ConsumersUnion®

POLICY & ACTION FROM CONSUMER REPORTS

January 26, 2018

Federal Trade Commission
Office of the Secretary
400 7th Street SW, 5th Floor
Suite 5610 (Annex A)
Washington, DC 20024

Re: Informational Injury Workshop P175413

Dear Sir or Madam:

Consumers Union, the advocacy division of Consumer Reports,[1] is an expert, independent, nonprofit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. We write to comment on the questions addressed in the December 12, 2017 workshop on informational injury hosted by the Federal Trade Commission (FTC or Commission).

Consumers' interests in their personal information are contextual and case- and individual-specific. As a result, it is challenging—and indeed inappropriate—for regulators to prescriptively identify and classify every potential value a person places on their data. Section 5 of the Federal Trade Commission Act was conspicuously crafted to apply to a broad and evolving array of consumer protection concerns.[2] For these reasons, we encourage an expansive definition of what could constitute an informational injury.

However, it is important to stress that under Section 5, "injury" is not a requisite element in deception cases. In an era of declining corporate accountability,[3] and given its significant

[1] Consumer Reports is the world's largest independent product-testing organization. It conducts its policy and mobilization work in the areas of privacy, telecommunications, financial services, food and product safety, health care, and other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million subscribers to its magazine, website, and other publications.

[2] Petitioner's brief, *Federal Trade Commission v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3rd Cir. 2015) ("Although Congress did not foresee modern electronic commerce when it enacted the relevant provisions of the FTC Act, it understood that threats to consumer welfare would evolve rapidly as the worlds of business and technology. It thus wrote section 5 in open-ended terms, granting the FTC broad authority to pursue unfair practices across a broad range of economic contexts.").

[3] Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 364-71 (2015), *available at* http://harvardlpr.com/wp-content/uploads/2015/07/9.2_3_Brookman.pdf.

existing legal and resource limitations, the Commission should not further hamstring itself in its mission to protect consumer interests. As such, we oppose any policy guidance to limit agency action in deception cases to instances where the Commission makes a subjective evaluation of consumer injury. Indeed, in deception cases, the deception *is* the injury because it distorts information in the marketplace, which hurts consumers and legitimate business alike.

And while *materiality* is a requisite element in deception cases, the Commission should not deviate from its long-standing policy that affirmative statements by companies are presumed to be material. Indeed, when a company chooses to describe a promote its practices in a certain manner, it can be presumed that the company has concluded that consumers find that information material to their decision-making.[4]

We recognize that deception can be tricky in the privacy realm because many consumers do not read privacy policies, which are often buried on websites, dozens of pages long, and/or written in legalese that is difficult to understand. In addition, most consumers would not even know to look for the privacy policies of the myriad companies that collection their information behind the scenes. However, companies should still be responsible for any claims they choose to make about their data practices. Further, the audience for privacy policies includes, not just consumers, but also policymakers, enforcement agencies, consumer groups, members of the media, academics, security and privacy tools, and nonprofits—all of whom monitor privacy policies for policy, consumer protection, and even investment purposes. Companies should not be able to reap political, public relations, or financial benefits from deceptive statements about privacy without being accountable to those most affected: consumers.

What are the qualitatively different types of injuries from privacy and data security incidents? What are some real life examples of these types of information injury to consumers and to businesses?

As noted above, injury is not currently an element of deception and for good reason—the deception itself injures consumers and the marketplace and companies should bear responsibility for it.

Putting that aside, we encourage the Commission to employ an expansive definition of what constitutes an informational injury to consumers, and we agree with the five types of consumer informational injury that Acting Chairman Maureen Ohlhausen identified in her September 19th, 2017 speech announcing the informational injury workshop: deception injury or subverting consumer choice, financial injury, health or safety injury, unwarranted intrusion injury, and

[4] *FTC Policy Statement on Unfairness*, FED. TRADE COMM'N (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

reputational injury.[5] However, we disagree with the Acting Chairman's views in certain respects. First, the suggestion that the FTC must make its own assessment of injury prior to bringing a "subverting consumer choice" case. Instead, we suggest that the FTC rely on whether or not companies contravened their affirmative statements in order to assess whether the consumer's preferences were violated.

Additionally, we suggest that the FTC adopt an expansive view of what constitutes an "unwarranted intrusion" such that it takes into account sensitive information and invasive intrusions on a consumer's privacy. For example, in the *Vizio* case, second-by-second information about the video displayed on a consumer's TV was collected and then combined with specific demographic information, such as sex, age, income, marital status, household size, education level, home ownership, and household value.[6] In robocall cases, machine-generated telephone solicitations are invading consumer's homes and privacy.[7] And in a series of cases involving *Aaron's* rent-to-own computers, the companies enabled spyware on the rentals that monitored computers in their homes.[8] These types of practices are all harmful and highly invasive, and should be viewed as actionable injury under the FTC Act.

