Reform, Comment Letter on Informational Injury Workshop P175413 at 3-4 (Oct. 27, 2017), https://www.instituteforlegalreform.com/uploads/sites/1/20171027__Comments_of_ILR_to_FTC_re_Informational_Injury_-_AS_FILED.PDF.

⁹ Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600, 48,602 (Sept. 26, 2018).

¹⁰ *Id.* at 48,600.

¹¹ See Alan Raul & Christopher Fonzone, *Trump Admin. Approach to Data Privacy, and Next Steps*, Law360 (Sept. 27, 2018), <https://www.law360.com/articles/1086945/the-trump-admin-approach-to-data-privacy-and-next-steps>.

¹² See, e.g., FTC, Commission Statement of Policy on the Scope of the Consumer Unfairness Jurisdiction (Dec. 17, 1980) (appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1075 (1984)), <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>. (hereinafter "Unfairness Policy Statement") ("[T]he focus on injury is the best way to ensure that the Commission acts responsibly and uses its resources wisely."); *id.* at 1074 ("[C]ertain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary. Most of the Commission's unfairness matters are brought under these

ILR commends the FTC for convening public hearings on whether changes to our economy and business practices, new technologies, or international developments require new approaches to consumer protection.¹³ New approaches and solutions should, however, be predicated on an understanding of the problems they seek to solve. A foundational issue underlying the consumer protection topics discussed at the Commission’s hearings is determining in what circumstances business practices involving data concerning consumers are deceptive, fraudulent, and objectively harmful. In December 2017, the Commission held a workshop on this topic that brought together interested parties from across industries, civil society, and academia. In connection with the FTC’s ongoing hearings, and drawing upon the December 2017 workshop, ILR recommends that the Commission issue guidance on a framework for considering intangible harms relating to data uses and privacy for purposes of guiding determinations about which of these injuries are actionable under section 5 of the FTC Act. We recommend that this framework include a rigorous analysis of costs and benefits to consumers and businesses alike. Specifically, ILR recommends that the Commission:

(1) prescribe rigorous standards for its own assessment of when data-related practices are actionable, namely, whether they cause tangible injury, or alternatively, cause concrete intangible injury that is predicated on clear and well recognized harms;

(2) ensure clear and rigorous characterization and substantiation of any putative harm the Commission acts to prevent, abate, or sanction;

(3) require specific facts showing that harms are *likely* to result in substantial injury, where alleged harms have not yet materialized;

(4) consider whether a business has misled consumers about data-related practices that matter to consumers;

(5) analyze consumer behaviors concerning privacy and data security issues to help the Commission better understand what information about commercial data practices is material to today’s consumers; and

(6) study and seek to provide a clear analytic framework for how the Commission will assess the costs and benefits to consumers and competition of commercial data practices, and thus, the cost-benefit implications of regulation or enforcement with respect to such practices.

circumstances. They are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision-making.” (Footnotes omitted)); *id.* at 1061 n.47 (“[T]he principal focus of our unfairness policy is on the maintenance of consumer choice or consumer sovereignty”).

¹³ Press Release, FTC Announces Hearings on Competition and Consumer Protection in the 21st Century (F.T.C. June 20, 2018), <https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st>.

I. ACTIONABLE INJURIES, WHETHER TANGIBLE OR INTANGIBLE, MUST BE CONCRETE.

“Unjustified consumer injury is the primary focus of the FTC Act.”¹⁴ Whether the theory is unfairness or deception, concrete injury to consumers is a necessary element of a violation of section 5 of the FTC Act.¹⁵ Identifying injury should therefore be the first step in any FTC section 5 enforcement action. And an assessment of the magnitude and severity of consumer harm should guide the Commission in prioritizing the exercise of its enforcement authorities in this area.

Of course, injury comes in many forms. But to qualify as an “injury” under section 5 of the FTC Act, the harm must be concrete, or real. That is, as the Supreme Court has explained in another context, the injury cannot be “abstract” or “hypothetical.”¹⁶ To recognize injuries that fail to meet even this minimal standard—which is required for plaintiffs to get their day in court under Article III of the Constitution¹⁷—would be inconsistent with the plain text and clear purpose of the FTC Act.

An injury need not, however, be tangible to be concrete. We recommend that the Commission recognize both tangible and intangible injuries relating to individual privacy and alleged misuses of consumer information, and propose a standard, based in long-recognized tort principles, for distinguishing actionable intangible privacy-related injuries from those that are merely abstract or hypothetical. We outline below four discrete types of injury the Commission has recognized over time under its section 5 authorities and discuss briefly how each applies to data-related harms in particular.

A. Tangible Injuries

Tangible injury can present itself in at least three (at times overlapping) forms: physical, monetary, and disruption injuries. Such injuries have often formed the basis of section 5 enforcement actions in other contexts. They also apply to unfair or deceptive uses or treatment of information concerning consumers.¹⁸

- *Monetary Injuries.* Monetary injury is a clear form of concrete harm. Indeed, the FTC’s 1980 Unfairness Policy Statement notes that, “*in most cases* a substantial injury involves monetary harm.”¹⁹ Identity theft can, for instance, create significant economic harms to

¹⁴ Unfairness Policy Statement, 104 F.T.C. at 1073.

¹⁵ See 15 U.S.C. § 45(a), (n); Unfairness Policy Statement, 104 F.T.C. at 1073 (“Unjustified consumer injury is . . . the most important of the three [unfairness] criteria”); FTC Policy Statement on Deception (Oct. 23, 1984) (appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 183 (1984)), <https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception> (hereinafter “Deception Policy Statement”) (“[I]njury and materiality are different names for the same concept.”).

¹⁶ See *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2018) (describing the requirement for “concrete injury” to satisfy Article III standing).

¹⁷ See, e.g., *id.*

¹⁸ Determining whether injury is concrete is discrete from the closely related questions whether that injury is “substantial” and “likely” to occur. We discuss the latter two requirements in section II.A, *infra*.

