U.S. CHAMBER
Institute for Legal Reform

1615 H Street, NW
Washington, DC 20062-2000
www.uschamber.com

October 27, 2017

**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: Informational Injury Workshop P175413**

Dear Mr. Clark:

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

Respectfully Submitted,

Oriana Senatore

Oriana Senatore
Vice President Policy & Research
U.S. Chamber Institute for Legal Reform

## TABLE OF CONTENTS

## I. INTRODUCTION

The U.S. Chamber Institute for Legal Reform ("ILR") is pleased to submit this response to the Federal Trade Commission's (the "FTC" or "Commission") Public Notice seeking comments for its Workshop on Informational Injury ("Workshop").[1] The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than three million companies of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and dedicated to promoting, protecting, and defending America's free enterprise system. ILR is an affiliate of the Chamber dedicated to making our nation's civil legal system simpler, faster, and fairer for all participants. ILR applauds the Commission's work to promote rigorous thinking about injury in the context of privacy and data security. Because data is vital to 21st Century products and services, the potential misuse of information is an important area for attention. ILR highlights two themes as the FTC prepares for the Workshop:

- Policymakers and regulators should define informational injury by focusing on substantial, actual harms rather than conjectural and hypothetical injuries.
- Businesses are aggressively addressing data security and, as victims of attacks, they suffer harm from information misuse.

## II. DIGITAL INFORMATION IS VITAL TO INNOVATION IN A CONNECTED WORLD, AND THE UNITED STATES STRIKES AN APPROPRIATE BALANCE IN PROTECTING DATA PRIVACY.

As the Commission knows, information drives the economy and fuels innovation.[2] Two years ago, the Chamber launched an initiative focused on the intersection between technology and business called the Technology Engagement Center (C_TEC)—which focuses on how

[1] Federal Trade Commission, FTC to Host Workshop on Informational Injury; Seeking Public Comment, *available at* https://www.ftc.gov/system/files/attachments/press-releases/ftc-announces-workshop-informational-injury/public_notice_injury_workshop.pdf ("Public Notice").

[2] *Public Notice* at 1; *see also* Federal Trade Commission, *Big Data: A Tool for Inclusion or Exclusion?*, FTC Report, at 1 (Jan. 2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf. ("[T]he volume, velocity, and variety of data . . . [are] growing at a rapid rate as technological advances permit the analysis and use of this data in ways that were not possible previously.") ("FTC Big Data Report").

emerging technologies like artificial intelligence ("AI"), which is expected to reduce costs and create growth between $14-$33 trillion annually,[3] are changing the nature of business and providing tremendous benefits for society and the economy. The FTC has recognized that data creates opportunities, including increasing educational attainment, providing non-traditional access to credit, increasing the quality of health care by tailoring treatment, and increasing access to employment.[4] As the U.S. Chamber of Commerce Foundation explains:

> The data movement is a force for good. It is fodder for research and a catalyst for innovation. It is the bedrock of informed decision-making and better business and the key to unlocking more efficient, effective government and other services. It unleashes economic growth, competition, profitability, and other breakthrough discoveries. And it is at once a product of an ever-more technologically sophisticated world and a tool to advance, enhance, and shape all of its domains going forward. This widespread emergence and use of Big Data is revolutionary, and history will record the early 21st century as the beginning of a data revolution that defined a century.[5]

Examples of the considerable gains from the data-driven economy abound:

- ***Health care:*** Health care professionals use data to predict epidemics, cure diseases, improve quality of life, and avoid preventable deaths.[6] IBM's Watson—a supercomputer that combines AI and sophisticated analytical software for use in the field of open domain question answering—used AI to diagnose a woman's rare form of leukemia that doctors had incorrectly diagnosed months earlier.[7]
- ***Energy:*** Data has transformed the energy sector. For example, utilities use data analytics to manage energy flow and distribution, and help cities conserve valuable resources.[8] Analytics are driving major changes in energy sourcing and output, helping the United States increase production and export of, for example, natural gas.

---

[3] McKinsey Global Institute, *Disruptive Technologies: Advances that will transform life, business, and the global economy* (2013), *available at* https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies.
[4] *FTC Big Data Report* at 5-8.
[5] U.S. Chamber of Commerce Foundation, *The Future of Data-Driven Innovation*, at 1 (Oct. 2014), *available at* http://www.uschamberfoundation.org/sites/default/files/The%20Future%20of%20Data-Driven%20Innovation.pdf.
[6] MAPR Data Technologies, *Data Convergence in Healthcare* (2017), *available at* https://mapr.com/mapr-guide-big-data-healthcare/.
[7] John Fingas, *IBM's Watson AI saved a woman from leukemia*, Engadget (Aug. 7, 2016), *available at* https://www.engadget.com/2016/08/07/ibms-watson-ai-saved-a-woman-from-leukemia/.
[8] Cambridge Semantics, *Finding Order in Chaos: Governed, Smart Data Lakes Extract Value from Big Data* (Aug. 2017), *available at* http://blog.cambridgesemantics.com/how-big-data-and-the-smart-grid-will-benefit-energy-users.