Any efforts to narrow the application of the FTC Act would be unwise in an era when it is harder and harder to discern companies' privacy practices and hold them accountable, and when the types of privacy harms in the marketplace have rapidly proliferated. In this regard, Consumers Union offers two ideas to strengthen privacy accountability in this country. First, consumers need better information and tools to evaluate and compare privacy choices. To that end, Consumer Reports and its partners have developed The Digital Standard,[9] an open standard for testing products for privacy and security in order to help consumers make informed decisions in the marketplace. The testing includes assessments of a company's stated privacy practices in both the user interfaces and in their privacy policies. This effort depends on the transparency that

---

[5] Maureen K. Ohlhausen, *Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases*, FED. TRADE COMM'N (Sept. 19, 2017), https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf.

[6] *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent*, FED. TRADE COMM'N (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

[7] Maureen Mahoney, *Fed Up with Robocalls? Here's What You Can Do Right Now*, CONSUMERS UNION (July 21, 2017), http://consumersunion.org/campaign-updates/fed-up-with-robocalls-heres-what-you-can-do-right-now/.

[8] *See e.g., Aaron's*, FTC File No. 122-3264 (2013), https://www.ftc.gov/enforcement/cases-proceedings/122-3256/aarons-inc-matter.

[9] The Digital Standard (theDigitalStandard.org) was launched on March 6th, 2017 and is the result of a collaboration with our cybersecurity partners, Disconnect, Ranking Digital Rights, and the Cyber Independent Testing Lab. The Standard is designed to hold companies accountable and equip Consumer Reports and other organizations to test and rate products for how responsibly they handle our private data. This is a collaborative and open source effort. The Standard is designed to empower consumers to make informed choices about the connected products, apps, and services consumers use everyday.

privacy policies and user interfaces provide consumers. In addition, one of the important criteria under our Digital Standard[10] is that the user can see and control everything the company knows about the individual. In order for a company's data practices to be responsible under the Standard, the company must enable the consumer to be able to know to know what user information the company is collecting, the company only requests and collects information that is needed to make the product or service work correctly, and the company explicitly discloses every way in which it uses the individual's data.[11]

Second, the unfairness statement,[12] which was published in 1980, needs to be updated and modernized to reflect the broader harms that consumers face. For instance, under "Consumer Injury" the unfairness statement states: "In most cases a substantial injury involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defenses arising from the transaction."[13] This statement reflects an undue focus on monetary harms and does not reflect the kinds of harms that proliferate and are at issue in many FTC cases, like *Aaron's*, *Vizio*, and others. The unfairness statement must be updated to reflect the realities of a post-internet, Internet of Things, Artificial Intelligence, and otherwise highly connected world.

How do businesses evaluate the benefits, costs, and risks of collecting and using information in light of potential injuries? How do they make tradeoffs? How do they assess the risks of different kinds of data breach? What market and legal incentives do they face, and how do these incentives affect their decisions?

Businesses are run by humans, and humans exhibit a natural human tendency to overestimate a small chance of something good happening and to underestimate the chances of something bad happening.[14] This is a core tenet of behavioral economics, and explains why people play the lottery despite the odds and decreasing marginal value of money, or do not buckle their seat belts despite the low costs and tremendous risk. Translated to data privacy, companies will tend to undervalue data security, and undervalue data minimization as well, discounting the likelihood of a security event, but overly optimistic about the potential for found wealth in data troves. Therefore, consumer protections framework should reflect the reality of human nature, and align

---

[10] *The Standard*, THE DIGITAL STANDARD, https://www.thedigitalstandard.org/the-standard.
[11] *Id*.
[12] *FTC Policy Statement on Unfairness*, FED. TRADE COMM'N (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
[13] *Id*.
[14] Klaus Mathis & Ariel David Steffen, *From Rational Choice to Behavioural Economics*, UNIV. OF LUCERNE (2015) https://www.unilu.ch/fileadmin/fakultaeten/rf/mathis/Dok/1_Mathis_Steffen_From_Rational_Choice_to_Behavioural_Economics.pdf.

incentives to account for irrational tendencies. Company tendencies to undervalue security are exacerbated by weak data security standards that do not fully require them to bear the societal cost of data breaches; the FTC lacks the authority to leverage penalties in most cases and it is difficult to tie identity theft to individual data breaches, which means that companies are insufficiently incentivised from implementing reasonable data security.