¹⁹ Unfairness Policy Statement, 104 F.T.C. at 1073 (emphasis added).

consumers as well as financial institutions.²⁰ Errors in credit reports can lead to denials of credit, insurance, or employment, and to higher costs for those who obtain such services despite the error.²¹

- *Physical Injuries.* Although physical injuries are relatively infrequent in the FTC’s cases, the Commission has taken several enforcement actions against practices that pose risks to health and safety under section 5.²² Unlawful uses of information can lead to physical harm, for instance, if information is used to stalk and assault a person, or to subject consumers (or their property) to other criminal activity or damage.²³ Consider, for example, physical damage resulting from cyber exploitations that can cause networks or devices to be taken offline.
- *Disruption Injuries.* A third type of tangible injuries are disruption injuries. These injuries result from practices that needlessly raise transactions costs for consumers, or that result in wasted time and effort. For instance, when unwanted telemarketing calls at dinnertime disrupted consumers’ lives and impeded their willingness to answer their phones, the FTC implemented its National Do Not Call Registry.²⁴ The Commission has also challenged the practice of “mouse trapping,” in which a business redirected consumers to its websites and then trapped them by launching multiple browser windows, each with an advertisement, and further impeded their ability to browse by opening additional windows when the user closed each window.²⁵ While disruption injuries often exact relatively small financial costs on individual consumers, they can collectively impose significant costs and chill important consumer behaviors. Determining how to assess and quantify such injuries is an important part of better understanding the tangible harms that may result from unwanted data usage.

²⁰ Erika Harrel, *Victims of Identity Theft, 2014*, at 7 (Rev. Nov. 13, 2017), <https://www.bjs.gov/content/pub/pdf/vit14.pdf> (In 2014, 14% of identity theft victims experienced personal out-of-pocket financial losses. Forty-nine percent of these victims had total losses of \$99 or less. About 16% of these victims reported out-of-pocket expenses of \$100 to \$249).

²¹ Robert B. Avery, Paul S. Calem, & Glenn B. Canner, *Credit Report Accuracy and Access to Credit*, Federal Reserve Bulletin (2014), <https://www.federalreserve.gov/pubs/bulletin/2004/04index.htm>.

²² See, e.g., Unfairness Policy Statement, 104 F.T.C. 949 (1984) (finding an unfair trade practice where company failed to disclose risk of fuel geysering in tractors); *In re Philip Morris, Inc.*, 82 F.T.C. 16 (1973) (finding an unfair trade practice where company distributed free razor blades that could harm children); Stipulated Final Order for Permanent Injunction, *FTC v. Vital Living Products, Inc.*, No. 3:02CV74-MU (W.D. N.C. Feb. 27, 2002), FTC File No. 022-3060, <https://www.ftc.gov/sites/default/files/documents/cases/2002/02/vitalorder.pdf> (finding deceptive acts or practices where company made false and misleading representations regarding the accuracy and effectiveness of its anthrax test kits).

²³ See, e.g., Complaint, *In re Trendnet, Inc.*, No. 122-3090 (F.T.C. Feb. 7, 2014), <https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf> (complaint alleging security flaws in Internet security camera increase risk that consumers will be targeted for criminal activity).

²⁴ See Lesley Fair, *10 Years of National Do Not Call: Looking Back and Looking Ahead*, F.T.C. (June 27, 2013), <https://www.ftc.gov/news-events/blogs/business-blog/2013/06/10-years-national-do-not-call-looking-back-looking-ahead>. Illegal robocalls have unfortunately diminished the value of the Do Not Call Registry for many consumers.

²⁵ See *F.T.C. v. Zuccarini*, No. CIV.A. 01-CV-4854, 2002 WL 1378421 (E.D. Pa. Apr. 9, 2002).

B. Intangible Injuries

While *tangible* harms are clearly concrete, it is more difficult to determine when *intangible* harms satisfy this threshold. In what circumstances are these harms actionable “injuries”? The Commission and others have long grappled with this general question.²⁶ In its 1980 Unfairness Policy Statement, the FTC concluded that “[e]motional impact and other more subjective types of harm . . . will *not ordinarily* make a practice unfair.”²⁷ Members of Congress echoed this conclusion by codifying most of the FTC’s Unfairness Policy Statement in legislation.²⁸ Many intangible injuries are in the eye of the beholder, which is precisely the problem the Commission—and later Congress—was trying to solve by codifying an objective, three-part test for unfairness under 15 U.S.C. § 45(n) in 1994. The Commission has noted that, “[i]n an *extreme* case, . . . emotional effects might possibly be considered as the basis for a finding of unfairness.”²⁹ What, then, is the proper test for determining which intangible informational injuries are sufficiently concrete and objectively harmful to be potentially actionable under the FTC Act?

The statute provides some guidance. Section 5 states that the Commission “may consider established public policies as evidence to be considered” “[i]n determining whether an act or practice is unfair.”³⁰ But such “public policy considerations may not serve as a primary basis for such determination.”³¹ The existence of broadly adopted common law alone cannot therefore be *an independent* basis for a finding of concrete injury. Tort law, however, is a particularly appropriate source for the Commission to consider in determining whether an intangible harm rises to the level of potential actionable injury, in part, because it shares the same cost-benefit foundations as section 5 unfairness analysis.³² Such laws certainly may help define the instances in which consumers suffer intangible harms that are not merely subjective but instead take the form of well-established, widely recognized, concrete harms.

With respect to privacy harms in particular, longstanding, widely recognized tort law provides an appropriate, ascertainable, and well-established standard for determining when such

²⁶ Cf. *Spokeo*, 136 S. Ct. at 1549 (“Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.”); Opinion of the Commission, *In re: LabMD, Inc.*, FTC Docket No. 9357 (F.T.C. July 29, 2016), <https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf> (“the disclosure of sensitive health or medical information causes additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n)”).

²⁷ Unfairness Policy Statement, 104 F.T.C. at 1073 (emphasis added).

²⁸ S. Rep. No. 103-130, 1993 WL 322671, at *13 (F.T.C. Aug. 24, 1993) (“Emotional impact and more subjective types of harm alone are not intended to make an injury unfair.”). As explained in the next paragraph, statute, as enacted by Congress, allows for a more limited use of public policy than the 1980 statement itself. In a 1982 letter, the Commission modified its view, disavowing the ability to rely on public policy alone in its unfairness cases.

²⁹ Unfairness Policy Statement, 104 F.T.C. at 1073 n.16 (citing the Fair Debt Collection Practices Act’s prohibition on harassing calls) (emphasis added).

³⁰ 15 U.S.C. § 45(n).

