NetChoice *Promoting Convenience, Choice, and Commerce on the Net*

Carl Szabo, Vice President and General Counsel
NetChoice
1401 K St NW, Suite 502
Washington, DC 20005
202-420-7498
www.netchoice.org

October 27, 2017
SUBMITTED ELECTRONICALLY
Federal Trade Commission

NetChoice Public Comments to FTC Request for Comments on the FTC Workshop on Informational Injury

NetChoice respectfully submits the following comments regarding the Federal Trade Commission's ("FTC") request for comments on the Informational Injury.[1]

NetChoice is a trade association of leading e-commerce and online companies, plus thousands of small businesses that rely on e-commerce. We work to promote the integrity and availability of the global internet and are significantly engaged in privacy issues in the states, in Washington, and in international internet governance organizations.

We caution the Commission in its analysis of "informational injury" against creating causes of action for theoretical injuries. Some commenters will attempt to infer theoretical injuries as a way to extract quick pay-days from businesses or other citizens – concluding that injury to one's information gives standing to a civil action. Such a movement from showing of actual harms to an assertion of theoretical harms could have immense and deleterious consequences.

Moreover, we find that when a person's information is abused, ample existing laws already provide remedy.

In the following we discuss the dangers of treating "information injuries" alone as actionable events. We show that treating these injuries as actionable will result in real harm for consumers and businesses. We outline a proper framework for FTC analysis of informational injuries. Finally, without a showing that existing laws fail to address any real harms, we show the risk of pursuing this analysis does not offset the potential consequences to our constitutional right of due process.

As stated by Acting Chair Ohlhausen:

> "Before seeking new privacy legislation, it is important to identify a gap in statutory authority or to identify a case of substantial consumer harm that we'd like to address, but can't, with our existing authority, especially given the array of financial, medical, and health

[1] FTC Request for Comments - *FTC to Host Workshop on Informational Injury* (#721).

and safety harms already reachable under our current FTC authority or other laws. Otherwise, it is difficult to tell whether the additional protections are necessary or will, on balance, make consumers better off because information sharing has benefits for consumers such as reducing online fraud, improving products and services, and increasing competition in the market overall."[2]

Establishing Causes of Action For Theoretical Harms Creates a Regime Of Guilty Until Proven Innocent

Our country is founded, in part, on the notion that a defendant is presumed innocent until proven guilty.[3] However, recent efforts to inject theoretical harms as causes of action into civil and administrative proceedings represent a reversal of this cherished notion – shifting the burden of proof from the plaintiff to the defendant.

Moreover, it moves away from the Constitutional requirements for standing for lawsuits.[4] The requirements for Article III standing are:

> "To establish Article III standing, a plaintiff must demonstrate '(1) *an injury-in-fact*, (2) a sufficient causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision.'"[5]

Moreover, in *Spokeo v Robins*,[6] the US Supreme Court further extrapolated that:

> "Particularization is necessary to establish injury in fact, but it is not sufficient. An injury in fact must also be 'concrete' .... A 'concrete' injury must be '*de facto*'; that is, it must actually exist."[7]

The Supreme Court concluded by saying: "It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm"[8] showing the reticence of acknowledging harm in theory vs harm in fact.

Now this isn't to say that intangible harms aren't actionable, and in fact, the US Supreme Court in *Spokeo* says just as much.[9] But just like tangible harms, the plaintiff must show *actual harm*.

At a recent event, a representative from Public Knowledge complained that, "it is difficult to quantify the harm." But the bar of difficulty in bringing a civil case is essential to the operation of the US court system.

---

[2] FTC Commissioner Maureen K. Ohlhausen Speech Before the Hudson Institute, *The Government's Role in Privacy: Getting it Right*, (October 16, 2012).
[3] *See e.g. Coffin v. United States* 156 U.S. 432 (1895).
[4] *See, e.g.* US Const. Art III § 2 Cl1. "The Judicial Power shall extend to all Cases . . .[and] to Controversies . . ."
[5] *Finkelman v. National Football League*, 810 F.3d 187 (3rd Cir. 2016) (emphasis added).
[6] *Spokeo, Inc. v. Robins*, 578 U.S. ___ (2016).
[7] *Id.*
[8] *Id.*
[9] "Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete." (*Id.*).