- ***Innovative Online Services:*** The flow of digital information has led to new online services. For example, Netflix uses viewing data to inform its development of original content.[9] Consumers have an array of free online content, products, and services, including ad-supported search engines and social networking sites.[10]
- ***Government Services:*** The government and citizens benefit from the data-driven economy. Police departments use predictive analytics to prevent crime, and transit agencies analyze location data to manage public transportation.[11] Governments utilize digital information to prevent fraud,[12] enhance education,[13] and promote sustainability.[14]

Consumer data "forms the foundation of a wide variety of services, products, and business models, with enormous benefits to both competition and consumers."[15] Many benefits come when data is reused, combined with other data, and used to answer questions not yet posed when the data was collected.[16] To fully achieve the maximum positive impact, 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

---

[9] *See* David Carr, *Giving Viewers What They Want*, The New York Times (Feb. 24, 2013), *available at* http://www.nytimes.com/2013/02/25/business/media/for-house-of-cards-using-big-data-to-guarantee-its-popularity.html.

[10] *Data Driven Advertising: Consumer Perspective Story*, Introduction, IAB, http://data.iab.com/definition.html#consumer ("An advertising-supported web . . . enables publishers to share their content and services for free with their audiences."); The White House, Exec. Office of the President, Big Data: Seizing Opportunities, Preserving Values, at 41 (May 2014), *available at* https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf. ("Consumers are reaping the benefits of a robust digital ecosystem that offers a broad array of free content, products, and services.").

[11] Public CIO, *Big Data and Analytics*, at 2 (2015), *available at* https://afd34ee8b0806295b5a7-9fbee7de8d51db511b5de86d75069107.ssl.cf1.rackcdn.com/PCIO15_Special_Report_Q3_V.pdf.

[12] *Id.* at 8.

[13] U.S. Department of Education, *Enhancing Teaching and Learning Through Education Data Mining and Learning Analytics* (Oct. 2012), *available at* https://tech.ed.gov/wp-content/uploads/2014/03/edm-la-brief.pdf (highlighting how the Department of Education uses analytics to increase student grades and retention).

[14] Smith School of Enterprise and the Environment, *Big Data and Environmental Sustainability: A Conversation Starter* (Dec. 2014) (noting that big data is increasingly becoming an integral element of environmental sustainability), *available at* http://www.smithschool.ox.ac.uk/library/working-papers/workingpaper%2014-04.pdf.

[15] Maureen K. Ohlhausen and Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80-1 Antitrust L. J. 121, 130, (2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/686541/ohlhausenokuliaralj.pdf.

[16] Bart Custers and Helena Uršič, *Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection* (Feb. 2016), at 4-15, 6 Int'l Data Privacy L. Issue 1, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3046774.

over-burdensome and disproportionate liability.

The current U.S. approach to data privacy strikes a critical balance, protecting sensitive information, while allowing companies and researchers to innovate. This balance has contributed to massive economic growth and is expected to boost U.S. GDP in the decades to come.[17] Though United States businesses and consumers confront a "perilous patchwork" of legal obligations,[18] this regime generally imposes regulation and liability when there is actual or likely harm.

As it considers informational injury, the FTC should avoid following the path of the European Union ("EU"), which treats all personal data as sensitive and belonging only to the consumer, with any exposure causing injury, potentially leading to excessive and abusive litigation.[19] In contrast to the U.S. approach—under which privacy laws tend to be sector-specific and based on data's sensitivity,[20] with U.S. citizens being protected by consumer protection laws, contracts, and sector-specific regimes—the EU treats "data protection and privacy [as] fundamental rights."[21] Under the EU General Data Protection Regulation ("GDPR"), all information and data about EU citizens will be regulated and restricted.[22] This

---

[17] *See* Susan Lund et al., *Game changers: Five opportunities for US growth and renewal*, McKinsey Global Institute (July 2013), *available at* https://www.mckinsey.com/global-themes/americas/us-game-changers.

[18] *See generally* Institute for Legal Reform, *A Perilous Patchwork: Data Privacy And Civil Liberty In The Era Of The Data Breach* (Oct. 2015), *available at* http://www.instituteforlegalreform.com/uploads/sites/1/APerilousPatchwork_Web.pdf.

[19] *See* e.g., EU Charter of Fundamental Rights, Article 8 – Protection of personal data, *available at* http://fra.europa.eu/en/charterpedia/article/8-protection-personal-data.

[20] Health care and financial information are subject to specific restrictions, for example. Brian Eaton, *GDPR: How is it Different from U.S. Law & Why this Matters?*, Lexology (Sept. 14, 2017), *available at* https://www.lexology.com/library/detail.aspx?g=4b2843f7-f67a-4015-bca9-96bd2fe344c9.

[21] European Parliament, Policy Department, Citizens' Rights and Constitutional Affairs, *A Comparison Between US and EU Data Protection Legislation for Law Enforcement*, at 67 (2015), *available at* http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%282015%29536459_EN.pdf.