³¹ *Id.*

³² See Richard Posner, *Economic Analysis of Law* 167-69 (3d ed. 1986) (arguing negligence is based on balancing costs and benefits of accident prevention).

harms can rise to the level of concrete injury notwithstanding their intangible nature.³³ Under the *Restatement (Second) of Torts*, privacy torts are generally limited to intrusions or disclosures that “would be highly offensive to a reasonable person.”³⁴ Courts across the country have used that standard—and the substantive privacy torts to which it is tied—to guide their determinations about when intangible privacy harms may rise to the level of concrete, objective injuries.³⁵ This is not to say that intangible informational injuries must necessarily be limited to the four privacy torts codified in the *Restatement*, but rather that the “highly offensive to a reasonable person” standard provides an appropriate barometer for determining whether an intangible privacy harm can rise to the level of being an unfair or deceptive trade act or practice under the FTC Act.³⁶

The elements of the privacy torts are also instructive.³⁷ The tort of intrusion upon seclusion, for instance, reaches conduct that invades another’s privacy in a manner that is unauthorized and offensive—conduct “analogous to tortious or criminal trespass.”³⁸ Limiting intangible informational injuries to those that satisfy defined thresholds rooted in existing law would help provide regulated entities guidance and prioritize enforcement resources. In the absence of further guidance, businesses are at risk of arbitrary enforcement and the nearly impossible task of seeking

³³ See, e.g., Opinion of the Commission, *In re: LabMD, Inc.*, Docket No. 9357, 19 (July 28, 2016), <https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf> (“Tort law also recognizes privacy harms that are neither economic nor physical.” (citing Restatement (Second) of Torts § 652B (1977), the “highly offensive” standard)); cf. *Spokeo*, 136 S. Ct. at 1549 (noting that “the law has long permitted recovery by certain tort victims even if their harms may be difficult to prove or measure”); *id.* (stating, in the context of Article III standing injury, that “it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts”).

³⁴ Restatement (Second) of Torts § 652B (1977) (intrusion upon seclusion); *id.* § 652D (publicity given to private life); *id.* § 652E (publicity placing person in false light). *But cf. id.* § 652A (appropriation of name or likeness).

³⁵ See *Mey v. Got Warranty, Inc.*, 193 F. Supp. 3d 641, 645 (N.D. W. Va. 2016) (“Invasion of privacy is . . . an intangible harm recognized by the common law. Almost all states recognize invasion of privacy as a common law tort.” (citation omitted)). Federal district courts have, for instance, referred to the privacy torts in assessing whether injury was sufficient to satisfy Article III standing requirements. See, e.g., *Oneal v. First Tenn. Bank*, No. 4:17-CV-3-TAV-SKL, 2018 WL 1352519, at *9 (E.D. Tenn. Mar. 15, 2018) (“the Court finds that the common law tort tradition does not support a finding of concreteness here”); *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 517 (S.D.N.Y. 2017) (holding that plaintiffs had failed to satisfy Article III standing in case alleging that video game company violated their privacy by collecting their facial scans without complying with state law procedural requirements because, among other things, plaintiffs “do not allege that their biometric identifiers have been used for anything other than for in-game play in NBA 2K15, a use for which the plaintiffs expressly consented,” including because, “at common law, not every unlawful or unauthorized collection of information . . . gave rise to an intrusion [upon] seclusion,” noting the “highly offensive” standard of the tort), *aff’d in part, vacated in part on other grounds*, 717 F. App’x 12 (2d Cir. 2017); *Mount v. PulsePoint, Inc.*, No. 13 CIV. 6592 (NRB), 2016 WL 5080131, at *4 (S.D.N.Y. Aug. 17, 2016) (plaintiffs demonstrated Article III standing because the harms they alleged from the circumvention of their browser’s cookie-blocking setting to place cookies on their devices “are sufficiently grounded in the harm protected against by the common law tort of intrusion upon seclusion”), *aff’d*, 684 F. App’x 32 (2d Cir. 2017).

³⁶ Cf. Washington Legal Foundation, Comments on the Informational Injury Workshop P175413 at 6-7 (Oct. 27, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00026-141554.pdf (discussing aspects of the privacy torts).

³⁷ See Appendix for a chart of the privacy torts.

³⁸ See *Vigil*, 235 F. Supp. 3d at 517.

to anticipate what some consumers, and the FTC, may consider “unfair,” as measured against an unarticulated standard.³⁹ Limiting intangible informational injuries to such injuries would not, moreover, impair the Commission’s ability to pursue the types of cases it has pursued in the past that are congruent with tort theories.⁴⁰ The Commission’s role, as it is in many other areas, should be to bring actions using the same general standard (adapted to the FTC’s particular authorities) to protect consumers where the costs of litigation make private protection of these important rights impractical. Of course, in addition to finding that an intangible harm is concrete, the FTC would also need to find that the other components of a section 5 injury—discussed below—are satisfied. The existence of a concrete harm is simply the first step in the analysis.

Regardless of the standard the Commission adopts, it is critical that businesses and consumers understand the scope of the Commission’s jurisdiction. Certainly not every injury caused by uses of information concerning consumers falls within the FTC’s purview. The Fair Housing Act seeks to protect consumers, for instance, and uses of information can create Fair Housing Act liability. But Congress has chosen a specific, contextual regulatory scheme, along with specified executive branch mechanisms, for enforcing against such harms. Quite simply, these laws involve considerations and tradeoffs that are outside the Commission’s expertise. Indeed, in many instances, the most effective and appropriate way to protect against intangible harms is through specific legislation and regulation because the tradeoffs between privacy-related risks and benefits to the public at large require careful, contextual balancing and consideration of individual as well as societal risks and benefits. Consider, for instance, the tradeoffs in determining how to protect personal health information in the ordinary course from health information that is relevant to public health matters. Statutory and regulatory schemes—rather than case-by-case enforcement—can impose calibrated, context-specific frameworks involving requirements that are both procedural (*e.g.*, mechanisms for lodging complaints, opportunities to cure) and substantive (*e.g.*, requirements for risk assessments and internal audits). These schemes can help focus compliance efforts while giving government and consumers a toolbox of authorities for ensuring the proper balance is struck, and that enforcement authorities with appropriate expertise are involved.

