

Information Technology and Innovation Foundation
1101 K Street NW, Suite 610
Washington, DC 20005

August 20, 2018

Donald Clark
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex C)
Washington, DC 20580

RE: Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201

Dear Secretary Clark,

The Information Technology & Innovation Foundation (ITIF) is pleased to submit these comments in response to the request for comment (RFC) from the Federal Trade Commission (FTC) on whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection enforcement law, enforcement priorities, and policy.¹

ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington, and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation, and productivity.

Please find our response to the following topic:

THE COMMISSION'S REMEDIAL AUTHORITY TO DETER UNFAIR AND DECEPTIVE CONDUCT IN PRIVACY AND DATA SECURITY MATTERS

The FTC provides an important function in protecting consumers and ensuring competition in many areas of the U.S. economy. In addition to having authority to investigate and combat unfair and deceptive practices,

¹ "Hearings on Competition and Consumer Protection in the 21st Century," Federal Trade Commission, n.d.
<https://www.ftc.gov/policy/hearings-competition-consumer-protection>.

the FTC enforces multiple sector specific laws, such as the CAN-SPAM Act, the Children’s Online Privacy Act, the Truth in Lending Act, the Equal Credit Opportunity Act, and the Fair Credit Reporting Act. While the FTC has done much to protect consumer privacy and security, there are opportunities to better protect consumers while at the same time encouraging innovation in today’s digital economy.

The FTC Should Limit Its Enforcement Actions for Unfair and Deceptive Conduct to Cases Where There Is Concrete Consumer Harm

The FTC’s enforcement actions send important signals to businesses in the private sector about how they should allocate their resources to comply with laws and regulations. Ideally, these signals should encourage businesses to take actions that protect consumers and discourage businesses from taking actions that harm consumers; while not discouraging companies from taking risks that might generate innovation that is beneficial to consumers. Unfortunately, this has not always been the case as the FTC has taken action against companies even when lacking evidence of tangible consumer harm (see, for example, ITIF’s discussion of the FTC’s actions against Nomi Technologies despite finding no action of consumer injury).²

In the context of data, harm refers to the extent to which consumers are materially and negatively impacted by misuse of their personal information, which they could not have reasonably avoided themselves. Harms can come in several forms.³ Autonomy violations result in harm for consumers when information they consider sensitive and would prefer to keep private becomes public through involuntary means. Harms that arise from autonomy violations are often reputational or interpersonal. Discrimination occurs when personal information is used to deny a person access to something, such as employment, housing, loans, and other goods.⁴ Finally, economic harm occurs when a consumer suffers a financial loss or damage because of the misuse of their personal information. Most economic harms that result from personal information are identity theft, fraud, or larceny, which are not the primary focus of most privacy policies and regulation. A harm-based standard is important because cultural norms and standards over what individuals consider privacy-invasive

² Daniel Castro, “Testimony of Daniel Castro on Legislative Hearing on 17 FTC Bills,” Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, May 24, 2016, <http://docs.house.gov/meetings/IF/IF17/20160524/104976/HHRG-114-IF17-Wstate-CastroD-20160524.pdf>.

³ Robert Atkinson, Daniel Castro and Alan McQuinn, “ITIF Filing to FTC on Informational Injury Workshop” (Information Technology and Innovation Foundation, October 27, 2017), <https://itif.org/publications/2017/10/27/itif-filing-ftc-informational-injury-workshop>.

⁴ There are many types of discrimination, including based on age, class, disability, employment, language, gender, genetic information, national origin, pregnancy, race or ethnicity, religion, sex, sexual orientation, and more.

and what they are willing to share changes over time, and this type of regulatory principle will adjust with changing expectations.