[22] *See* EU GDPR, *GDPR Key Changes* (noting that the aim of the GDPR is to protect all EU citizens from

threatens to disrupt data flows, is expected to cause up to a 1.3% contraction in EU gross domestic product ("GDP"),[23] and will impose millions of dollars in compliance costs.[24] The United States should avoid this approach and continue to analyze "informational injury" in a manner consistent with traditional U.S. legal principles.

## III. GOVERNMENT SHOULD FOCUS ON SUBSTANTIAL, ACTUAL HARM, NOT HYPOTHETICAL INJURIES.

The FTC's inquiry is timely, given persistent, novel lawsuits about data privacy harm and a coming technology revolution in the Internet of Things, AI, and other innovations. Class action plaintiffs have been pushing courts to relax traditional standing requirements, even after the Supreme Court's decision in *Spokeo, Inc. v. Robins.*[25] As we enter an increasingly data-driven digital future, some want the FTC to expand judicially enforceable data privacy rights that the agency and the plaintiffs' bar can enforce. Doing so would be unwise and would ultimately increase litigation at the expense of technological advancement.

In the Public Notice ("PN"), the FTC defines "information misuse" as information about consumers being "misused by a party with whom they have interacted, by a third party who has accessed that information through a business arrangement, because of a data breach, or through other means."[26] While each of those circumstances is likely to present different facts, it makes sense in each setting for the government to focus on concrete, evidence-based harms. ILR agrees

---

data and privacy breaches under a single directive), *available at* http://www.eugdpr.org/the-regulation.html (last visited Oct. 25, 2017).

[23] U.S. Chamber of Commerce, *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, at 15 (2013), *available at* https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

[24] PricewaterhouseCoopers, *Pulse Survey: US Companies ramping up General Data Protection Regulation (GDPR) budgets* (2017), *available at* https://www.pwc.com/us/en/increasing-it-effectiveness/publications/gdpr-readiness.html.

[25] *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540 (2016).

[26] *Public Notice* at 1.

with Acting Chairman Ohlhausen that government should focus on "stopping substantial consumer injury instead of . . . hypothetical injuries."[27] Chairman Pai of the Federal Communications Commission agrees that "we must act on concrete evidence, not hypothetical harms."[28]

### A. The Commission Should Focus on Evidence of Actual Harm, Guided by Article III's Standing Requirements, To Identify Actionable Injury.

The FTC Act limits the Commission's Section 5 unfairness authority to practices that "cause[] or [are] likely to cause *substantial injury* to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[29] The Constitution's Article III standing requirements limit judicially cognizable harms to concrete, particularized, and actual or imminent injuries.[30] In considering what substantial injury means for Section 5, policymakers and regulators should use the Constitution's standing limitations as minimum expectations to define "harm."[31] Article III principles reflected in *Lujan v. Defenders of Wildlife*,[32] *Clapper v. Amnesty International*,[33] and *Spokeo, Inc. v. Robins*[34] teach that a party must have suffered a concrete, particularized, and

---

[27] Federal Trade Commission, *Painting the Privacy Landscape: Information Injury in FTC Privacy and Data Security Cases*, at 3 (Sept. 19, 2017), *available at* https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf ("Acting Chairman Ohlhausen Remarks").

[28] FCC, Statement of Comm'r Ajit Pai, Concurring in Part and Dissenting in Part to Notice of Proposed Rulemaking And Declaratory Ruling (Nov. 2014), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-185A5.pdf.

[29] 15 U.S.C. § 45(n) (emphasis added).

[30] *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992).

[31] Pursuant to Article III, courts can only decide "cases" and "controversies." U.S. Const. art. III, § 3. "One element of the case-or-controversy requirement is that plaintiffs must establish that they have standing to sue." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 408 (2013) (internal quotations marks omitted).

[32] *Lujan*, 504 U.S. 555.

[33] *Clapper*, 568 U.S. at 408.

[34] *Spokeo*, 136 S.Ct. 1540.

actual or imminent injury.[35] "[C]onjectural" or "hypothetical" injuries are insufficient.[36]

***First***, an injury must be ***particularized*** to the party seeking redress. In *Lujan*, conservationists challenged regulations, arguing that the government's lack of consultation increased the extinction rate of endangered species.[37] While the desire to observe an animal species is cognizable,[38] the Constitution "requires more than an injury to a cognizable interest. It requires that the party seeking review be himself among the injured."[39] ***Second,*** an injury must be ***concrete***. A statutory violation without actual harm is not enough. In *Spokeo*, the Court found that a consumer did not have standing to sue under the Fair Credit Reporting Act of 1970 (the "FCRA")[40] for a company's violation of the FCRA's procedural requirements—such as a consumer reporting agency having an incorrect zip code on file. The Court noted that an injury must be particularized[41] and rejected the argument that statutory violations are *de facto* concrete, reasoning that actual harm must occur.[42] While a statutory violation could lead to a concrete harm, standing requires more than just the "bare procedural violation."[43] ***Third,*** an injury must be ***actual or imminent***. A "threatened injury must be *certainly impending* to constitute injury in fact," and "[a]llegations of *possible* future injury" are not sufficient.[44]

