



Federal Trade Commission
Office of the Secretary
Constitution Center
400 7th Street, SW, 5th Floor, Suite 5610 (Annex A)
Washington, D.C. 20024

October 27, 2017

Re: Informational Injury Workshop P175413

Internet Association (“IA”) appreciates the opportunity to comment on the Federal Trade Commission’s (“FTC” or “Commission”) evaluation of consumer harms in the privacy and security context.¹ IA commends the FTC for recognizing the vital use of information flows in today’s economy and focusing the workshop on the dual aims of preserving those information flows – which are necessary to continued innovation and progress – and the importance of protecting consumers.

IA is the unified voice of the Internet economy, which has led to the creation of millions of jobs and comprises 6% of the U.S. Gross Domestic Product.² It represents the interests of America’s leading Internet companies and their global community of users,³ and it is dedicated to advancing public policy solutions that strengthen and protect Internet freedom, foster innovation and economic growth, and empower users. The Internet economy relies on the flow of information to function and grow, and IA and its members have witnessed first-hand the effects of heavy-handed data privacy and security regulation on competition and innovation – particularly how sweeping legislation or aggressive regulations can thwart nascent technologies and young online companies disproportionately.

¹ *FTC to Host Workshop on Informational Injury; Seeking Public Comments*, Public Notice (Sept. 29, 2017), available at https://www.ftc.gov/system/files/attachments/press-releases/ftc-announces-workshop-informational-injury/public_notice_injury_workshop.pdf (“Public Notice”).

² See, e.g., *Measuring the U.S. Internet Sector*, Steven Siwek for the Internet Association, 5-7 (Dec. 10, 2015), available at <http://internetassociation.org/wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf>.

³ IA’s members include Airbnb, Amazon, Coinbase, Doordash, Dropbox, eBay, Etsy, Expedia, Facebook, Google, Groupon, Handy, HomeAway, IAC, Intuit, LinkedIn, Lyft, Match Group, Microsoft, Monster, Netflix, Pandora, PayPal, Pinterest, Quicken Loans, Rackspace Hosting, Reddit, Salesforce, Snap Inc., Spotify, Survey Monkey, Ten-x, Thumbtack, TransferWise, TripAdvisor, Turo, Twitter, Uber, UpWork, Yelp, Zenefits, Zillow Group, and Zynga.



In the Public Notice, the Commission seeks comment on, *inter alia*, the different types of injuries from data privacy and security incidents, frameworks to assess and quantify such injuries, and how such frameworks might differ for different types of injury.⁴ It also seeks comment on how consumers perceive and evaluate the benefits, costs, and risks of sharing information and how businesses evaluate the risks of informational injuries.⁵

As discussed in more detail below, the FTC should focus its data privacy and security efforts in the first instance on the informational injuries that Congress has specifically directed the FTC to enforce under Federal legislation. When the Commission brings a privacy or security enforcement action under Section 5 of the FTC Act, it should ensure that such enforcement addresses actual, concrete injuries instead of speculative or presumed harms. This analysis should be supported by substantial empirical data and analytical rigor, rather than instinct, speculation, or intuition. In evaluating the costs and benefits of a given practice, the FTC should recognize that consumers are increasingly sophisticated when it comes to understanding how digital products work and the benefits they receive from data-driven innovation and free, ad-supported online content. It should also help empower consumers and businesses further through outreach and education efforts, including by raising awareness further about available privacy tools, data hygiene, and other best practices.

I. The FTC Should Prioritize Data Privacy and Security Enforcement Where Specifically Directed by Congress

The American people, through Congress, have repeatedly taken clear positions with respect to the privacy- and data security- related matters that merit heightened protection. With respect to the FTC, Congress has shown time and again that it can: (1) pass targeted privacy and security legislation; and (2) expressly authorize the FTC to enforce such laws when appropriate. For example:

- The Children’s Online Privacy Protection Act⁶ (“COPPA”) requires specific privacy protections for information collected from children;
- The Health Information Technology for Economic and Clinical Health (“HITECH”) Act⁷ requires data breach notifications for certain health information;
- The Fair Credit Reporting Act⁸ (“FCRA”) regulates the collection, dissemination and use of consumer identity and creditworthiness information; and
- The Gramm-Leach-Bliley Act⁹ (“GLBA”) governs the use and disclosure of nonpublic personal financial information.