As stated above, the requirements for standing ensure that cases have merit. Ensuring plaintiffs must demonstrate quantifiable harm protects defendants too; plaintiffs cannot bring forth harassment via fact deficient cases.

To shift the burden of proof from the plaintiff to the defendant, and force the defendant to prove a negative (that there is no possibility of harm) violates our sense of justice – a shift that would occur under a regime where assertion of theoretical information harms alone are causes of action.

We ask that FTC avoids the pitfalls of these violations of justice. If there is a consideration of intangible harms, it should only address real harms not theoretical ones.

Discouraging Innovation

There are several ways that "informational injury" can occur, however, for purposes of this section, we will focus on two: errors in voluntary disclosure by a business and unauthorized access. These two scenarios play out in the realm of person searches such as *Spokeo* and data breaches.

Errors in Voluntary Disclosure by a Business

In the instance of *Spokeo*,[10] the plaintiff, Thomas Robins, complained that his profile on Spokeo incorrectly stated he is "married, has children, is in his 50's, has a job, is relatively affluent, and holds a graduate degree." Mr. Robins then sought recompense for the error under the Fair Credit Reporting Act.[11]

Had the US Supreme Court found that Mr. Robins's potential embarrassment by Spokeo's mistake constituted injury in fact, we might see a drop-off of any such aggregation service – as a mistake means potentially millions in liability.

Treating Unauthorized Access to Business Records as De Facto Harm to Consumers

As much as we all want to blame a business that suffered a data breach, the business is a victim. Setting aside the question the courts are currently analyzing, whether failure to properly secure data can warrant an action under Section 5 of FTC Act,[12] we look at the economic impact of holding a business liable for any "informational injury" that might result.

Experts say that a business's data breach is not if but when.[13] This means that nearly every business that has data may suffer a data breach at some point. Moreover, most data breaches are a result of hacking or external assaults on a system.[14]

Some advocate that if a breach occurs, regardless of whether the stolen data was abused for an actual harm to the user of the business – informational injury – the business should be liable to the user. This creates distortions in the marketplace and doubly punishes businesses that are also victims of a data breach.

---

[10] *Id.*
[11] *Id.*
[12] 15 USC § 41, *et al*.
[13] Stegmaier and Luehr, *Cyber Security: Not if, but when…* (June 2015).
[14] *Id.*

It twice punishes businesses for being victims of a data breach. First, the business first suffers loss of user trust and reputational harm – sometimes irreparable damage. Second, it imposes incredible ongoing liability for the victimized business as it is subject to lawsuits from every user whose data was stolen with theoretically high damages for each suit.

This creates incredible disincentives for innovation. It discourages businesses and researchers from seeking new innovative ways to deliver new services to users and/or lower costs to users.

Some commenters will likely say that such strict penalties will force businesses to better protect user data. But this is a false assumption. It assumes that existing forces don't already encourage protection. But today, when a business suffers a data breach, it suffers other consequences: loss of user trust, reputational harm, and financial harm for those users whose data was abused. We should not expect significant increases in security of personal information with increased punitive liability.

Outline for an FTC "Informational Injury" Harms Study

We understand that the FTC has yet to complete analysis and identification of real world harms of "informational injury." When it does, such a study should avoid inclusion of theoretical harms and anecdotes to drive the conversation, otherwise such a report does a disservice to the FTC and consumers.

Below, we outline a balanced way to analyze "informational injuries."

Outline for a Study of Actual "Informational Injuries"

> *[T]he injury must be substantial. The Commission is not concerned with trivial or merely speculative harms.* [15]

At the core of the FTC is its ability to bring an action under Section 5 of the FTC Act[16] against unfair trade practices. The unfairness arm requires a showing of harm – something the FTC has extensive history in identifying. As noted below, the FTC has yet to engage in a comprehensive study of actual harms from informational injuries. This is a challenge for the FTC as real harms may not exist. However, given the FTC's extensive experience with its unfairness research, the FTC is well equipped to take on this challenge.

A. Start from a neutral base and not a predisposition to finding harms.

To maintain confidence in the results, the FTC should operate as an impartial fact finder and not a policy officer looking for crimes. If the FTC starts from the position that harms are occurring or there are problems to find, the results of the study will skew in that direction. Moreover, even if the FTC maintains its impartiality, a predisposition or hypothesis towards harms will cloud public opinions of the results.