---

[35] *Lujan*, 504 U.S. at 560-61. The other standing elements require that injury be traceable to the defendant's actions, and it must be likely that a favorable decision will redress the injury.
[36] *Id.* at 560.
[37] *Id.* at 559, 562.
[38] *See Sierra Club v. Morton*, 405 U.S. 727 (1972).
[39] *Lujan*, 504 U.S. at 562-63. *See also Sierra Club*, 405 U.S. at 734-735 (noting that, although "[a]esthetic and environmental well-being . . . are important ingredients of the quality of life of our society," standing requires an injury to be both cognizable and specific to the person asserting a claim).
[40] *Spokeo*, 136 S.Ct. 1540.
[41] *Id.* at 1548.
[42] *Id.* at 1549-50 (citing *Summers v. Earth Island Inst.*, 555 U.S. 488, 496 (2009) (holding that "[d]eprivation of a procedural right without some concrete interest that is affected by the deprivation . . . is insufficient to create Article III standing")).
[43] *Id.* at 1550.
[44] *Clapper*, 568 U.S. at 409 (citations omitted).

### B. Despite *Spokeo*, Plaintiffs Still Bring "No-Injury" Claims about Broad Informational Injury.

Courts continue to confront cases advancing claims based on speculative harm in the data security context. The Second Circuit has held that the possibility that an attacker might use stolen information in the future is too speculative to constitute injury.[45] Likewise, the Fourth Circuit correctly found in a data breach case that "*Clapper*'s discussion of when a threatened injury constitutes an Article III injury-in-fact is controlling."[46] By contrast, the Seventh Circuit in a similar case held that the loss of personal information is sufficient,[47] and the D.C. Circuit held that plaintiffs in a data breach class action had standing based on allegations that the theft of their information could be used to harm them in the future.[48] Policymakers and courts should follow the Second and Fourth Circuits and, more importantly, Supreme Court precedent. The Supreme Court has made clear that injury-in-fact requires the plaintiff to allege real-world adverse consequences from an alleged violation. The Seventh and D.C. Circuits would confer Article III standing on any plaintiff subject to a data breach based on the fear of future harm.

A recent FTC case highlights the insufficiency of a mere statutory violation without a claim of actual harm. Even though the case does not deal with Article III standing directly, its lessons are in line with the Supreme Court's standing requirements. In early 2017 in *FTC v. D-Link Corp.*, the Commission filed a complaint against D-Link, a manufacturer of routers, IP cameras, and other computer hardware, in the Northern District of California.[49] The complaint alleged that D-Link failed to take reasonable steps to protect devices it sold, which left them

[45] *Whalen v. Michaels Stores, Inc.*, 689 F. App'x. 89 (2d Cir. 2017).
[46] *Beck v. McDonald*, 848 F.3d 262, 272 (4th Cir. 2017).
[47] *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015).
[48] *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017).
[49] Complaint for Permanent Injunction and Other Equitable Relief, *FTC v. D-Link Corp.*, 2017 WL 65168 (N.D. Cal. Jan. 5, 2017).

vulnerable to "a significant risk of unauthorized access."[50] D-Link moved to dismiss, arguing that the FTC had failed to assert actual or likely injury, and instead relied on speculative harm.[51] The court agreed, finding that the Commission failed to identify a single incident involving an exploitation.[52] The court noted that the FTC was relying on "a mere possibility of injury at best," which fails to provide a basis for action.[53] This was not the first time that the Commission has acted on the possibility of harm—it has earlier alleged that a company's unreasonable data security practices violate Section 5, even where there was no evidence that an attack exploited a claimed vulnerability.[54]

The implications are clear: in the informational injury context, a mere violation of a privacy policy or similar commitment should not be cause for action if it does not result in a concrete harm, the substantiality of which is established with evidence and not mere speculation. The FTC should clarify that "substantial harm" requires tangible, actual harm, or an imminent threat of same, as in traditional Article III requirements. It should look to evidence and not fear or speculation, particularly about the malicious acts of third parties. These principles should form the bare minimum for any substantial harm analysis under Section 5.

### C. Addressing Hypothetical Injuries May Have Unintended Consequences.

---

[50] *Id.*

[51] Plaintiff's Response in Opposition to Defendant D-Link Corporation's Motion to Dismiss, *FTC v. D-Link Corp.*, 2017 WL 4678937 (N.D. Cal. Apr. 17, 2017).

[52] Order Re Motion To Dismiss, *FTC v. D-Link Corp.*, 2017 WL 4150873, (N.D. Cal. Sept. 19, 2017).

[53] *Id.* at *5. The district court suggested to the FTC an alternative theory of harm, but that theory has its own infirmities and likewise would strain the actual harm requirement.