In addition to these sector- and information-specific privacy laws, the FTC also plays a role in protecting consumers from unwanted and potentially intrusive commercial messages under the

⁴ See Public Notice.

⁵ *Id.*

⁶ 15 U.S.C. §§ 6501-06.

⁷ Pub. L. 111–5 § 13410(d).

⁸ 15 U.S.C. § 1681.

⁹ Pub. L. 106-102.



Controlling the Assault of Non-Solicited Pornography and Marketing (“CAN-SPAM”) Act¹⁰ and the Telemarketing Consumer Fraud and Abuse Prevention Act.¹¹

The FTC should respect Congress’ determinations and focus its data privacy and security enforcement in the first instance on addressing the informational harms that Congress has expressly directed the Commission to prevent.

II. The FTC’s Efforts to Identify and Address Informational Injuries Should Focus on Actual, Concrete Consumer Harms

As the FTC seeks to identify and measure informational injuries present in data privacy and security incidents, the Commission should focus on instances in which there is actual, concrete harm that is supported by empirical data and robust analysis. In contrast, purely theoretical or assumed harms, or the mere possibility of future harm, would be insufficient to form the basis of an informational injury. In essence, informational injuries must involve harms that are provable based on actual facts, not presumed based on intuition.

As the Commission has recognized, actual, concrete consumer harm is most likely to be found where quantifiable economic loss has occurred.¹² For example, where a bad actor hacks a consumer financial account and uses the access to manipulate funds, it is clear that there has been an actual financial injury to the consumer, to the financial institution, or both. As another example, where a malware attack leads to the shutdown of an online commerce platform, that act may lead to a readily identifiable and quantifiable loss of profits for the operator of the platform and similar losses to a small business owner who relies on the platform to serve its customers.

The need to identify actual, concrete harms does not necessarily exclude emotional or other intangible harms from qualifying as informational injuries. But such harms should be clearly demonstrable and supported by robust, data-driven economic and empirical analyses. As Acting Chairman Ohlhausen recently stated, consumer informational injuries should be *measurable*.¹³ Moreover, the alleged harms cannot be speculative or theoretical – the focus on “*real*, not speculative, consumer harm . . . is part of [the] statute.”¹⁴ It is far less likely that subjective emotional harms alone could be sufficiently concrete to support Section 5 enforcement.

¹⁰ Pub. L. 108-187.

¹¹ 15 U.S.C. §§ 6101-6108.

¹² See, e.g., FED. TRADE COMM’N, POLICY STATEMENT ON UNFAIRNESS (1980), available at <https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness>.

¹³ See Acting Chairman Maureen K. Ohlhausen, *Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases* (Sept. 19, 2017), available at https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf.

¹⁴ See, e.g., Remarks of FTC Commissioner Maureen K. Ohlhausen, *The Internet of Everything: Data, Networks & Opportunities at the U.S. Chamber of Commerce Foundation and U.S. Chamber’s Center for Advanced Technology & Innovation*, Washington, D.C. (Sept. 22, 2015); FED. TRADE COMM’N, *Protecting Consumer Privacy in an Era of Rapid Change*, Preliminary Staff Report (2010) (citing Remarks of FTC Chairman Tim Muris at the Privacy 2001 Conference (Oct. 4, 2001)); FED. TRADE COMM’N, POLICY STATEMENT ON DECEPTION (1983), *appended to* Cliffdale Assocs., Inc., 103 F.T.C. 110, 175, 182-83 (1984).



Most importantly, by prioritizing informational injuries that involve actual, concrete consumer harm, the FTC’s allocation of resources would be in alignment with the core mandate of Section 5 to bring enforcement actions in the public interest.¹⁵

A. The FTC’s Assessment of Informational Injuries Should be Guided by Robust, Data-Driven Economic and Empirical Analyses

The FTC should look to economics and statistics to support the development of a robust analytical framework that is grounded in demonstrable, established theories and evidence from the market.¹⁶ The FTC is well-positioned to draw on existing internal resources to support data-driven determinations of informational injuries: the Bureau of Economics houses expertise dedicated to ascertaining the effects of specific market activities on consumer welfare and competition.¹⁷

By leveraging existing Bureau of Economics experience and knowledge and rigorously analyzing alleged consumer harms, the FTC can both (1) empirically assess whether and to what extent an alleged informational injury causes or is likely to cause a tangible negative effect on consumer welfare, and (2) direct its enforcement efforts on those alleged informational injuries that it has ascertained cause the greatest amount of such consumer harm. To support this effort, the FTC should allocate sufficient resources to the Bureau of Economics and ensure that all informational injury determinations – especially any that are based on an alleged “likelihood” of harm¹⁸ – are the result of robust, systematic, and defensible analyses.