B. The FTC should identify real world informational injuries identified by consumers.

> *In most cases a substantial injury involves monetary harm … [and U]nwarranted health and safety risks may also support a finding of unfairness.*[17]

---

[15] *Id.*
[16] 15 USC § 41, *et al.*
[17] *Id.*

Rather than seeking theoretical informational injuries to consumers, the FTC should analyze informational injuries that consumers already identify. This helps maintain impartiality and efficiency of FTC resources. After all, who is better to understand the harm to the consumer than the consumer reporting it?

One possible starting point is the FTC's consumer complaint center. Last year the complaint center received more than 3 million complaints.[18] The FTC can analyze this list and see if any are as a result of informational injuries. Moreover, the FTC can conduct surveys, conversations with consumers, analysis of complaint letters, and town hall discussions.

C. Separate actual informational injuries from privacy informational injuries

> *"Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair."*[19]

To maintain credibility and provide ability for action, this study should identify actual informational injuries and not privacy informational injuries. To identify and act upon firm data, the FTC should limit the scope of this study to actual informational injuries to consumers. These actual informational injuries can include financial, employment, and physical harms.

If these harms exist, the FTC can then begin its harms-benefits analysis.

Beware Exaggerating misuses of information

The FTC has a history of convening workshops designed for thoughtful discussion of issues. However, as we saw at the Big Data Workshop, there are discussions of speculative harms – combining them with charged words that inspire apprehension and opposition to the growth of information.

We ask that the FTC be mindful that the Informational Injuries Workshop avoids such a devolution. The workshop should avoid included charged words like, "discrimination," "unethical" and "illegal" to this describe possible harms.

Of course, if any of the theoretical activities discussed are illegal, the FTC, Department of Justice, and other agencies can already take action. And if they are illegal, NetChoice supports law enforcement engagement.

However, talking in hypotheticals injects groundless and unscientific rhetoric into what should otherwise be a calm rational discussion.

Existing Laws Already Address Potential Harms from Informational Injuries

As discussed above, the FTC already enjoys enforcement authority under Section 5 should it identify uses of big data that are unfair. Likewise, dozens of other federal laws can address the hypothetical harms cited during the workshop: Health Insurance Portability and Accountability

---

[18] "Between January and December 2016, the CSN received more than 3 million consumer complaints, which the FTC has sorted into 30 complaint categories." FTC Consumer Sentinel Network Data Book, Feb. 2017, p.2

[19] FTC Policy Statement on Unfairness, Dec. 17, 1980, *available at* http://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness

Act (HIPAA),[20] Fair Credit Reporting Act (FCRA)[21], and Equal Employment Act (EEA)[22], just to name a few.

We ask that if FTC identifies harms not offset by benefits, the FTC engage in analysis to identify if existing laws already address the harms. For example, if information is used to harm employment, the FTC should research existing employment discrimination and protection laws and identify if gaps exist. The same is true for credit scores and racially based discrimination. If gaps are found, the FTC should look at different ways to fill the gaps, some of which may, but need not necessarily include, legislation.

Until this analysis occurs, the FTC should avoid calling for legislation – especially when actual harms have not yet been identified and balanced against benefits.

Before creating new rules and regulations, we ask the FTC to follow the recommendation of Acting Chair Ohlhausen to see if existing rules accomplish the objectives the FTC seeks:

> "Before seeking new privacy legislation, it is important to identify a gap in statutory authority or to identify a case of substantial consumer harm that we'd like to address, but can't, with our existing authority, especially given the array of financial, medical, and health and safety harms already reachable under our current FTC authority or other laws. Otherwise, it is difficult to tell whether the additional protections are necessary or will, on balance, make consumers better off because information sharing has benefits for consumers such as reducing online fraud, improving products and services, and increasing competition in the market overall."[23]

Role for Government

The role for government should be in areas where users and business cannot act alone, including law enforcement, international data flows, and pre-empting a patchwork of state laws conflicting with federal interests. Government should use its powers to pursue online fraud and criminal misuse of data, not to create rules that narrowly prescribe what and how data should be used.

Overall, we support the notion that companies and customers – not governments – must take the lead on data privacy. Companies need to pursue innovation without asking for permission from government agencies. And consumers must understand the decisions they make, but they must be allowed to make those decisions.