[54] *See, e.g.*, *In the Matter of HTC America Inc.*, FTC File No. 1223049 (2013) (asserting Section 5 authority by claiming that HTC introduced numerous security vulnerabilities in the process of customizing its mobile devices' operating system, even though there was no evidence of exploitation). In general, the FTC has been active in bringing informational injury enforcement actions. *See, e.g.*, *In the Matter of Taxslayer, LLC*, No. 1623063 (2017) (FTC alleged that malicious hackers gained full access to nearly 9,000 TaxSlayer accounts between October and December 2015); *In the Matter of Lenovo Inc.*, No. 1523134 (2017) (FTC alleged that Lenovo harmed consumers by pre-loading software on some laptops that compromised security protections to deliver ads).

Focusing on hypothetical injuries can cause "unintended side effects"[55] and consumer harm. Examples include:

- ***Imposing Unnecessary Costs:*** If policymakers or regulators stray from addressing activity that threatens or causes substantial harm, they encourage "no injury" litigation that has little benefit for consumers or the economy. The number of data privacy and security related lawsuits has increased significantly in recent years.[56] Firms specialize in class actions and the so-called "lighting rod effect"—where attorneys file multiple cases against single companies connected to large, publicized breaches.[57] The number of class actions related to data breaches increased 7% from 2015 to 2016, with most clustering around the same high-profile breaches.[58] Such actions come on top of actions from FTC, state attorneys general, and Congressional oversight activity. In 2015 alone, U.S. companies spent an average of $7.01 million on each data breach, including litigation costs.[59] Because of litigation costs, the United States is the most expensive country in the world for a corporation to the victimized by a data breach.[60]

- ***Worsening Notice Fatigue:*** An overly broad approach to informational injury will generate too many consumer disclosures, resulting in notice fatigue.[61] If the government requires that consumers be inundated with incident notifications that do not flag actual and concrete harms, consumers may be less likely to react appropriately in the case of a breach that is likely to cause actual harm. This counsels in favor of limiting corrective action to instances where there is concrete harm or a strong likelihood of such harm.

- ***Exacerbating Security Fatigue:*** Broad notions of "informational injury" may lead to security fatigue, which the National Institute of Standards and Technology ("NIST")

---

[55] *Acting Chairman Ohlhausen Remarks* at 3.

[56] U.S. Chamber Institute for Legal Reform, *Engineered Liability: The Plaintiffs' Bar's Campaign to Expand Data Privacy and Security Litigation*, at 2 (Apr. 2017), *available at* http://www.instituteforlegalreform.com/research/engineered-liability-the-plantiffs-bars-campaign-to-expand-data-prviacy-and-security-litigation.

[57] *See* Shayna Posses, *How Lawyers Are Keeping Hacked Clients Out of Court*, Law 360 (June 27, 2017), *available at* https://www.law360.com/articles/936095/how-lawyers-are-keeping-hacked-clients-out-of-court.

[58] David Zetoony et al., *2016 Data Breach Litigation Report*, 19-3 J. of Consumer & Com. L. 150 (2016) *available at* http://www.jtexconsumerlaw.com/V19N3/V19N3_Data.pdf.

[59] IBM & Ponemon Institute, *2016 Cost of Data Breach Study: United States*, at 2 (June 2016), *available at* https://securityintelligence.com/cost-of-a-data-breach-2016/.

[60] IBM & Ponemon Institute, *2017 Cost of Data Breach Study: Global Overview*, at 5 (July 2017), *available at* https://securityintelligence.com/media/2017-ponemon-institute-cost-of-a-data-breach-study/.

[61] Prepared Statement of the FTC, Hearing on Discussion Draft of H.R.__, Data Security and Breach Notification Act of 2015 Before the Subcomm. on Commerce, Manufacturing, & Trade of the H. Comm. on Energy & Commerce, 114th Cong. (Mar. 18, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/630961/150318datasecurity.pdf ("[A]ny trigger for providing notification should be sufficiently balanced so that consumers can take steps to protect themselves when their data is at risk, while avoiding over-notification, which may confuse consumers or cause them to ignore the notices they receive.").

describes as a weariness or reluctance to deal with computer security caused by people "being bombarded by 'watch out for this or watch out for that.'"[62] A majority of computer users experience security fatigue, which leads users to risky computing behavior at work and in their personal lives.[63] Given the digitization of modern life—*e.g.*, online banking, digitized health records, and online commerce—this could impact our future security and economic welfare. The FTC has an important role to play in avoiding security fatigue and has acknowledged in other settings that "overly extensive disclosures" can harm consumers.[64] The FTC can help by continuing to call for reasonable uniform federal data breach notification standards.[65]

- ***Taxing Government Resources:*** Expanding the concept of actionable "informational injury" to more speculative injuries will divert limited government resources away from serious problems and actual consumer harm. Policymakers should focus on preventing and redressing concrete and serious harms.

The FTC can mitigate such effects by recognizing harm from "informational injuries" only when consumers face concrete, particularized, and actual or imminent injury.

## IV. CONSUMERS' PERCEPTIONS AND BALANCING OF PRIVACY AND CONVENIENCE ARE COMPLEX AND EVOLVING.

The FTC asks how "consumers perceive and evaluate the benefits, costs, and risks of sharing information in light of potential injuries."[66] Consumers have shown an ability to balance

---

[62] NIST, *'Security Fatigue' Can Cause Computer Users to Feel Hopeless and Act Recklessly, New Study Suggests* (Oct. 4, 2016), *available at* https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly.