B. The FTC Should Take Action for Deception Only Where a Statement or Omission Has a Provable Effect on Consumer Behavior

The FTC has made it clear that not all misstatements rise to the level of deception in violation of Section 5. Only where a misstatement (or omission) is *material* is action warranted. As Acting Chairman Ohlhausen has pointed out, however, the FTC has not always adhered to the materiality standard. For example, in *Nomi*,¹⁹ a divided Commission issued a complaint and

¹⁵ 15 U.S.C. § 45(b).

¹⁶ See Dissenting Statement of Commissioner Joshua D. Wright, *In the Matter of Apple, Inc.*, FTC File No. 1123108 (Jan. 15, 2014) (discussing how economic theory and analysis should have been used to ascertain the effects of the consent order on consumers and arguing that the Commission should not support a case without demonstrating through rigorous analysis that the cost of the alleged action outweighed the benefit to consumers or the competitive process).

¹⁷ See Joshua Wright, *The FTC and Privacy Regulation: The Missing Role of Economics*, Speech at the George Mason University Law and Economic Center’s Briefing on *Nomi*, Spokeo, and Privacy Harms (Nov. 12, 2015), available at http://masonlec.org/site/rte_uploads/files/Wright_PRIVACYSPEECH_FINALv2_PRINT.pdf.

¹⁸ See, e.g., 15 U.S.C. § 45(n); see also *LabMD, Inc. v. FTC*, No. 16-16270-D, Order Granting Stay (11th Cir. Nov. 10, 2016) (“it is not clear that a reasonable interpretation of § 45(n) includes intangible harms like those that the FTC found in this case”); *FTC v. D-Link Corp.*, Case No. 3:17-cv-000039-JD (N.D. Cal. Sept. 19, 2017) (order partially granting motion to dismiss) (stating the sum total of harms “make out a mere possibility of injury at best” and “stands in sharp contrast to complaints that have survived motions to dismiss”).

¹⁹ FTC File No. 1323251 (Aug. 28, 2015).



accepted a proposed consent order about a company that offered tracking analytics services to brick-and-mortar retailers. Nomi's privacy policy stated that it offered an opt out of its tracking technology both online and at the physical retail locations, although some physical retailers never implemented the opt-out mechanisms. The FTC's complaint presumed that the lack of an in-person opt out (while an online was available) was material – that it caused people to behave differently than they otherwise would have. However, there was no evidence to support this position.²⁰

As then-Commissioner Ohlhausen noted in her dissent, the FTC “should not apply a *de facto* strict liability approach to a young company that attempted to go above and beyond its legal obligation to protect consumers but, in so doing, erred without benefiting itself. I fear that the majority's decision in this case encourages companies to do only the bare minimum on privacy, ultimately leaving consumers worse off.”²¹

Similarly, it also remains unclear how the FTC evaluated materiality or quantified the consumer harm in *In re Goldenshores Technologies, LLC*. In that matter, an app privacy policy failed to disclose to consumers that the app transmitted users' precise location and unique device identifier to third parties. The FTC's complaint assumes this to be a material omission and thus a harm to consumers, but no publicly released analysis or evidence accompanies this statement.²²

²⁰ See, e.g., Dissenting Statement of Commissioner Joshua D. Wright, *In the Matter of Nomi Technologies, Inc.*, FTC File No. 1323251 (Apr. 23, 2015) (stating that “[a]ctual evidence of consumer behavior indicates that consumers that were interested in opting out of the Listen service took their first opportunity to do so” and that “[t]o presume the materiality of a representation in a privacy policy concerning the availability of an additional, in-store opt-out mechanism requires one to accept the proposition that the privacy-sensitive consumer would be more likely to bypass the easier and immediate route (the online opt out) in favor of waiting until she had the opportunity to opt out in a physical location”). There are also many examples outside the Section 5 context in which the failure to demonstrate harm is a bar to recovery, notwithstanding potential technical violations. See, e.g., *Smith et al. v. The Ohio State Univ.*, Case No. 2:15-CV-3030 (S.D. Ohio June 8, 2016) (finding no harm where there was no actual injury from a violation in which plaintiffs alleged that a FCRA disclosure and authorization contained extraneous information in technical violation of FCRA); *Jackson v. Abendroth & Russell, P.C.*, Case No. 4:16-CV-00113-RGE-HCA (S.D. Iowa Sept. 12, 2016) (finding no standing for claim under Fair Debt Collection Practices Act in which plaintiff alleged debt collection letter failed to include informational disclosures required by the Act related to the ability to dispute the debt but where plaintiff never indicated he intended to dispute the debt).