It is clear from the neverending spate of data breach incidents—many of which were preventable by basic security hygiene[15]—that companies are not sufficiently protecting the data under their control. And the failure to sufficiently protect the privacy and security of users injures consumers. This torrent of data breaches is concrete evidence that companies are not sufficiently internalizing risks of data exposure (even before the announcement of the Equifax data breach, a Pew poll in January of 2017 found that nearly two-thirds of Americans have experienced some sort of data theft[16]). And the harm from these data breaches are not only pervasive[17] but also expensive (in 2016 alone, the Department of Justice found that the estimated cost of identity theft amounted to $15.4 billion).[18]

There is also a clear divide between consumer-facing companies and non-consumer-facing ones and how they respond to public pressure regarding the collection and security of their data. Whether or not the company is consumer facing is an indication of whether or not reputational injury is a deterrent (albeit, often an insufficient one) for failing to adequately protect consumer data. For instance, in 2016 the rideshare app Uber released an update that allowed the app to track users' locations for at least five minutes after their Uber ride had actually ended (if not constantly).[19] After sustained public outcry, the company finally eliminated the feature in an

---

[15] *90% of Data Breaches are Avoidable*, Online Trust Alliance (Feb. 2, 2012), https://www.cybersecurityintelligence.com/blog/90-of-data-breaches-are-avoidable-1003.html ("Ninety one percent of data breaches that occurred from January to August of 2015 could have easily been prevented using simple and well-established security practices, such as applying software patches to a server, encrypting data or ensuring employees do not lose their laptops…"); *see, e.g.*, Meghan Kloth Rohlf, *Yahoo Data Breaches: A Lesson in What Not to Do*, Lexology (March 2, 2017), https://www.lexology.com/library/detail.aspx?g=cdf1c89f-75bf-4524-8e3e-6425529a7349 ("...in 2013, when the first data breach occurred, Yahoo was still using a discredited technology for data encryption known as MD5. The weaknesses of MD5 had been known by security experts and hackers for more than a decade and public warnings had been issued advising that MD5 was "unsuitable for future use.""); Lily Hay Newman, *Equifax Officially Has No Excuse*, Wired (Sept. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse/ ("...Equifax has confirmed that attackers entered its system in mid-May through a web-application vulnerability that had a patch available in March").

[16] Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, Pew Research Ctr. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

[17] 86% of identity theft victims experienced the fraudulent use of existing account information. Erika Harrell, *Victims of Identity Theft*, Bureau of Justice Statistics (Sept. 27, 2015), https://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408.

[18] *Id*.

[19] Andrew J. Hawkins, *Uber Wants to Track Your Location Vene When Youre Not Using the App*, The Verge (Nov. 30, 2016), https://www.theverge.com/2016/11/30/13763714/uber-location-data-tracking-app-privacy-ios-android.

update in mid-2017.[20] In comparison, a company like Equifax is mostly non-consumer-facing and thus has little incentive to respond to the public and their concerns about their private data being secure. In the fall of 2017, the company announced that the personal information belonging to over 145 million Americans had been breached, including information such a names, addresses, Social Security numbers, dates of birth, and credit card and credit dispute information.[21] In the former case, the company expanded its reach to collect more and highly personal location data about their users and later changed their practices due to pushback from the public. By contrast, in the latter instance, a company that controls highly personal information about millions of Americans but does not answer to these individuals failed to protect their information. In response to strong pressure from Consumers Union and its activists, [22] as well as partner organizations, the credit reporting giant did make *some* remediation following the breach.[23] However, consumers still lack control over the security of their highly personal information that companies like Equifax and others control and use.

How do consumers perceive and evaluate the benefits, costs, and risks of sharing information in light of potential injuries? What obstacles do they face in conducting such an evaluation? How do they evaluate tradeoffs?

Although consumers have clear preferences about what data is collected about them and how it is used, they are unable to effectively evaluate the costs and benefits of sharing their personal data, due in part to the opacity of data flows which further hampers an individual's ability to meaningfully evaluate privacy risks and potential benefits.[24] In many cases, companies acquire information about consumers from an intermediary, such as the marketing technology and services company Acxiom, and use this information without the individual's knowledge or control. Compounding these issues, it is hard for consumers to evaluate the future risk to their privacy against immediate conveniences (and possess the same cognitive biases discussed in the previous section).

---

[20] Dustin Volz, *Uber to End Post-Trip Tracking of Riders as Part of Privacy Push*, REUTERS (Aug. 29, 2017), https://www.reuters.com/article/us-uber-privacy/uber-to-end-post-trip-tracking-of-riders-as-part-of-privacy-push-id USKCN1B90EN.

[21] Winnie Sum, *2.5 Million More Americans Added to the Equifax Security Leak, What to do Now*, FORBES (Oct. 2, 2017), https://www.forbes.com/sites/winniesun/2017/10/02/what-you-should-do-now-after-the-equifax-security-leak/#5a1e 4de42123.