[63] *Id.*

[64] Federal Trade Commission Public Comment on "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers" Communicating Upgradability and Improving Transparency Working Group, at 6, *available at* https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications-information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf.

[65] Prepared Statement of the FTC, Hearing on Discussion Draft of H.R.__, Data Security and Breach Notification Act of 2015 Before the Subcomm. on Commerce, Manufacturing, & Trade of the H. Comm. on Energy & Commerce, 114th Cong., at 9 (Mar. 18, 2015), *available at* http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-RichJ-20150318.pdf (noting that the FTC has long supported a federal notification law on a bipartisan basis); Prepared Statement of the FTC on Data Security Before the Subcomm. on Commerce, Manufacturing, & Trade, of the H. Comm. on Energy & Commerce, 112th Cong., at 11 (May 4, 2011), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110504datasecurityhouse.pdf. ) (reiterating FTC support for federal legislation on breach notification).

[66] *Public Notice* at 1.

the benefits and risks associated with the digital economy, and they benefit from many choices in how to interact online. Consumers' views on privacy depend on individualized factors, making it difficult for a policymaker or regulator to assess what "consumers" as a group want.[67] The government should exercise caution in predicting consumers' complex, personalized, and shifting expectations.

Policymakers can struggle to keep pace with the rapid technological innovation that defines the modern economy.[68] Likewise, consumers' privacy preferences rapidly evolve. A 2016 Pew Report found that consumers' preferences on "offer[ing] information about themselves in exchange for something of value are shaped by both the conditions of the deal and the circumstances of their lives."[69] As the Pew Report notes, privacy preferences are shaped by individual circumstances. It is unrealistic to assume that the expectations of someone born in the last decade—a so-called "digital native"—will be the same as someone who came to technology later in life. Research has shown the variability in consumer privacy preferences is driven by numerous complex factors.[70] It is not only difficult to capture consumers' privacy preferences at a given moment, but misleading to assume that all consumers possess the same preferences.

A desire to define informational harm broadly may be driven, in part, by the concern that

---

[67] *See* Tim McKay, PhD, CISSP, *Who Are You? Authenticating Consumer Identity Is Becoming Increasingly Important in Healthcare*, 85-9 J. Ahima 32 (Sept. 2014), *available at* http://library.ahima.org/doc?oid=107441#.VzpB7XIUWUk (noting that "security and privacy judgments are personal").

[68] *See* Nerushka Bowman, *How does regulation keep up with technology and innovation: Part 1* (June 23, 2017), *available at* http://nerushkabowan.com/2017/06/23/how-does-regulation-keep-up-with-technology-and-innovation-part-1/.

[69] Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, Pew Research Center (Jan. 14, 2016), *available at* http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/ ("2016 Pew Report").

[70] *See, e.g.*, *Rethinking Personal Data: Trust and Context in User-Centered Data Ecosystems*, World Economic Forum, 4 (2014), *available at* http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf (finding that preferences vary based on type of data, type of entity, device type, collection method, data usage, trust in service providers, value exchange, as well as attitudes about and adeptness with technology, awareness about the personal data ecosystem, and perceptions of government protection).

consumers are not able to make informed decisions. This is incorrect. Increasingly, consumers are making decisions with an understanding of the current ecosystem,[71] demonstrating knowledge of tradeoffs associated with today's digital economy. One example is the rapid proliferation of smartwatches and fitness trackers, for which "consumers have been willing to sacrifice a little privacy to gain the benefits associated with [the devices]: improved wellness, vanquishing unhealthy eating habits, and feeling more liberated to manage their health."[72] Consumers balance competing values[73] and, in encouraging news, they are increasingly taking steps to protect themselves against cybersecurity threats. A recent study showed that 77% of Americans now use PINs or passwords on their smartphones—a 54% increase in the last five years.[74] That study showed a 58% increase in the percentage of Americans with an anti-virus program installed on their smartphones.[75] Consumers' privacy expectations are diverse and influenced by the entire digital ecosystem.

## V. DESPITE BUSINESSES' CONCERN ABOUT DATA SECURITY AND THE CARE THEY TAKE IN HANDLING INFORMATION, THEY ARE STILL VICTIMIZED BY INFORMATION MISUSE AND DATA BREACHES.

The FTC asks about informational injury to businesses, as well as how businesses

---

[71] James C. Cooper, *Lessons From Antitrust: The Path to a More Coherent Privacy Policy*, U.S. Chamber of Commerce (Feb. 2017), *available at* https://www.uschamberfoundation.org/reports/lessons-antitrust-path-more-coherent-privacy-policy.

[72] Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, Washington Lawyer (Dec. 2015), *available at* https://www.dcbar.org/bar-resources/publications/washington-lawyer/articles/december-2015-data-privacy.cfm.