²¹ See, e.g., Dissenting Statement of Commissioner Maureen K. Ohlhausen, *In the Matter of Nomi Technologies, Inc.*, FTC File No. 1323251 (Apr. 23, 2015).

²² Despite references in prior Commission reports that certain geolocation data should be treated as sensitive for purposes of the FTC's voluntary data privacy recommendations, see, e.g., FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change*, Report, 58-59 (2012) (“FTC Privacy Report”), it is not clear that the Commission engaged in an adequately fulsome analysis in the *Goldenshores* case or elsewhere to assess the requisite materiality or harm to find that the company violated the FTC Act for not following the recommendations.



As illustrated by the above examples, the FTC should avoid presuming materiality in deception cases where it appears that consumers were not impacted by the misstatement (*e.g.*, they never read and relied on the statement or were not disadvantaged).

C. The FTC Should Not Enumerate *Per Se* Informational Injuries

Just as the FTC should focus on informational injuries involving concrete, provable harms supported by empirical evidence, it should also avoid presuming informational injury based solely on the nature of the information at issue. The impact from any particular disclosure or use of information is a broad spectrum – in some circumstances, a particular data use or disclosure could be so benign as to register no injury whatsoever, whereas in other circumstances there could be substantial harm to consumers. Therefore, the Commission should reject the notion that any specific disclosure or use of a particular type of information, including information that is conserved “sensitive,” is *per se* harmful or automatically constitutes an informational injury.

Instead, an analytical, empirical, and case-by-case analysis should be used to ascertain the effect of a specific transaction on consumer welfare, taking into account key contextual issues such as consumer expectations and how the information was used.

Moreover, to help ensure that the FTC is focused most effectively in support of its mandate to protect consumers, it is important that the FTC evaluate specific “substantial” and “material” harms on a case-by-case basis rather than presume that they exist.²³ Doing so will help avoid a misalignment between protecting consumers and avoiding unnecessary burdens on innovation and competition.²⁴

D. The FTC Should Not Reduce Benefits to Consumers and Competition Through Overbroad or Novel Informational Injuries

As the FTC seeks to identify and measure informational injuries in the context of its unfairness authority, the benefits to consumers and competition produced by the practices involved must be thoroughly examined.²⁵ Consumers benefit from the rich and diverse array of free, high-quality online content and services; innovation; and economic growth that are all fueled by data. For example, a recent study by Harvard Business School professor John Deighton found that the

²³ *Contra In the Matter of D-Link Corp.*, FTC File No. 1323157 (May 22, 2017).

²⁴ *See* Dissenting Statement of Commissioner Maureen K. Ohlhausen, *In the Matter of Uber, Inc.*, FTC File No. 1523082 (Jan. 19, 2017) ([I]n describing a \$20 million settlement that was “not tied to an estimate of consumer harm,” then-Commissioner Ohlhausen stated that “[c]onsumer protection enforcers ought to ask and answer two basic questions: How, and by how much, were consumers harmed by the alleged violations? Answering these questions helps ensure consumer protection enforcement is calibrated to the consumer injury and therefore protects consumers without deterring beneficial commercial activity.”).

