ITIF
The Information Technology & Innovation Foundation

How and When Regulators Should Intervene

BY DANIEL CASTRO AND ALAN MCQUINN | FEBRUARY 2015

If regulators apply the same kind of blanket penalties and remedies regardless of either intent or harm, the result will be less innovation.

Since the rise of the modern regulatory state in the 1970s, there has been a debate over how agencies should regulate and how legislative bodies should conduct regulatory oversight. On what basis should regulatory agencies, particularly agencies designed to protect consumers, be judged?[1]

Clearly, one standard has been whether or not they adequately protect customers from unfair, deceptive, or fraudulent practices, something U.S. federal financial regulatory agencies failed miserably at in the 2000s. Another standard that many moderates and conservatives have advocated is the application of cost-benefit standards to regulatory rules. Ideally, regulation should create a system of incentives to promote desirable behavior and disincentives to discourage undesirable behavior in the marketplace and do so in a way that limits compliance costs. However, as the economy has become more innovation-based, there has been considerably less focus on how regulatory agencies can both protect consumers and avoid as much as possible undermining incentives for innovation. Getting regulation right when it comes to innovation-based business activities is critical because innovation is increasingly the source of national competitive advantage and economic growth.

The challenge for a nation's regulatory system stems from the fact that innovation by its very nature involves risks and mistakes—the very things regulators inherently want to avoid. And yet from a societal perspective there is a significant difference between mistakes that harm consumers due to maleficence, negligence, willful neglect, or ineptitude on the part of the company and those that harm consumers as a company strives to create innovations that benefit society. Likewise, there should be a distinction between a company's actions that violate regulations and cause harm to consumers (or competitors) and ones that cause little or no harm. If regulators apply the same kind of blanket penalties and remedies regardless of either intent or harm, the result will be less innovation.

Innovation is about risk, and if innovators fear they will be punished for every mistake (including those often made by mid-level engineers just going about their jobs and those with inconsequential impacts on consumers), then they will be much less assertive in trying to develop the next new thing.

Regulations can have two types of unintended consequences: They can block beneficial innovations if they are too burdensome, and they can fail to guard against harmful innovations if they are too lax. Regulatory agencies often focus on minimizing the latter since this type of mistake makes the agency look ineffective and exposes it to public backlash. For example, the U.S. Federal Drug Administration (FDA) does not want to get caught approving an unsafe drug. However, agencies face less pressure to avoid unintentionally preventing harmless innovations that provide societal benefit because the opportunity costs are difficult to recognize or measure. Likewise, when the pace of market change is slow and international competition is minimal, it costs little to overregulate in a way that inhibits innovation. However, when the level of innovation and international competition increases, as it has over the last few decades, the cost of overregulation increases considerably.

While the regulatory framework developed here applies to most regulatory agencies, this report will focus on how the U.S. Federal Trade Commission (FTC) has, or should have, applied its regulatory oversight in various cases involving tech companies whose products or services go through rapid cycles of change. This report offers a typology that regulators can use when evaluating which infractions should be pursued based on two dimensions—whether that company acted intentionally or negligently and whether a company's action caused real consumer harm. This proposed framework reflects a sliding scale based on these criteria, where unintentional and harmless actions elicit the smallest penalty and intentional and harmful actions elicit the largest. Penalties should therefore be designed to encourage companies to make sure they do not willfully commit infractions or impose real harm on users. This can provide a model for when and how the FTC should exercise its discretion to intervene when companies commit infractions.

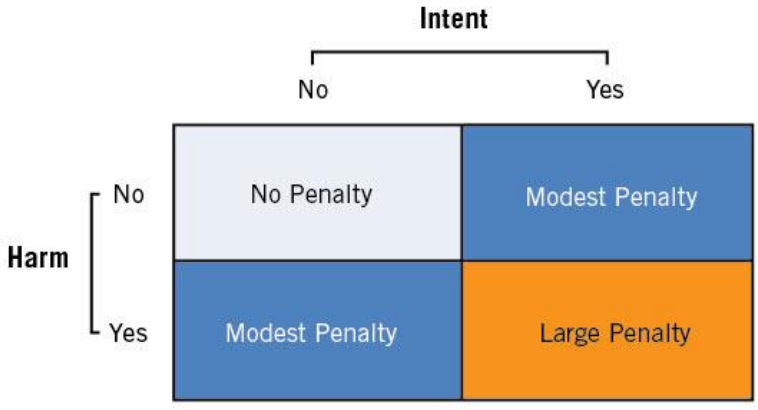

Figure 1: Recommended level of regulatory penalty based on harm and intent

This report will explore the dimensions of harm and intent, using this typology as a guide for allocating penalties against companies. It further clarifies what type of penalty should be administered in each of these four circumstances. This type of flexible system is necessary to strike a balance between protecting consumers and ensuring that unnecessarily harsh penalties do not act as a disincentive to innovation. Penalties that are too severe have the real possibility of causing U.S. companies to be overly cautious, putting them at a disadvantage compared to foreign competitors. In addition, unnecessarily harsh penalties by the FTC or other U.S. agencies help legitimize punitive behavior against U.S. firms by foreign governments in their quest to build national tech champions, as we see currently in China and Europe.

This report will offer further clarification of each square in the above table. It will then explore each with an example viewed through the lens of the best regulatory response.

HARM AND INTENT

When evaluating company actions to determine if regulatory enforcement action is needed, regulators should consider two main factors: harm and intent. Harm refers to the extent to which consumers or competitors have been negatively impacted by a company's actions, while intent refers to the extent to which companies willfully choose to commit a certain act, or exhibit negligence or incompetence. The following hypothetical situations explore both factors.