[73] James C. Cooper, *Lessons From Antitrust: The Path to a More Coherent Privacy Policy*, U.S. Chamber of Commerce (Feb. 2017), *available at* https://www.uschamberfoundation.org/reports/lessons-antitrust-path-more-coherent-privacy-policy.

[74] CTIA – The Wireless Association, *Consumers Increasingly Adopting Safeguards to Protect Mobile Devices Against Cybersecurity Threats* (Oct. 20, 2017), *available at* http://www.publicnow.com/view/6800C13C13CB002D227CF6978190A18BED5AE7D3?2017-10-20-11:00:17+01:00-xxx8027.

[75] *Id.* The study also indicated a 43% increase in the percentage of Americans with the ability to remotely locate, lock, and erase software on their smartphones.

evaluate the risks related to data collection and breaches.[76] American businesses are constantly under attack by malicious actors. Some advocates for expanded privacy harms claim that businesses are cavalier and corporate security officials have "yet to grasp a fundamental reality of the modern business world."[77] They blame the rise in data breaches on lax corporate concern. Quite the contrary. Businesses work hard to protect customers' data, investing heavily in prevention and remediation. No company wants to be the next victim.

Cyber criminals target businesses and other organizations to steal consumer data and intellectual property, commit fraud, conduct espionage, or disrupt operations, among other motives. The business service and health care sectors alone accounted for over 80% of all breaches in 2016,[78] and 43% of all attacks target small businesses.[79] These attacks do not mean that companies are not taking cybersecurity seriously. Companies are taking significant steps to protect themselves and the data they collect, store, and use. For example, Microsoft invests over $1 billion annually on cybersecurity.[80] Bank of America has stated that it has an "unlimited budget" to prevent cybercrime.[81] According to *Forbes*, total spending on security awareness *training alone* reaches $1 billion every year.[82] The U.S. Chamber has been leading a national

---

[76] *Public Notice* at 1.
[77] Amicus Brief of National Consumers League at 7, *Attias v. CareFirst Inc.*, 1:15-cv-882 (D.C. Cir No. 16-7108) (Doc. No. 1657795) (01/27/2017).
[78] ITRC, *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at* http://www.idtheftcenter.org/2016databreaches.html.
[79] Joshua Sophy, *43 Percent of Cyber Attacks Target Small Business*, Small Business Trends (June 21, 2016), *available at* https://smallbiztrends.com/2016/04/cyber-attacks-target-small-business.html.
[80] Cybersecurity Ventures, *Cybersecurity Market Report* (2017), *available at* https://cybersecurityventures.com/cybersecurity-market-report/.
[81] Steve Morgan, *Bank of America's Unlimited Cybersecurity Budget Sums Up Spending Plans in War Against Hackers*, Forbes (Jan. 27, 2016), *available at* https://www.forbes.com/sites/stevemorgan/2016/01/27/bank-of-americas-unlimited-cybersecurity-budget-sums-up-spending-plans-in-a-war-against-hackers/#3a3d9060264c.
[82] Steve Morgan, *The Business of Cybersecurity: 2015 Market Size, Cyber Crime, Employment, and Industry Statistics*, Forbes (Oct. 16, 2015), *available at* https://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-

discussion on cybersecurity, promoting the NIST *Framework for Improving Critical Infrastructure Cybersecurity*[83] and helping members across the country. The Chamber has a Cyber Leadership Council[84] and recently hosted its Sixth Annual Cybersecurity Summit in Washington, as well as large events in Nashville, TN, Columbia, SC, and Glen Ellyn, IL.

Despite significant and sound risk management practices, attacks are unrelenting and becoming more sophisticated.[85] Indeed, experts agree that intrusions and breaches are not a matter of "if" but "when." "The hackers today have the advantage because they have time on their side and they only have to be correct once to initiate a compromise while a corporation has to be correct 100 percent of the time to keep hackers at bay."[86] This is just as true for federal agencies like the Securities and Exchange Commission and, famously, the Office of Personnel Management, which was victimized by theft of information of as many as 18 million people.[87] In 2016, there were approximately 1.6 billion records reported stolen or improperly disclosed, an increase from 480 million in 2015.[88] Ransomware attacks increased by 300% between 2015 and

---

cyber-crime-employment-and-industry-statistics/#3e8765535d0d.

[83] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), *available at* https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[84] *See* Press Release, U.S. Chamber of Commerce, *U.S. Chamber Announces Launch of Cybersecurity Leadership Council* (July 7, 2015), https://www.uschamber.com/press-release/us-chamber-announces-launch-cybersecurity-leadership-council.

[85] Mandiant, *M-Trends 2017: A View From the Front Lines*, at 9 (2017), *available at* https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html.

[86] Helpnet Security, *Industry reactions to the Deloitte cyber attack* (Sept. 25, 2017), *available at* https://www.helpnetsecurity.com/2017/09/25/industry-reactions-deloitte-cyber-attack/ (quoting Sam Curry, CSO, Cybereason).