How and When the FTC Should Intervene With Unfair and Deceptive Conduct

As described in Figure 1, when deciding whether to take enforcement measures, ITIF recommends that the FTC consider two key factors: the extent to which a company acted intentionally or negligently, and the extent to which a company's action caused real, substantial consumer harm. Importantly, the FTC should not subject companies to punitive measures for actions they take in good faith that did not cause consumer harm because doing so would force companies to prioritize regulatory compliance rather than preventing consumer injury (e.g., hiring privacy lawyers to rewrite their online terms of service to minimize legal exposure from a data breach rather than hiring security experts to remedy cybersecurity vulnerabilities). In addition, the FTC should treat companies whose maleficence, negligence, willful neglect, or ineptitude results in harm to consumers differently than those that harm consumers through unintentional missteps as they strive to create innovations that benefit society. While penalties will be required in both scenarios, the FTC should save its most aggressive enforcement actions for the former.⁵ Moreover, it is important for the FTC to understand that the digital economy, unlike business practices in the “analog” economy, is anything but mature. New technologies, consumer offerings, and business models are continuing to emerge. In such an environment, consumer protection regulation needs to ensure that it is not so strict and punitive as to harm innovation, especially in cases where there was no intent to do harm and where no harm was done.

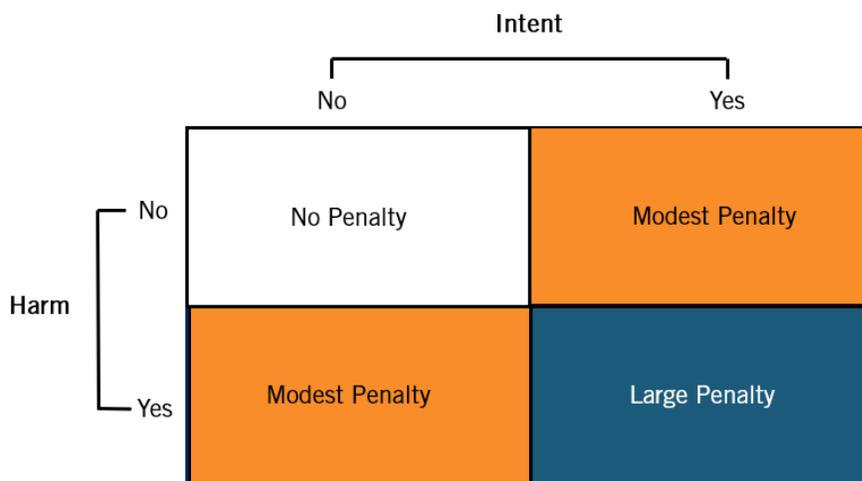
⁵ Daniel Castro, “Latest Privacy Kerfuffle Shows Limits of Proposed Privacy Legislation,” *Innovation Files*, February 21, 2012, accessed August 8, 2018, <http://www.innovationfiles.org/latest-privacy-kerfuffle-shows-limits-of-proposed-privacylegislation/>.

Figure 1: Recommended level of regulatory penalty based on harm and intent/negligence.

The FTC should pay attention to harm and intent when using its enforcement authority against companies involved in unfair and deceptive conduct to avoid creating perverse incentives.⁶ The FTC should use these criteria to decide on the appropriate response, where unintentional and harmless actions elicit the smallest penalty and intentional and harmful actions elicit the largest. Penalties should be designed to encourage companies to make sure they do not willfully commit infractions or impose real harm on users. Intent refers to the extent to which companies willfully choose to commit a certain act. For enforcement purposes, negligence, willful neglect, and ineptitude should also be considered intentional actions. By focusing on intent, the FTC can better determine which companies are acting in good faith to bring innovation to market and which are maliciously engaging in unfair or deceptive practices.

Consider the following the following four scenarios:

Scenario 1: A company makes a mistake that does not result in tangible consumer harm. In this instance, regulators should work to resolve the complaint, but not impose any penalties. For example, many tech companies publish written policies describing their products and services, but with the rapid pace of change, these descriptions can become out of sync with the latest versions. Certainly, companies should strive to keep these updated, but in the race to innovate, it is not surprising that on occasion something gets overlooked.