While a complete discussion of the scope of the FTC’s section 5 jurisdiction is beyond the scope of this paper, the intangible injuries identified by the torts mentioned above, and intangible harms that are predicated on clear and well-recognized standards that are fairly within the Commission’s expertise and FTC Act jurisdiction, should be the Commission’s focus when considering intangible data-related injuries.

³⁹ *Cf. FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 249 (3d Cir. 2015) (discussing fair notice issues).

⁴⁰ For instance, the Commission’s complaint in *In re Aaron’s Inc.*, resembles an allegation of an intrusion upon seclusion tort. *See* Complaint, *In re Aaron’s, Inc.*, Docket No. C-4442, ¶ 4 (F.T.C. Mar. 10, 2014), <https://www.ftc.gov/system/files/documents/cases/140311aaronscmp.pdf>, (software product installed on rented computers enabled franchisees “to disable a computer remotely” and “to remotely install and activate” Detective Mode capability that “could—and did—surreptitiously monitor the activities of computer users, including by logging keystrokes, capturing screenshots, and using the computer’s webcam”). In *Eli Lilly & Co.*, the Commission alleged that the company disclosed Prozac.com website email subscribers’ email addresses by sending out a mass email with a disclosed list of recipients. *See* Complaint, Docket No. C-4047 (F.T.C. May 8, 2002), <https://www.ftc.gov/sites/default/files/documents/cases/2002/05/elilillicmp.htm>. The alleged harm here resembles a claim of publicity given to private life.

II. SECTION FIVE AUTHORITIES ARE INTENDED TO PROTECT CONSUMER WELFARE AND CHOICE.

Identifying a concrete injury is an essential part of a section 5 action. But it is only the first step in the analysis. In addition to demonstrating injury, the unfairness and deception prongs of section 5 require that the injuries be substantial and at least likely to occur, or material, respectively. These statutorily required elements seek to limit section 5's authorities to their core purpose: to promote consumer choice in competitive markets. Both unfairness and deception authorities aim to protect consumer welfare and choice, rather than serve as a vehicle for imposing the Commission's preferences on consumers who have elected a different path.⁴¹

We discuss each authority in turn.

A. Unfairness Injuries

Substantial injury. To be actionable under section 5, a concrete injury must also be "substantial," a requirement that clearly excludes *de minimis* or trivial harms and limits the Commission's authority to practices that cause significant harm.⁴² Because the issue is whether the *act* or *practice* is unfair, the FTC measures substantiality in the aggregate: the injury may be substantial because of a relatively small harm to a large number of consumers or because of a very large harm to a smaller number of consumers.⁴³ But *how* the FTC measures harm is critical. Economists and researchers have long used willingness to pay as the measure of the value of a good to consumers.⁴⁴ Here, willingness to pay *to avoid* injury is the appropriate measure of the quantification of consumer injury from information uses. Aggregate injury, in other words, is best measured by consumers' willingness to pay to avoid the injury, as well as the number of consumers adversely affected by the practice. In measuring consumers' willingness to pay, the Commission should emphasize *actual* market behavior, rather than surveys about preferences.⁴⁵ Of course,

⁴¹ See Unfairness Policy Statement, 104 F.T.C. at 1061, n.47 ("T]he principal focus of our unfairness policy is on the maintenance of consumer choice or consumer sovereignty, an economic concept that permits relatively specific identification of conduct harmful to that objective."); *id.* at 1055-56 ("[D]eception jurisdiction acts to safeguard the exercise of consumer sovereignty.").

⁴² *E.g.*, Merriam-Webster's Collegiate Dictionary 1245 (11th ed. 2011) ("substantial" means "considerable in quantity, significantly great"); *see also* Definition of Substantial, Cambridge Dictionary, <https://dictionary.cambridge.org/us/dictionary/english/substantial> (last visited Aug. 12, 2018) ("large in size, value, or importance"); FTC Unfairness Statement, 104 F.T.C. at 1073.

⁴³ Unfairness Policy Statement, 104 F.T.C. at 1064 n.55.

⁴⁴ *See, e.g.*, Klaus Wertenbroch & Bernd Skiera, *Measuring Consumers' Willingness to Pay at the Point of Purchase*, J. of Mktg. Research at 228 (May 2002).

⁴⁵ A Thomson Reuters poll found that the majority (58%) of consumers prefer organic food to conventional food, but organic food accounts for only about 5% of U.S. food sales. The same phenomenon has been repeatedly observed with respect to privacy preferences specifically: consumers say one thing, but they do something else entirely. *See* Huffington Post, *Consumers Prefer Organic Food, Survey Says* (July 22, 2011), https://www.huffingtonpost.com/2011/07/22/consumers-prefer-organic-food_n_906988.html; *see also* U.S. Organic Industry Survey 2018, Organic Trade Association, <https://www.ota.com/news/press-releases/19681> (organic food accounts for 5.5% of food sold in U.S. retail channels) (last visited Sept. 24, 2018).

consumer choice is meaningful to the extent that consumers have access to relevant and timely information. The FTC can perform an educational role to advance consumer awareness.⁴⁶ As a general matter, where it is clear that the injury outweighs any possible countervailing benefits, there is little need for detailed quantitative analysis. Yet, when the balance between injury and offsetting benefits to consumers is close, careful quantitative analysis is essential.⁴⁷

Likely to cause harm. Putative unfairness harms that have not yet materialized must also be “likely” to cause substantial injury. That is, they must have a high probability of materializing, such as where harm is demonstrably more likely than not to occur,⁴⁸ or where there are specific facts showing substantial risk of harm. At a minimum, the statute requires more than a possibility that harm will materialize.⁴⁹ Indeed, it has become a maxim in the cybersecurity community that there are only two kinds of companies: those that have been hacked and those that are going to be hacked;⁵⁰ or, in a more recent rendition: those that have been hacked, and those who don’t know they’ve been hacked.⁵¹ Effective regulatory frameworks recognize that information security controls should account for the risks reasonably associated with the data and appropriate to the particular business environment. Because all activities have risks, the possibility that something bad *could* happen is not enough. In the digital age, cybersecurity risks will always exist; the question is whether *substantial* injury is *likely* to occur based on the particular facts at hand, and whether the act or practice at issue can be said to have caused that injury.