²⁵ *See, e.g.*, Remarks of Commissioner Maureen K. Ohlhausen, Digital Advertising Alliance Summit, Washington, D.C. (June 5, 2013) (“Ohlhausen DAA Remarks”) (“[P]rivacy, like most issues under FTC jurisdiction, must also be viewed through a competition lens if we are to reach the best outcome for consumers. . . . [M]any companies are designing and marketing products with privacy as an important feature. Additional protections for personal information can be a competitive advantage in securing business from privacy-conscious consumers.”), *available at* <https://www.ftc.gov/public-statements/2013/06/remarks-commissioner-maureen-k-ohlhausen>.



advertising-supported Internet contributed 1.121 *trillion* dollars to the U.S. economy and was responsible for 10.4 million jobs — in 2016 alone.²⁶

FTC guidance and enforcement has the power to alter existing market practices, and if not approached carefully, such action will create a ripple effect of unintended, suboptimal results. Creating new theories of harm or applying existing theories too broadly without rigorous analysis risks distorting competition and hindering innovation, especially for the vibrant online ecosystem.²⁷ For example, actions that require opt-in consent disproportionately hurt young and innovative start-ups that are just beginning to grab a foothold in the competitive online world.²⁸ The FTC must take care to avoid such outcomes.

III. The FTC Should Recognize that Consumers are Increasingly Sophisticated When it Comes to Understanding How Data Improves Their Experience Online, and It Should Help Empower Consumers and Businesses Further Through Outreach and Education Efforts.

The Commission seeks comment on how consumers “perceive and evaluate the benefits, costs, and risks” of sharing information.²⁹

The Internet economy depends on user data to function – the personal information or other data that users provide is absolutely essential to creating accounts and using the vibrant – and often free – online services offered today. There are more than 2 billion active monthly Facebook users,³⁰ 173 million daily Snapchat users,³¹ and 90 million U.S. households with an Amazon

²⁶ *The Economic Value of the Advertising-Supported Internet Ecosystem*, study commissioned by the Interactive Advertising Bureau (Mar. 15, 2017), available at <https://www.iab.com/insights/economic-value-advertising-supported-internet-ecosystem/>.

²⁷ See, e.g., 15 U.S.C. § 45(n) (“In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.”); cf. Concurring Statement of Acting Chairman Maureen K. Ohlhausen, *In the Matter of Vizio, Inc.*, FTC File No. 1623024 (Feb. 6, 2017) (noting that Count I alleged granular television viewing activity to be sensitive information the disclosure of which without consent would cause “substantial injury” based on a policy position alone without engaging in examination of whether the practice causes substantial injury in fact).

²⁸ See, e.g., Ohlhausen DAA Remarks (“[N]ew restrictions on the ability of companies to collect or disseminate information could erect barriers to entry in what has historically been a very open sector of the information economy. Instituting new privacy restrictions may preclude new entrants from obtaining valuable consumer information that incumbent competitors already possess. If the need for consumer information were great enough and the rules restrictive enough, competition may be stifled by inefficient industry consolidation and foregone entrepreneurial opportunities.”).

²⁹ Public Notice.

³⁰ *Facebook Reports Second Quarter 2017 Results* (Jul. 26, 2017), available at https://s21.q4cdn.com/399680738/files/doc_financials/2017/Q2/FB-Q2'17-Earnings-Release.pdf.

³¹ Caroline Cakebread, *Snapchat has 173 million users but it’s struggling to grow outside North America* (Aug. 11, 2017), available at <http://www.businessinsider.com/one-chart-shows-snapchats-user-growth-2017-8>.



Prime account.³² As Americans spend more and more of their daily lives online, they are increasingly sophisticated when it comes to understanding how the data they share can provide significant benefits. Consumers are also becoming more sophisticated around the policy and information practices of the Internet economy.

Unfortunately, much of the literature on how and the extent to which consumers understand the privacy and security practices of online products and services has failed to capture this increasing sophistication. Further, much of the literature on online products and services has lacked rigorous empirical analysis. Instead, it tends to focus on individual anecdotes – including self-reported mismatches between expectations and reality – without subjecting research data to robust economic or marketplace analysis.³³ Some research has also failed to consider whether other factors – such as the services involved or the industry to which the company collecting the data belonged – may explain consumers’ privacy choices. Some have noted that had the factors been considered, the studies could have led to strikingly different conclusions.³⁴

Other, more empirical literature paints a decidedly different picture of the typical online consumer as a sophisticated, context-sensitive individual when it comes to privacy matters.³⁵

Research intended to help understand how consumers evaluate the transactions they enter into within the Internet economy should be grounded in robust data to help ensure an accurate portrayal of consumer welfare and decision-making. Given that the Internet economy represents 6% of the U.S. GDP, a high standard must be employed.