[87] Evan Perez & Shimon Prokupecz, *U.S. data hack may have been 4 times larger than the government originally said*, CNN (June 24, 2015) *available at* http://edition.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html; Sam Sanders, *Massive Data Breach Puts 4 Million Federal Employees' Records at Risk*, NPR (June 4, 2015) *available at* http://www.npr.org/sections/thetwo-way/2015/06/04/412086068/massive-data-breach-puts-4-million-federal-employees-records-at-risk.

[88] Lewis Morgan, *List of data breaches and cyber attacks in 2016 – 3.1 billion records leaked*, IT Governance (Dec. 12, 2016), *available at* https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2016-1-6-billion-records-leaked/.

2016.[89] The majority of fraud now takes place online,[90] which provides criminals with a larger attack surface than traditional fraud targets and one where crimes often go unpunished.[91] There is no such thing as perfect security, and even the most technologically innovative, state-of-the-art security protocols will not prevent all attacks from succeeding.[92]

Policymakers and regulators must remember that behind every malicious data breach is a criminal who has willfully violated U.S. law to harm a business, its employees, consumers, and investors. In discussing informational injury, Acting Chairman Ohlhausen noted how data breaches impact consumers.[93] These harms are also devastating to businesses that fall victim to a breach. Harms suffered by victim companies include:

- ***Significant Costs and Financial Injury***: Even when a breach has not harmed consumers, the current patchwork regulatory regime subjects businesses to significant costs and financial injury, with lawsuits, regulatory oversight, and compliance costs piled on top of the operational costs of response and recovery.

- ***Property Loss, Including Consumer Data and Intellectual Property:*** The forecast average loss for a breach of 1,000 records is between $52,000 and $87,000.[94] These losses add up quickly. For example, there were 980 breaches in 2016, with over 35 million records exposed.[95] In addition to losing valuable consumer data that businesses expend resources obtaining, breaches can expose private records related to employees. Companies' intellectual property is also at risk. As former NSA chief General Keith Alexander said years ago, cybercrime and "[t]he loss of industrial information and intellectual property through cyber espionage constitutes the 'greatest transfer of wealth

---

[89] *See* DOJ, Computer Crime and Intellectual Property Section, *How to Protect Your Networks from Ransomware*, at 2 (2016), *available at* https://www.justice.gov/criminal-ccips/file/872771/download.
[90] Verizon, *2017 Data Breach Investigations Report*, at 21, *available at* www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.
[91] *Id.*
[92] Paul Rubens, *Cybersecurity: Defending 'unpreventable' cyber attacks*, BBC News (Feb. 3, 2015), *available at* http://www.bbc.com/news/business-31048811.
[93] *Acting Chairman Ohlhausen Remarks*, at 5-8.
[94] Verizon, *2015 Data Breach Investigations Report*, at 29, *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf.
[95] Identity Theft Resource Center, *2016 Data Breach Category Summary* (Dec. 13, 2016), *available at* http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2016.pdf.

in history.'"[96] The theft of companies' intellectual property results in a loss of competitiveness—on a company-by-company basis, as well as at the national level.

- ***Reputational Injury:*** Nearly all harms suffered in the wake of information misuse implicate reputation.[97] This is certainly true for businesses, for whom reputation is valuable.[98] Notable large-scale attacks have led to a considerable loss in company reputation and revenue. One survey found that when a company suffers a breach, the majority of people say they will not do business with that company.[99]

To help mitigate some of the damage from attacks, policymakers should simplify the post-breach regulatory landscape by adopting a federal standard for breach notification. Such a standard, consistent with the best approaches in state law and recognizes that both consumers and businesses are victims of data breaches, would help address informational injury suffered by businesses from information misuse, reduce confusion in the marketplace, and provide consumers and businesses with clear expectations.[100]

## VI. CONCLUSION

The U.S. Chamber Institute for Legal Reform urges policymakers and regulators at the state and federal level to take care in considering the legal and regulatory framework surrounding injury from information misuse, and focus on the risks of actual, concrete harm to set a baseline for "substantial injury." The FTC should act upon evidence and objective criteria, not speculation and hypotheses. Overall, policymakers should be looking to reduce complexity, regulatory uncertainty, and post-breach burdens that do not clearly help consumers. This

---

[96] J. Rogin, *NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history"*, Foreign Policy (July 9, 2012), *available at* http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.
[97] *See Acting Chairman Ohlhausen Remarks* at 7-8.
[98] *See* Martin Armstrong, *The World's Most Valuable Brands*, Statista: The Statistics Portal (Sept. 26, 2017), *available at* https://www.statista.com/chart/11250/the-worlds-most-valuable-brands/ (estimating Apple's brand value at over $184 billion).
[99] Semafone, *86% of Customers Would Shun Brands Following a Data Breach* (Mar. 27, 2014), *available at* https://semafone.com/press-releases/86-customers-shun-brands-following-data-breach/.
[100] U.S. Chamber of Commerce, *2016 U.S. Chamber Policy Priorities*, at 26, *available at* https://www.uschamber.com/sites/default/files/2016_policy_priorities-final.pdf.

includes helping limit no-injury lawsuits after data breaches and promoting a uniform federal breach notification regime.