We offer this conceptual view of an industry self-regulatory framework that dynamically adapts to new technologies and services, encourages participation, and enhances compliance.

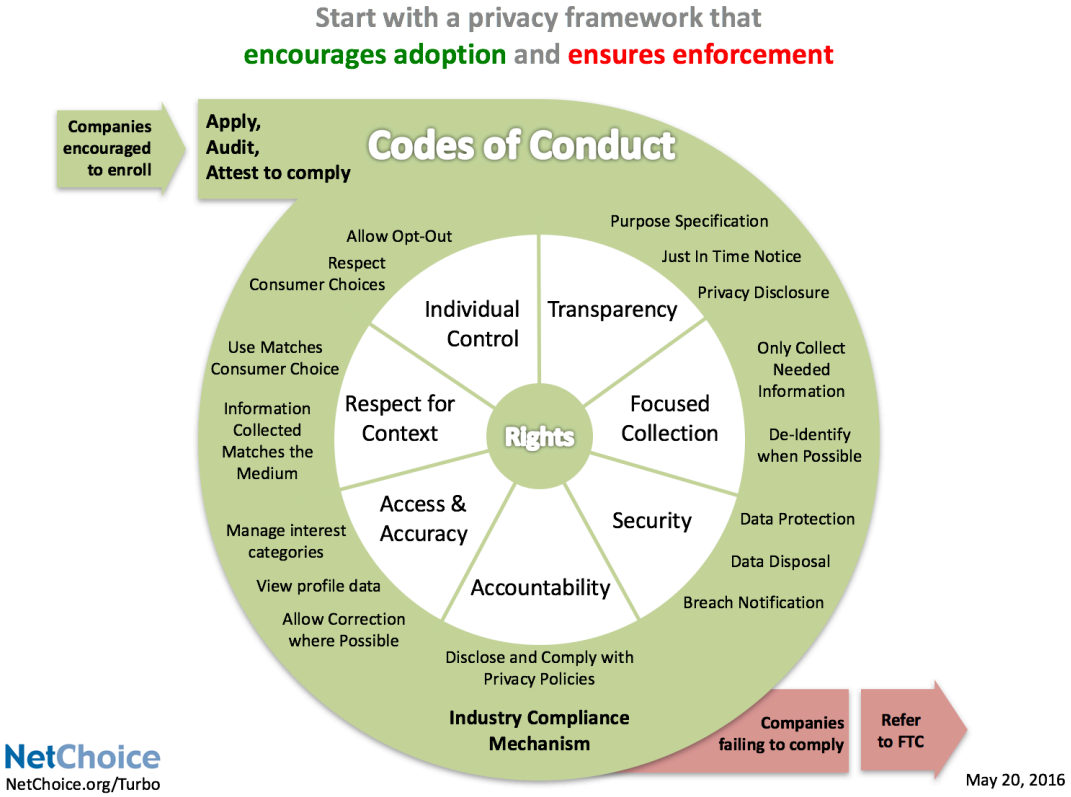
As seen in the conceptual overview, components of the Fair Information Practice Principles form the aspirational core that influences business conduct regarding data privacy. From previous work by the FTC, NAI, and IAB, we've established the foundational principles for the

---

[20] Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996.
[21] 15 U.S.C. § 1681.
[22] Title VII of the Civil Rights Act of 1964.
[23] FTC Commissioner Maureen K. Ohlhausen Speech Before the Hudson Institute, *The Government's Role in Privacy: Getting it Right*, (October 16, 2012).

collection and use of personal information: individual control, transparency, respect for context, access and accuracy, focused collection, accountability, and security.

Participating companies would publicly attest to implement Codes within their business operations, including periodic compliance reviews. If a company failed to comply with the adopted Codes, the FTC and state Attorneys General could bring enforcement actions, as is currently the case when companies fail to honor their adopted privacy policies.



Significantly, this framework does not require additional legislation to establish any new laws regarding "informational injury."

The FTC has an opportunity to shape the future of how we treat information. We only ask that they do so from a place of impartiality and study. We thank you for your consideration and we ask that you recognize the impact FTC regulation will have on either growing or limiting these wonderful and exciting new innovations.

Sincerely,

Carl Szabo
Vice President and General Counsel
NetChoice

NetChoice is trade association of leading e-commerce and online businesses.
www.NetChoice.org