As the FTC works to identify and measure informational injuries, it should also take care to respect the informed choices consumers have made and avoid overriding these decisions based

³² Nat Levy, *Prime hits 90M U.S. Households, Representing 63% of Amazon Customers, Study Claims* (Oct. 18, 2017), available at <https://www.geekwire.com/2017/prime-hits-90m-u-s-households-representing-63-amazon-customers-study-claims/>.

³³ *Contra* James Cooper, *Rational Ignorance and the Privacy Paradox*, *Forbes* (Jul. 18, 2016) (discussing the disconnect between consumers’ stated preferences and their “revealed preferences” (tradeoffs they actually make)), available at <https://www.forbes.com/sites/jamescooper1/2016/07/18/rational-ignorance-and-the-privacy-paradox/#68f5ca264ec9>.

³⁴ See, e.g., Kirsten Martin and Helen Nissenbaum, *Measuring Privacy: An Empirical Test Using Content to Expose Confounding Variables*, *COLUM. SCI. & TECH. L. REV.* (Fall 2016), available at <http://www.stlr.org/cite.cgi?volume=18&article=MartinNissenbaum> (stating that individuals’ actions are “finely modulated to contextual variables” and that a more nuanced view may explain away a great deal of what is claimed to be divergence of behavior from stated preference and opinion).

³⁵ See Dan Cvreck, Marek Kumpost, Vashek Matyas & George Danezis, *A Study on the Value of Location Privacy*, Proceedings of the 5th ACM Workshop on Privacy in the Electronic Society (2006). For a full review of this literature, see Alessandro Acquisti *et al.*, *The Economics of Privacy*, *J. ECON. LIT.* at 41 (forthcoming, 2017), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580411. See also Hal R. Variann, Glenn Woroch & Fredrik Wallenburg, *Who Signed Up for the Do Not Call List?* (2004), available at <http://eml.berkeley.edu/~woroch/do-not-call.pdf>; Ivan P. L. Png, *On the Value of Privacy from Telemarketing: Evidence from the “Do Not Call” Registry* (2007), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1000533; Scott Savage & Donald M. Waldman, *The Value of Online Privacy* (2013), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2341311.



on speculative harms and intuition. The fact that consumers are spending increasing amounts of time online and are growing in sophistication when it comes to data practices is a clear sign of a well-functioning market economy that should be encouraged.

The FTC and other stakeholders should help educate individuals further on available privacy tools, privacy practices, and norms. The FTC can also continue to encourage companies to engage in thoughtful data hygiene practices and provide simple, easily understandable privacy notices that are delivered at appropriate points in time, thereby increasing the likelihood that consumers will both receive and comprehend the privacy impact of an exchange.³⁶

IV. The FTC Should Continue Encouraging Organizations to Conduct Appropriate Privacy Risk Analyses and Adopt Other Best Practices to Understand Better the Risks and Potential Injuries from Their Data Activities.

In the Public Notice, the Commission seeks comment on how businesses evaluate the risks of collecting and using information.³⁷ As discussed below, businesses today use a variety of tools and approaches to help assess potential risks. The FTC should continue encouraging companies to engage in privacy risk analyses and adopt other best practices, but it should avoid unnecessarily hampering or limiting innovation and competition.³⁸

In recent years, there has been a surge in the number and prominence of privacy professionals charged with safeguarding corporate compliance with privacy laws and guiding best practices.³⁹

³⁶ Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: A JOURNAL OF LAW & POLICY FOR THE INFORMATION SOCIETY 543 (2008) (estimated cost of reading privacy policies is \$3,534 per year); Patrick Gage Kelley *et al.*, *A “Nutrition Label” for Privacy* (2009), at <https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf>; Patrick Gage Kelley *et al.*, *Standardizing Privacy Notices: An Online Study of the Nutritional Labeling Approach*, CyLab (2010), at <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1002&context=cylab>; Omri Ben-Shahar & Adam S. Chilton, *Simplification of Privacy Disclosures: An Experimental Test*, (Apr. 2016), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711474.

³⁷ Public Notice.