⁴⁶ See, e.g., F.T.C., Bureau of Consumer Protection, <https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection> (last visited Oct. 1, 2018) (referring to the FTC’s role in educating consumers); FTC, Division of Consumer & Business Education, <https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/ourdivisions/division-consumer-business> (last visited Oct. 1, 2018) (“[t]he Division of Consumer and Business Education’s mission is to give people the tools they need to make informed decisions”).

⁴⁷ See, e.g., International Center for Law and Economics, Comments on the Informational Injury Workshop P175413 at 2-3 (Oct. 27, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00031-141566.pdf. (“Where the same conduct that may produce informational injury also produces consumer benefit, determining whether the net effect is, in fact, harmful or not is essential.”).

⁴⁸ E.g., *Alaska Oil & Gas Ass’n v. Pritzker*, 840 F.3d 671, 684 (9th Cir. 2016) (referring to the “common meaning” of “likely” as being “more likely than not”); *United States v. Powell*, 761 F.2d 1227, 1233 (8th Cir. 1985) (“We believe the word should be read in its ordinary sense, as referring to something that is more likely to happen than not.”).

⁴⁹ See, e.g., The App Association, Comments on the Informational Injury Workshop P175413 at 6 (Oct. 27, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00024-141552.pdf. The showing required to demonstrate “substantial injury” is surely higher than the baseline requirement that plaintiffs demonstrate they can establish an injury sufficient to have their day in court, as is required by Article III of the U.S. Constitution. Yet even in the Article III standing context, courts have found that plaintiffs have failed to demonstrate any cognizable injury where they allege that “mere theft” of data alone gives rise to injury. See *Beck v. McDonald*, 848 F.3d 262, 274-75 (4th Cir. 2017), *cert. denied*, 137 S. Ct. 2307 (2017). In the section 5 context, the statute imposes a higher bar.

⁵⁰ See Robert S. Mueller, III, Director, FBI, Remarks at the RSA Cyber Security Conference (Mar. 1, 2012) <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies> (“I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”).

⁵¹ Zeus Kerravala, *John Chambers’ 10 Most Memorable Quotes as Cisco CEO*, Networkworld.com (July 24, 2015), <https://www.networkworld.com/article/2952184/cisco-subnet/john-chambers-10-most-memorable-quotes-as-cisco-ceo.html> (attributing the statement to John Chambers).

Courts' treatment of injury in the Article III context is instructive. To have their day in court, plaintiffs must demonstrate they can establish a concrete and particularized injury, as is required by Article III of the U.S. Constitution. The showing required to satisfy Article III's requirement of an "injury" is surely lower than what is required to demonstrate "substantial injury" under the FTC Act. Yet, even in the Article III context, courts have found that plaintiffs fail to demonstrate cognizable injury for purposes of standing where they allege that the fact that their data has been stolen itself gives rise to injury without further demonstration of harm.⁵²

In analyzing injury for purposes of Article III standing, courts have also examined whether *future* harms are sufficiently concrete to qualify as cognizable injuries. As the Supreme Court has explained, future injuries must be "imminent," not "conjectural" or "hypothetical" to satisfy Article III's injury requirement.⁵³ That is, they must be impending. This concept is "stretched beyond the breaking point when . . . the plaintiff alleges only an injury at some indefinite future time, and the acts necessary to make the injury happen are at least partly within the plaintiff's own control."⁵⁴ Similarly, a speculative future injury would not qualify under the FTC Act.⁵⁵

The district court in *FTC v. D-Link Systems Inc.*, for example, rejected as insufficient under section 5 the Commission's assertion that "remote attackers could take simple steps, using widely available tools, to locate and exploit [the routers and Internet-protocol camera] devices, which were widely known to be vulnerable."⁵⁶ Hypothetical risk alone was not, in other words, enough to satisfy section 5. The court dismissed the Commission's unfairness allegations in that case because "they ma[de] out a mere possibility of injury at best," noting "the lack of facts indicating a likelihood of harm."⁵⁷ The court further noted that:

The FTC does not identify a single incident where a consumer's financial, medical or other sensitive personal information has been accessed, exposed or misused in any way, or whose IP camera has been compromised by unauthorized parties, or who has suffered any harm or even simple annoyance and inconvenience from the alleged security flaws in the DLS devices. The absence of any concrete facts makes it just as possible that DLS's devices are not likely to substantially harm consumers,

⁵² See, e.g., *Beck*, 848 F.3d at 274-75; *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 695 (7th Cir. 2015) (holding that assertion that company lost plaintiffs' private information, without further specific harm, is "an abstract injury" insufficient to support standing, while finding standing on other grounds).

⁵³ *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992); *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 & n.5 (2013) (plaintiffs lacked standing because they did not plead "certainly impending" injury but only a "speculative chain of possibilities").

⁵⁴ *Lujan*, 504 U.S. at 565 n. 2.

⁵⁵ See Unfairness Policy Statement, 104 F.T.C. at 1073 ("The Commission is not concerned with . . . merely speculative harms."); cf. *id.* (discussing injuries consumers can reasonably avoid).

⁵⁶ *F.T.C. v. D-Link Corp.*, No. 3:17-CV-00039-JD, 2017 WL 4150873, at *5 (N.D. Cal. Sept. 19, 2017) (internal quotation marks omitted).

⁵⁷ *Id.*

and the FTC cannot rely on wholly conclusory allegations about potential injury to tilt the balance in its favor.⁵⁸

Thus, according to the court, the FTC could not demonstrate likelihood of harm in the absence of “concrete facts” showing that substantial harm was, at a minimum, more likely than not. Similarly, the Commission’s complaint in *HTC America*, alleges a “risk of financial and physical injury and other harm” because “malware placed on consumers’ devices without their permission could be used to record and transmit information” that “could be used, for example, to target spear-phishing campaigns, physically track or stalk individuals, and perpetrate fraud.”⁵⁹ Rather than presenting specific facts demonstrating the likelihood of specific injury, the complaint simply alleged that “malware developers have targeted *the types* of sensitive information and sensitive device functionalities” that could have been exposed on these mobile devices, as a general matter.⁶⁰

Like the FTC Act, Article III does, in some cases of substantial harm, recognize injuries that take the form of risks rather than harm that has materialized. But, as the Supreme Court has recently stated, in those cases “*substantial risks*” must be proven by “concrete facts showing that the defendant’s *actual action* has caused the substantial risk of harm” and cannot rest “on speculation about the unfettered choices made by independent actors.”⁶¹ At least that degree of certainty, proximity, and specific factual showing should be required under section 5 as well.