[22] *Equifax Security Breach Petition*, CONSUMER REPORTS, https://action.consumerreports.org/equifax_20171010_petition.

[23] Jeff Blyskal, *Is Equifax's Free ID Protection Service Good Enough?*, CONSUMER REPORTS (Oct. 6, 2017), https://www.consumerreports.org/identity-theft/is-equifaxs-free-id-protection-service-good-enough/.

[24] Aaron Alva, *Cross-Device Tracking: Measurement and Disclosures*, FED. TRADE COMM'N (Jan. 5, 2017), https://www.ftc.gov/news-events/blogs/techftc/2017/01/cross-device-tracking-measurement-disclosures; and see Kate Kaye, *FTC's Cross-Device Study Reveals Opacity of Data-Sharing Practices*, ADAGE (Jan. 6, 2017), http://adage.com/article/privacy-and-regulation/ftc-s-cross-device-study-reveals-opacity-data-practices/307392/.

Consumers have preferences about their data and are very concerned about their privacy. For example, Consumer Reports' survey found that 92% of Americans think companies should get permission before sharing or selling users' online data and that 70% of Americans lack confidence that their personal information is private and secure.[25] In addition, 88% of individuals say it is important that they not have someone watch or listen to them without their permission.[26] A Mozilla study found that a third of people feel like they have no control of their information online;[27] and, a study from Pew noted that respondents "regularly expressed anger about the barrage of unsolicited emails, phone calls, customized ads, or other contacts that inevitably arises when they elect to share some information about themselves."[28] The majority of consumers (74%) find it is "very important" to be in control of who can get information about them.[29] In addition, 67% of consumers highly value not having "someone watch you or listen to you without your permission" and 65% of consumers think it is "very important" to control what information is collected about them.[30] Indeed, this is not a new sentiment for consumers: a Pew research poll in 2014 found that 91% of adults "'agree' or 'strongly agree' that consumers have lost control over how personal information is collected and used by companies."[31] Consumers desire the ability to limit data collection, detrimental uses, and unnecessary retention and sharing, but lack the ability to easily and efficiently exercise those preferences.

These concerns have a tangible effect on how consumers conduct themselves online. The National Telecommunications & Information Administration's analysis of recent data shows that Americans are increasingly concerned about online security and privacy at a time when data breaches, cybersecurity incidents, and controversies over the privacy of online services have become more prominent.[32] These concerns are prompting some Americans to limit their online

---

[25] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[26] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security, and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[27] *Hackers, Trackers, and Snoops: Our Privacy Survey Results*, MOZILLA (Mar. 9, 2017), https://medium.com/mozilla-internet-citizen/hackers-trackers-and-snoops-our-privacy-survey-results-1bfa0a728bd5.

[28] Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, PEW RESEARCH CTR. (Jan. 14, 2016), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

[29] *See Americans' Attitudes*, supra note 26.

[30] *Id*.

[31] Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

[32] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NAT'L TELECOM. & INFO. ADMIN. (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

activity.[33]

Consumers are increasingly interested in protecting their privacy and the security of their data, but it is time consuming and hard for consumers to effectively manage the amount of data that is collected about them. The public depends on intermediaries like the Commission or Consumers Union to evaluate the products that are available to consumers and help them choose the best company or product to interact with. In looking for ways to protect the privacy and security of their data, consumers are increasingly looking for privacy protective products and tools. For instance, 11% of the global population uses an ad blocker while online and the usage of ad blockers grew by 30% in 2016 alone.[34]

Just as the harm a consumer faces from an informational injury is contextual, their decisions about how and where to share their data also depends on the context.[35] In order to help the consumer decide what tools are available to address their most concerning privacy and data security issues, University of Toronto's Citizen Lab launched the Security Planner,[36] an easy to use platform that tailors recommendations based on an individual's digital habits and the technology they use in order to help people be more safe online that is funded in part by Consumer Reports. Since the site's launch in mid-December, the site had over 49,000 users come to the site. Consumers clearly want and need ways to secure their data online, and look to intermediaries for recommendations on the best methods.

Thank you for the opportunity to comment on the December 12, 2017 workshop on informational injury. If you have any questions, please feel free to contact us at 202.462.6262.

Sincerely,

Katie McInnis
Policy Counsel
Consumers Union
1101 17th Street NW, Suite 500
Washington, DC 20036

---

[33] *Id*.
[34] Matthew Cortland, *2017 Adblock Report*, PAGEFAIR (Feb. 1, 2017), https://pagefair.com/blog/2017/adblockreport/.
[35] Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, PEW RESEARCH CTR. (Jan. 14, 2016), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/ ("Many Americans are in an "it depends" frame of mind when they think about disclosing personal information or keeping it private when considering different scenarios.")
[36] *Security Planner*, CITIZEN LAB, https://securityplanner.org/#/.