When this happens, companies should not face punitive sanctions for actions that do not cause consumer harm and that are undertaken in good faith. Moreover, if the FTC pursues large penalties against companies

⁶ Daniel Castro and Alan McQuinn, “How and When Regulators Should Intervene.”

for deviating from their stated policies, it may simply push companies to create broader, less transparent policies that exempt them from future liability and do not enhance consumer protections. Negligence should be considered intentional, thus harm caused by negligence does not fall into this category.

Consider the case the FTC brought against Nomi Technologies, a company that provided in-store retail analytics.⁷ The FTC's complaint stated that Nomi included a partially incorrect statement in its privacy policy about how consumers could opt out of data collection at retail locations—an option that Nomi was under no legal obligation to provide.⁸ Nomi's privacy policy stated, "Nomi pledges to... always allow consumers to opt out of Nomi's service on its website as well as *at any retailer using Nomi's technology*" (emphasis added).⁹ This was an error because while it offered consumers the ability to opt out of data collection on its website from all of its retail partners, none of its retailers offered consumers a separate, in-store, opt-out mechanism. Importantly, the FTC provided no evidence that any consumers were even affected, let alone harmed. At the time, Chairwoman Ramirez and Commissioners McSweeney and Brill argued that some consumers interested in opting out may have visited Nomi's website but chose not to do so. However, the population of potentially affected consumers was miniscule. Only 3,840 consumers even downloaded Nomi's privacy policy.¹⁰ Of that group, how many read the relevant portion of the policy, chose not to opt-out of all tracking using the website, visited at least one retail partner, carried a mobile phone, and wanted to opt-out at a particular store? No one at the FTC identified any consumers who fit this profile.

While the FTC did not impose any civil penalties on Nomi, by formally taking action when there was no injury to consumers, the FTC sent a signal that companies should spend more time on corporate lawyers and less time delivering value to consumers, including through developing privacy-enhancing technologies. This decision told companies like Nomi that they would be better off providing no privacy guarantees to their consumers; that way they will not fall victim to this sort of gotcha-style enforcement action. Rather than bringing a case and settlement against Nomi, the FTC should have shown some regulatory restraint by simply

⁷ Joshua Wright, "Dissenting Statement of Commissioner Joshua D. Wright," Federal Trade Commission, April 23, 2015, accessed August 8, 2018, http://www.ftc.gov/system/files/documents/public_statements/638371/150423nomiwrightstatement.pdf.

⁸ "In the Matter of Nomi Technologies, Inc.: Complaint," Federal Trade Commission, accessed August 8, 2015, <http://www.ftc.gov/system/files/documents/cases/150423nomicmpt.pdf>.

⁹ "In the Matter of Nomi Technologies, Inc.: Complaint," Federal Trade Commission.

¹⁰ Wright, "Dissenting Statement of Commissioner Joshua D. Wright."

notifying the company of the problem and verifying that it had been corrected. It was a waste of valuable agency resources that could have better been spent pursuing cases involving actual consumer harm.¹¹

Scenario 2: A company make an unintentional mistake that results in real, substantial harm to consumers. In this instance, regulators should again work with the company to fix the problem but impose only a modest penalty against the company to mitigate the damage that resulted from the company's error. The purpose of the penalty should be to make consumers whole again or to allocate resources to help prevent similar issues from happening again.

Consider the FTC's enforcement action against Amazon in 2011. At the time, the company faced a growing number of complaints that children had inadvertently accumulated excess charges by making in-app purchases.¹² Amazon responded to the enforcement action by contesting the allegations in a letter to the FTC denying the charges and vowed to defend itself in court.¹³ It appears these in-app charges were unintentional and Amazon has subsequently acted in good faith to fix the resulting problems.¹⁴ The company first self-corrected in 2012 by requiring a password for in-app charges over \$20.¹⁵ When this did not fully solve the

¹¹ Maureen Ohlhausen, "Dissenting Statement of Commissioner Maureen K. Ohlhausen," Federal Trade Commission, April 23, 2015, accessed August 8, 2018, http://www.ftc.gov/system/files/documents/public_statements/638361/150423nomiohlhausenstatement.pdf; Wright, "Dissenting Statement of Commissioner Joshua D. Wright," Federal Trade Commission.