Offsetting benefits. Section 5 further requires that the harms of allegedly “unfair” practices not be “outweighed by countervailing benefits to consumers or to competition.”⁶² As discussed further below, conducting a rigorous cost-benefit analysis in cases of informational injury is critical to ensuring that enforcement actions do not stifle innovation by substituting the Commission’s preferences for those of consumers.⁶³ Different services will offer different data privacy features at different costs. The diversity of offerings in this regard is essential to competition, and consumers’ choices about these features should be respected.

The cost-benefit analysis should also take into account the tremendous value of uses of information that are secondary to the original purpose for which the information was collected. For instance, many fraud control tools use information originally collected for a different purpose, such as credit reporting or marketing, to look for unauthorized uses of personal information. Utilizing information to target advertising increases its value to advertisers, which in turn increases revenues available to support information content and other services for consumers. Measuring the benefits to consumers and competition at large from these secondary uses (where benefits to consumers and competition are often indirect) is essential. (The cost-benefit analysis set forth in section 5 is economy-wide, rather than consumer-by-consumer.) Careful empirical analysis and

⁵⁸ *Id.* (Citation omitted)

⁵⁹ Complaint, *In re HTC Am., Inc.*, Docket No. C-4406, ¶ 16 (F.T.C. June 25, 2013), <https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf>.

⁶⁰ *Id.*

⁶¹ *Clapper*, 568 U.S. at 414 n.5 (emphasis added) (internal quotation marks omitted).

⁶² 15 U.S.C. § 45(n).

⁶³ *Cf.* 83 Fed. Reg. 48,600, 48,601 (“[t]he desired outcome is a reasonably informed user, empowered to meaningfully express privacy preferences”).

proper consideration of market-wide effects, is therefore particularly important, as the benefits of data use can be spread throughout the economy.

Uses of information can enhance competition in the marketplace, and regulation and enforcement efforts should carefully consider competitive impacts. The Commission should also bear in mind, for instance, that regulatory requirements may affect competitors differently. For instance, requirements relating to consumer notice will affect consumer-facing organizations very differently than organizations that have no direct consumer interface. In imposing new requirements, the FTC should ensure that it does not unintentionally provide certain businesses a leg up on the competition in ways that are detrimental to competition at large. Providing a level playing field and not artificially entrenching existing advantage are of course important factors for the FTC to consider.

As others have noted, the FTC's authority over both competition and consumer protection gives it valuable perspective in assessing costs and benefits.⁶⁴ The Commission should, however, coordinate closely with sector-specific regulators operating under specific statutory regimes, such as the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act, as appropriate.

Reasonable avoidance. Finally, section 5 requires that unfair injuries not be “reasonably avoidable by consumers themselves.”⁶⁵ As stated at the outset, the Commission's unfairness authority is intended to protect consumer choice. This final element of the section 5 test is therefore critical. As the Unfairness Policy Statement explains, “[m]ost of the Commission's unfairness matters are brought . . . not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision-making.”⁶⁶

To that end, and as explained further below, particularly when businesses provide consumers meaningful information and choices about uses of their information, data practices will not ordinarily be unfair.

B. Deception Injuries

This final element of the section 5 test is therefore closely linked, particularly in the informational injury context, with the FTC's deception authorities. Section 5's deception authority focuses on ensuring that consumers are not misled in choosing a product or service. This authority is especially pertinent to informational injuries because businesses often make representations to consumers about their privacy-related policies and practices. Privacy policies, privacy charters, and other consumer-facing privacy statements are becoming ever more common. The FTC's

⁶⁴ See F.T.C., Comment letter on the NTIA's Approach to Consumer Privacy at 13 (Nov. 9, 2018), <https://www.ftc.gov/policy/advocacy/advocacy-filings/2018/11/ftc-staff-comment-ntia-developing-administrations-approach>.

⁶⁵ 83 Fed. Reg. 48,600, 48,601.

⁶⁶ Unfairness Policy Statement, 104 F.T.C. at 1074.

section 5 deception authority provides an established framework for assessing whether consumers are harmed by these (or other) representations, on the one hand, or by material omissions about businesses' practices, on the other hand. Under established FTC policy, a practice is deceptive if there is a representation, omission, or practice that is likely to mislead consumers, acting reasonably in the circumstances, about a material fact.⁶⁷

Deceptive statements. As the Supreme Court noted in an early FTC consumer protection case, “[t]he consumer is prejudiced if upon giving an order for one thing, he is supplied with something else. In such matters, the public is entitled to get what it chooses, though the choice may be dictated by caprice or by fashion or perhaps by ignorance.”⁶⁸ If a business promises consumers a particular privacy or cybersecurity-relevant attribute, consumers should get it. If consumers are promised an information service that does not track location, for example, the Commission should ensure that promise is not deceptive. Consumers concerned about location tracking can choose such services, while those with less concern can choose a service that tracks and makes use of location information.

Not all statements about privacy or cybersecurity are, however, actionable under this framework. Under section 5, a deceptive statement must be not only material, but used to consumers' “detriment.”⁶⁹ As the Commission has stated, “[i]njury exists if consumers would have chosen differently *but for* the deception.”⁷⁰ Materiality therefore requires that different (and accurate) information would have likely influenced consumer choices, thereby limiting the Commission's attention to information that is likely to matter in the market and that injures consumers in an economic sense, because they lose the perceived benefits of the choice they would have made instead. The FTC has taken the position that some statements, like express claims, can be presumed to be material.⁷¹ But, in explaining this position, the Commission referred to claims made in advertising materials, where “the willingness of a business to promote its products reflects a belief that consumers are interested” in the claims.⁷² Not all express statements are, however, material. Express claims made in marketing materials, which are intended to induce the purchase of a product are distinguishable, for instance, from relatively less significant provisions buried in a lengthy customer contract. Not all provisions in a contract are material.⁷³ By the same token, not all representations in a privacy policy should be presumed material. Instead, the Commission

⁶⁷ See Deception Policy Statement, 103 F.T.C. at 165.