³⁸ Such a position would be consistent with FTC privacy and data security enforcement actions, which often describe comprehensive privacy and data security programs as including assessment of the material internal and external risks. *See, e.g., In the Matter of EPN, Inc.*, FTC File No. 1123143 (Oct. 3, 2012); *In the Matter of James B. Nutter & Co.*, FTC File No. 0723108 (June 12, 2009); *In the Matter of Reed Elsevier, Inc. and Seisint, Inc.*, FTC File No. 0523094 (July 29, 2008); *In the Matter of Lookout Services, Inc.*, FTC File No. 1023076 (June 15, 2011); *In the Matter of Premier Capital Lending*, FTC File No. 0723004 (Dec. 10, 2008). It would also be consistent with the FTC’s Internet of Things Staff Report, among other guidance. *See, e.g., FED. TRADE COMM’N*, *Internet of Things: Privacy & Security in a Connected World*, Staff Report (2015) (“companies should consider . . . conducting a privacy or security risk assessment”).

³⁹ *See, e.g., 2017 IAPP-OneTrust Privacy Professionals Salary Survey – Executive Summary* (stating that “[t]his year’s survey confirms that there is robust demand for privacy pros” and that “nearly nine of 10 privacy professionals came to privacy from another job”), available at <https://iapp.org/resources/article/2017-iapp-privacy-professionals-salary-survey-executive-summary/>; IAPP-EY Annual Privacy Governance Report 2016, Introduction (stating that “privacy is now a board-level issue for 70 percent of all organizations” and that 57 percent of respondents reported a likely



A number of companies across industry sectors are also allocating additional financial resources to address evolving privacy and security challenges.⁴⁰ Moreover, consistent with the Commission’s recommendations, many companies have also started to adopt “Privacy by Design” and “Security by Design” processes into their business operations,⁴¹ along with other tools to protect against privacy and security risks.

Going forward, the FTC should continue encouraging organizations to conduct appropriate privacy risk analyses and adopt other best practices. A privacy risk analysis can be an important tool in helping to protect against informational harms.⁴² It can take many forms, and instead of prescribing a specific method by which risk analyses must be carried out, the FTC should support a best practice framework for data privacy risk assessments that encourages companies to adopt the form that fits best within their industry and existing business structure. FTC guidance could, for example, provide that privacy risk analyses should involve a careful consideration of data practices. Guidance could also present factors that companies should consider incorporating into their analyses, such as:

- The nature of the data (including whether it is personal or sensitive);
- The processing operations performed on the data;
- To whom the data will be disclosed;
- The extent to which the entity will have control over the data and its processing; and
- How the data will be kept secure.

By facilitating a best practice approach, the FTC can encourage the careful consideration of data privacy risks while allowing companies the flexibility to incorporate privacy assessments where appropriate in their particular business structures.

increase in budgets for the next year), *available at* https://iapp.org/media/pdf/resource_center/IAPP-2016-GOVERNANCE-SURVEY-FINAL2.pdf.

⁴⁰ See, e.g., Fortune, *Here’s How Much Businesses Worldwide Will Spend on Cybersecurity by 2020* (Oct. 12, 2016) (stating that the International Data Corporation expects that businesses will spend \$101.6 billion on cybersecurity by 2020), *available at* <http://fortune.com/2016/10/12/cybersecurity-global-spending/>.

⁴¹ See, e.g., FED. TRADE COMM’N, *Careful Connections: Building Security in the Internet of Things*, 1 (Jan. 2015) (encouraging companies to implement security by design and stating that “[r]ather than grafting security on as an afterthought, build it into your products or services at the outset of your planning process”), *available at* <https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf>; FED. TRADE COMM’N, *Protecting Consumer Privacy in an Era of Rapid Change*, Report, 22 (2012) (discussing support for privacy by design), *available at* <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

⁴² For this reason, certain U.S. federal and state laws and regulations already require risk assessments. See, e.g., the Health Insurance Portability and Accountability Act, 45 C.F.R. § 164; E-Government Act of 2002, 44 U.S.C. § 101; New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies, 23 N.Y.C.R.R. Part 500.



V. Conclusion

The Commission is to be commended for its appreciation of the vital nature of information flows to the Internet economy and for seeking input on how best to identify and assess informational injuries in today's connected world. IA appreciates the opportunity to provide input on this important issue for the Internet economy, and we look forward to continued dialogue with the FTC and other stakeholders.

Respectfully submitted,

Michael Beckerman
President and CEO
Internet Association
1333 H Street, NW, 12th Floor West
Washington, D.C. 20005

Mark W. Brennan
Katherine Gasztonyi
Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, D.C. 20004
Counsel for Internet Association