¹² "FTC Alleges Amazon Unlawfully Billed Parents for Millions of Dollars in Children's Unauthorized In-App Charges," Federal Trade Commission, July 10, 2014, accessed August 8, 2018 <http://www.ftc.gov/news-events/press-releases/2014/07/ftc-alleges-amazon-unlawfully-billed-parents-millions-dollars>.

¹³ Recently, a federal judge refused to dismiss the case, and it seems that it will be decided in court. Andrew C. DeVore, "Amazon Letter to FTC," *Scribd*, July 1, 2014, accessed August 8, 2018, <http://www.scribd.com/doc/232376130/Amazon-letter-to-FTC>, and Brian Fung, "The FTC just scored a victory in its suit against Amazon," *Washington Post*, December 2, 2014, accessed August 8, 2018, <http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/02/the-ftc-just-scored-a-victory-in-its-suit-against-amazon/>.

¹⁴ "Set Parental Controls for In-App Purchases," *Amazon*, accessed August 8, 2018, <http://www.amazon.com/gp/help/customer/display.html?nodeId=201357720>, and DeVore, "Amazon Letter to FTC."

¹⁵ Grant Gross, "Amazon allowed kids to spend millions on in-app purchases, FTC says," *IT World*, July 10, 2014, accessed August 8, 2018, <http://www.itworld.com/article/2696340/it-management/amazon-allowed-kids-to-spend-millions-on-in-app-purchases--ftc-says.html>.

problem, the company continued updating its practices and controls to meet the special needs of some consumers.¹⁶ In this case, a substantial penalty is unwarranted since it does not appear that Amazon intended to cause harm to its consumers or violate any laws. As the aforementioned framework describes, the FTC should push for a settlement that ensures that Amazon refunds any mistaken charges and that the described harms cease. The FTC should also recognize that in cases like Amazon's, where the company is adapting to consumer needs and has caused little consumer harm, the Commission should not displace a company's judgment on how best to serve its customers with its own.

Scenario 3: A company intentionally commits an infraction but no harm results from that action. In this case, the FTC should work to resolve the problem and levy a modest penalty against the company. The purpose of the penalty should be to punish those who act irresponsibly or negligently and incentivize better behavior. However, unlike in situations where consumers have been harmed, there is no need to use penalties to try to make consumers whole again.

For example, Path is a social network that lets users share journal entries, photos, and location information between friends.¹⁷ From the start, Path billed itself as a different kind of social network, one where a user could interact and share personal and private messages and photos with just their closest friends. But despite its privacy hook, Path's service initially violated the Children's Online Privacy Protection Act (COPPA) Rule—which requires operators who knowingly allow children under 13 to use their services to notify parents and obtain consent prior to collection, use, or disclosure of personal information from children under 13—by collecting personal information from approximately 3,000 preteens without first getting consent.¹⁸ In 2013, the FTC brought a complaint against Path for knowingly collecting, using, and disclosing personal information from children, although it did not include any evidence of actual harm to users in its

¹⁶ Ibid.

¹⁷ Ellis Hamburger, "Path is back with a new messaging app that can talk to people and places," *The Verge*, June 20, 2014, accessed August 8, 2018, <http://www.theverge.com/2014/6/20/5827452/path-is-back-path-talk-messaging-app-acquires-talkto-unlimited-friends-list-dave-morin>.

¹⁸ "United States of America, Plaintiff, v. Path, Inc., Defendant," Federal Trade Commission, February 1, 2013, accessed August 8, 2018, <http://www.ftc.gov/enforcement/cases-proceedings/122-3158/path-inc>.

complaint.¹⁹ Path settled with the FTC and paid an \$800,000 civil penalty.²⁰ This case is an example of a company that purposefully gathered information on some of its users in violation of the law, although that violation caused little or no consumer harm. In this case, penalizing the company for violating the law was appropriate to help set an example for other companies.