⁶⁸ *FTC v. Algoma Lumber Co.*, 291 U.S. 67, 78 (1934) (internal citations omitted).

⁶⁹ Deception Policy Statement, 103 F.T.C. at 196.

⁷⁰ *Id.* at 183 (emphasis added).

⁷¹ *Id.* at 182.

⁷² *Id.* (internal quotation marks omitted).

⁷³ See, e.g., *Sims Buick-GMC Truck, Inc. v. Gen. Motors LLC*, 876 F.3d 182, 187 (6th Cir. 2017) (“A requirement is not material simply because a manufacturer opts to put it in a contract.”); *Universal Health Servs., Inc. v. United States*, 136 S. Ct. 1989, 2001-02 (2016) (“contractual requirements are not automatically material” under False Claims Act standard, a “demanding” materiality standard that “descends from common-law antecedents”) (internal quotation marks omitted).

should carefully consider whether and how privacy and data-related promises are likely to affect consumer choices.⁷⁴ A contextual analysis is required.⁷⁵

Deceptive omissions. What then about instances in which no promise is made? An omission of material information is deceptive only if the information is necessary to correct a *misimpression* that the message would otherwise convey. The Commission has explained that the omitted information must, moreover, be material in light of the representations made.⁷⁶ If consumers are not likely to rely on certain information in deciding to use a product or service, the information is not material.

Unfair omissions. Finally, omissions can be actionable if they satisfy the criteria for unfairness, including the cost-benefit analysis described above. Evidence that the undisclosed fact is important to a substantial number of consumers is particularly important in satisfying the unfairness criteria. If the additional information is unlikely to affect consumer choices, the omission of the information causes no concrete harm. This analysis recognizes that, while the direct costs of adding another line to a privacy policy are not significant, the indirect costs of providing additional information (or adding a further constraint on the scope of permitted data practices) can in some cases be more substantial. Providing too much information can lead to information overload and inferior choices.⁷⁷ Among other things, excessive information may lead consumers to ignore detailed disclosures entirely.⁷⁸ In many cases, consumers may not value more information on a product's or service's features or internal operations; there are many product features about which consumers have little idea or significant interest.⁷⁹ Unfairness analysis that considers offsetting benefits and reasonable avoidance is a good way to strike the right balance.

III. FTC GUIDANCE CAN HELP PRIORITIZE ENFORCEMENT AND IMPROVE INDUSTRY COMPLIANCE.

To reap the full benefits of the data economy—both for society and our economy as a whole—the Commission should regulate and enforce in this area with care and consistent with

⁷⁴ As Cooper and Wright have noted, privacy policies are often developed to comply with legal and self-regulatory requirements. See James C. Cooper & Joshua Wright, *The Missing Role of Economics in FTC Privacy Policy*, *The Cambridge Handbook of Consumer Privacy* at 465–488 (Evan Selinger, Jules Polonetsky, & Omer Tene eds., 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2894438.

⁷⁵ In other contexts, courts have recognized that materiality determinations are contextual. See, e.g., *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 43 (2011) (assessing materiality in the securities law context is a “fact-specific” inquiry).

⁷⁶ See Deception Policy Statement, 103 F.T.C at 165.

⁷⁷ See, e.g., Byung-Kwan Lee & Wei-Nal Lee, *The Effect of Information Overload on Consumer Choice Quality in an On-Line Environment*, 21 *Psychology & Mktg.* at 159 (2004); Jacob Jacoby, *Perspectives on Information Overload*, 10 *Journal of Consumer Research* at 432 (1984).

⁷⁸ It is well recognized that consumers frequently seek to simplify decisions, rather than explore the possibilities in more depth. See Omri Ben-Shahar & Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton Univ. Press 2014).

⁷⁹ See J. Howard Beales III & Timothy J. Muris, *FTC Consumer Protection at 100: 1970s Redux or Protecting Markets to Protect Consumers?*, 83 *George Washington L. Rev.* 2157, 2224–26 (2015).

legal principles that respect consumer choice in well-functioning markets. Protecting consumers from deceptive, fraudulent, and highly offensive uses of data is important, but it need not, and should not, stifle innovation. The Commission’s December 2017 informational injury workshop was an important step toward bringing greater rigor and clarity to the manner in which the Commission will evaluate informational injuries in carrying out its important mission. Drawing on that event, and in conjunction with the FTC’s hearings on Competition and Consumer Protection, ILR recommends that the Commission examine and issue guidance on its approach to informational injuries, especially with regard to the following seven topics:

- 1) **Identify actionable injury.** We urge the Commission to clarify how it will evaluate whether asserted injuries purportedly caused by businesses’ collection, processing, use, and disclosure of information qualify as concrete injuries that could be actionable under section 5 of the FTC Act. In particular, businesses and regulators need a rigorous process and ascertainable standards, as outlined above, for determining whether *intangible* injuries are sufficiently concrete to be actionable.⁸⁰ In the absence of such standards, FTC staff investigations could lack focus, imposing substantial costs on businesses that are subject to investigation for “injuries” that the Commission or federal courts ultimately determine are neither concrete nor substantial. Innovation may be deterred as companies seek to avoid practices that only a few may find objectionable. And compliance resources will be misdirected as companies seek to avoid any possible “injury” no matter how idiosyncratic and subjective. Determining whether an asserted injury is sufficiently concrete to be actionable should be a threshold question in any FTC investigation.⁸¹
- 2) **Ensure clear and rigorous characterization of the putative harm.** The Commission should require that any proposed enforcement concerning informational injury begin with a clear and rigorous characterization of the putative harm to consumers that the Commission’s proposed action would be intended to prevent, abate, or sanction. The FTC should not take final action without confirming that the harm in question has been duly characterized and substantiated and is indeed legally actionable.
- 3) **Explain standards for evaluating the likelihood of causing substantial injury.** Given the importance of establishing likelihood of harm with respect to informational injuries in particular, the Commission should clarify how it will evaluate whether acts or practices related to the collection, use, processing or disclosure of data concerning consumers are *likely* to cause substantial injuries in cases where those harms have not yet materialized. The Commission should make clear that likely injuries are those that are sufficiently likely to be impending or imminent, and that the mere existence—or assumption—of certain

⁸⁰ See Advertising Trade Association, Comments on the Informational Injury Workshop P175413 at 2 (Oct. 27, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00022-141550.pdf (“Without a concrete harm standard, allegations of injury based on subjective or potentially unverifiable harms would follow. The result would be significant uncertainty for consumers and businesses . . .”).