Scenario 4: A company acts with intent, including negligence, and its actions harm consumers. In this case, the FTC should consider imposing significant penalties. Penalties should both make consumers whole and deter bad behavior in the future. In this way, regulation can help foster innovation within industry by strongly discouraging companies from engaging in practices that both violate the law and harm consumers. By setting an example, the FTC can also spur other companies seeking to minimize their risk and exposure to focus their compliance efforts and update their practices.

Consider the FTC's enforcement action in 2017 against Dish Network, a Colorado-based satellite television provider, for violating the FTC's Telemarketing Sales Rule (TSR), the Telephone Consumer Protection Act, and state law.²¹ The TSR is designed to improve consumer choice regarding telemarketing calls by creating the National Do Not Call (DNC) Registry, a database of phone numbers that consumers can add themselves to which indicates their preference not receive telemarketing calls.²² The court found that Dish initiated, or caused its telemarketers to initiate, telephone calls to phone numbers on the DNC Registry over 66 million times, in violation of the TSR.²³ Indeed, telemarketers allegedly dialed a single consumer's phone number 15

¹⁹ "Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books," Federal Trade Commission, February 1, 2013, accessed August 8, 2018, <https://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived>.

²⁰ *Ibid.*

²¹ "FTC and DOJ Case Results in Historic Decision Awarding \$280 Million in Civil Penalties against Dish Network and Strong Injunctive Relief for Do Not Call Violations," Federal Trade Commission, June 6, 2017, accessed August 14, 2018, <https://www.ftc.gov/news-events/press-releases/2017/06/ftc-doj-case-results-historic-decision-awarding-280-million-civil>.

²² "Q&A for Telemarketers & Sellers About DNC Provisions in TSR," Federal Trade Commission, August 2016, accessed August 14, 2018, <https://www.ftc.gov/tips-advice/business-center/guidance/qa-telemarketers-sellers-about-dnc-provisions-tsr>.

²³ "FTC and DOJ Case Results in Historic Decision Awarding \$280 Million in Civil Penalties against Dish Network and Strong Injunctive Relief for Do Not Call Violations," Federal Trade Commission.

times in 2010 and 2011, despite its inclusion on the DNC Registry.²⁴ As a result, Dish received the largest civil penalty ever obtained for a violation of the FTC Act—\$168 million. This case is an example of a company that willfully violated the law and violated consumers clear choice to not receive telemarketing calls. In this case, the FTC was right to seek an appropriately hefty penalty that both deters other companies from violating the TSR and ensures future compliance from Dish.

When weighing enforcement actions against companies, the FTC should consider several things. First, intentions matter. As companies, especially newer companies, race to innovate, mistakes will inevitably happen. If the FTC wants to foster innovation, it should ensure the punishment fits the crime. Moreover, consumers are better served by targeted rules and enforcement actions that address specific harms. If the FTC focuses on levying large fines and long-term consent decrees for actions that caused little to no harm, companies will focus less on releasing safe, useful products and services, and more on legal fees and internal audits. By following the framework discussed in these comments, the FTC can both protect consumer privacy and advance innovation.

Sincerely,

Rob Atkinson
President, Information Technology and Innovation Foundation

Daniel Castro
Vice President, Information Technology and Innovation Foundation

Doug Brake
Director, Broadband and Spectrum Policy, Information Technology and Innovation Foundation

Joe Kennedy
Senior Fellow, Information Technology and Innovation Foundation

Alan McQuinn
Senior Policy Analyst, Information Technology and Innovation Foundation

Josh New
Senior Policy Analyst, ITIF's Center for Data Innovation

²⁴ “Are you owed \$1,200? Maybe, if you got a Dish Network telemarketing call,” *CBS News*, May 7, 2018, accessed August 14, 2018, <https://www.cbsnews.com/news/dish-network-do-not-call-lawsuit-eligible-to-collect-1200-per-call/>.