⁸¹ See Maureen K. Ohlhausen, *Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases* at 4 (Sept. 19, 2017), https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf (“[R]egardless 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.”).

security or privacy risks is not sufficient absent additional facts showing likelihood of concrete harm as a result.

- 4) **Focus on deception injuries.** Through its deception authorities, the Commission can examine asserted informational injuries to determine if a consumer has freely chosen a product or service with particular privacy or data-related features. This examination can help inform in some cases not only whether deception exists but also unfairness. We recommend that the Commission evaluate privacy and data-related harms under the deception prong of section 5 to determine whether a business’s communications about privacy- and security-related risks or features are materially deceptive. Where the business has provided meaningful and accurate information to consumers about its data-related practices in a manner in which consumers would rely on that information, consumers may be presumed to have chosen the product features they selected.
- 5) **Examine materiality.** Understanding what information about privacy and data security is in fact material to consumers today is essential to enforcing the Commission’s deception authority and understanding consumer choices related to data practices. We recommend that the Commission analyze consumer behaviors and understandings about these issues to better understand what information about data practices is important to consumers. Study of this topic would also help the private sector more directly address consumers’ values and concerns.
- 6) **Study costs and benefits to consumers and competition.** Finally, the Commission should study and seek to provide greater clarity about its analytic framework for assessing the costs and benefits to consumers and competition of businesses’ uses of information. Several commenters for the December 2017 workshop noted the need for rigorous economic analysis of the harms and benefits of data practices to support the Commission’s enforcement actions in this area.⁸² Data-driven enforcement will, as one commenter noted, “protect against the risk that FTC might ‘erroneously condemn’ business practices that provide consumers net benefits.”⁸³ Consumers are increasingly sophisticated about the trade-offs in the marketplace;⁸⁴ enforcement efforts should not deprive consumers of the ability to make choices regarding the services (and data protections) they elect. In developing these frameworks, the FTC could work with the Office of Management and

⁸² See CTIA, Comment Letter on Informational Injury Workshop P175413 at 4 (Jan. 26, 2018), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00040-142817.pdf; Internet Association, Comment on Informational Injury Workshop P175413 at 4 (Oct. 27, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00028-141556.pdf; Software & Information Industry Association, Comment Letter on Informational Injury Workshop P175413 at 5-6 (Oct. 27, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00018-141546.pdf.

⁸³ Computer & Communications Industry Association, Comment Letter on Information Injury Workshop P175413 at 3 (Oct. 27, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00025-141553.pdf. (quoting FTC Commissioner Joshua D. Wright, *The Economics of Digital Consumer Protection: One Commissioner’s View* at 6 (July. 31, 2014), https://www.ftc.gov/system/files/documents/public_statements/573061/010731_techfreedom.pdf).

⁸⁴ See, e.g., Internet Association, Comment Letter on Informational Injury Workshop P1754413 at 7-8 (Oct. 27, 2017).

Budget (OMB), which has a history of working with federal departments and agencies to conduct cost benefit analysis for purposes of regulatory review.⁸⁵ Indeed, the Commission has recognized the importance of agency review of the cost-effectiveness of regulation.⁸⁶ Ensuring that rigorous economic analysis supports the Commission’s enforcement efforts will help ensure that the injuries the FTC seeks to protect against are “measurable” in concrete terms.⁸⁷ Rigorous evaluation of consumer preferences, with a focus on actual market behaviors, is needed to support such analysis.

ILR respectfully offers these thoughts and recommendations for consideration. The FTC’s ongoing hearings provide an important opportunity to examine and adjust the Commission’s approach to data privacy and security consumer protection issues and to design rigorous cost-benefit analysis to support these efforts. ILR welcomes the opportunity to engage with the Commission and other interested parties on these important topics.

⁸⁵ See Executive Order No. 13579 of July 11, 2011, 76 Fed. Reg. 41,587 (July 14, 2011) (regulatory decisions “should be made only after consideration of their costs and benefits (both quantitative and qualitative)” of those decisions). As Executive Order 13579 states:

Executive Order 13563 of January 18, 2011, “Improving Regulation and Regulatory Review,” directed to executive agencies, was meant to produce a regulatory system that protects “public health, welfare, safety, and our environment while *promoting economic growth, innovation, competitiveness, and job creation.*” *Independent regulatory agencies, no less than executive agencies, should promote that goal.*

Id. § 1(b)(emphasis added).

Note that Executive Order 13563 refers back to the principles of Executive Order 12866, which required regulation to be reviewed and justified, among other things: (a) based on a reasoned determination that its benefits justify its costs (recognizing that some benefits and costs are difficult to quantify); (b) by a determination that the regulation imposes the least burden on society consistent with the regulatory objectives; (c) by relying on “performance objectives” (*i.e.*, outcomes), where feasible, rather than specifying the behavior or manner of compliance; and (d) after considering alternatives to direct regulation, including providing information upon which the public can make choices. Moreover, these prior regulatory review Executive Orders make clear that cost-benefit analysis is necessary and appropriate even with respect to the regulation of intangible harms that may be difficult or impossible to quantify (as might the case for some alleged privacy or data practice risks).

⁸⁶ See Press Release, *Statement by FTC Chairman Jon Leibowitz Regarding President Obama’s Regulatory Reform Initiative* (July 11, 2011), <https://www.ftc.gov/news-events/press-releases/2011/07/statement-ftc-chairman-jon-leibowitz-regarding-president-obamas>.

⁸⁷ See Acting Chairman Maureen K. Ohlhausen, *Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases* at 4 (Sept. 19, 2017), https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf (“Courts and FTC cases often emphasize *measurable* injuries from privacy and data security incidents . . .”).

APPENDIX

Tort	<i>Restatement (Second) Torts</i> Explanation
Intrusion upon seclusion (§ 652B)	One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person .
Appropriation of name of likeness (§ 652C)	One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.
Publicity given to private life (§ 652D)	One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person , and (b) is not of legitimate concern to the public.
False light (§ 652E)	One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person , and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.