First, if a company makes a mistake and something happens that does not result in real consumer harm (as opposed to either no harm or hypothetical harm), then 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. As we have argued before, to do so would only create perverse incentives for companies to slow down the pace of innovation.[2] Moreover, if the FTC mindlessly pursues large penalties against companies 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.

Second, if an action is unintentional but results in real harm to consumers, then regulators should again work with the company to fix the problem but levy only a modest penalty against the company to mitigate the damage that resulted from the company's mistake. The purpose of the penalty should be to make consumers whole again or to allocate resources to help prevent similar issues from happening again.

Third, if a company intentionally commits an infraction but no harm results from that action, then regulators should not only work to resolve the problem, but also 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.

Finally, if a company acts with intent, including negligence, and its actions harm consumers, then regulators 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.

The following four case studies provide examples of each of these situations and illustrate the optimal regulatory response.

Case Study 1: No Harm, Unintentional

In 2011 and 2012, Google used special code to place certain advertising-tracking cookies on the computers of customers using Apple's Safari web browser who had intended for that kind of tracking to be blocked.[3] Apple designed Safari to block such tracking by default.[4] Google's actions were said to contradict a web page on its help center, which contained instructions on how Safari users could avoid tracking. Google refuted this claim, calling it a mischaracterization and stressed that its advertising cookies in question did "not collect personal information."[5] Nevertheless, immediately upon discovering the problem, Google removed the infringing code.[6] In 2012, the FTC sued Google for misrepresenting privacy assurances, eventually settling with the company to the tune of $22.5 million.[7] This was the largest penalty the FTC had ever levied against a single company at the time. (In 2014, the FTC fined Apple $32.5 million for mistaken in-app purchases.[8])

To better understand the dynamics of this case, it is useful to explore the technology involved. When a user visits a website, the website can request that the user's web browser store certain data on that computer in a cookie—a small data file.[9] Many browsers allow this activity by default, but some, like Safari, block most third-party cookies. It is also important to note that many web pages pull content from more than one domain. For example, a website might also use a Facebook Like or a Google "+1" button on its page. To allow this type of functionality to work properly, the web browser must allow some third-party cookies. While some third-party cookies track individual users, many are used for website analytics—such as monitoring how many unique users visit a website—and do not harm user privacy or collect personally identifiable information.

When deciding whether to give a cookie access, the web browser (in this case Safari) tries to determine whether the user has sent information to the particular domain that generated the cookie.[10] If this request is sent to a specific domain (such as by a Google "+1" button), then the cookies for that domain will be allowed. If not, they will be denied. Google used

this browser functionality so that it could set cookies on websites using its Google "+1" button or display Google ads by using code that would send an HTTP request to a Google domain. After sending this request, Safari would accept third-party cookies from the Google domain. Therefore, Safari users who had enabled their blocking feature may have thought that third-party sites could not track their online behavior even though they actually could.[11]

Despite the fact that this tracking was inadvertent, did not lead to any harm for consumers, and was corrected immediately upon discovery, the FTC decided to sue Google—presumably to make an example of it.[12] The main focus of the lawsuit was an outdated page from Google's help center that assured Apple users that Safari's setting would block unwanted tracking. Google had last updated the help page in 2009, two years prior to the lawsuit.[13] Because Google was already under a 20-year consent decree stating that it would not misrepresent its privacy practices to its consumers, it was penalized $16,000 per violation per day for its mistake ($22.5 million in total).[14]

In this case, the agency focused its limited resources on penalizing a company for unintentional actions that did not result in any actual user harm. Instead it should have been directing those resources to cases where users suffered real harm or to companies that intentionally committed infractions, including spammers, purveyors of malware, and fraudulent e-commerce companies.[15] In line with the above framework, when a company unintentionally makes a mistake that results in no harm, a better strategy for the FTC would have been for it to work to resolve the complaint rather than impose a fine, especially such a hefty one.

Case Study 2: Harm, Unintentional

Amazon holds the original patent for 1-Click technology, the service that enables users to buy Amazon products with a single click of a mouse, button, or finger.[16] This ability to make transactions effortlessly is a core part of Amazon's brand, and provides a great consumer experience. However, when Amazon began allowing 1-Click in-app purchases on its Kindle Fire tablet in late 2011, the company faced a growing number of complaints that children had inadvertently accumulated excess charges by making in-app purchases.[17] Children who were playing games on the Kindle Fire sometimes accidentally bought virtual items such as "coins," "stars," and "acorns," which typically ranged in price from $1 to $5 (but could be as high as $99).[18] Mobile games, such as the popular Candy Crush, offered these purchases to enhance the game or to give a user access to more advanced levels in the game. These apps use a "freemium" business model whereby a limited version of the app is available at no charge, but the app developer earns money through in-app purchases. As the app store operator, Amazon receives 30 percent of each purchase.[19] For this reason, some have assumed malice on the part of the company rather than an attempt by the company to make its consumers' lives easier.

In mid-2014, the FTC announced that it was filing a lawsuit against Amazon alleging that the company had failed to set appropriately tight controls for in-app purchases made by children.[20] The agency asserts that Amazon made it too easy for children to make these purchases and believes the company is liable for refunding affected parents. Amazon

responded to the announcement by contesting the allegations in a letter to the FTC denying the charges and vowed to defend itself in court.[21] It appears these in-app charges were unintentional and Amazon has subsequently acted in good faith to fix the resulting problems.[22] The company first self-corrected in 2012 by requiring a password for in-app charges over $20.[23] When this did not fully solve the problem, the company continued updating its practices and controls to meet the special needs of some consumers.[24] Importantly, not all consumers want to have to go through the extra step of adding a password for each in-app purchase. For many, the ease of not having to include a password provided real value. Nonetheless, not only did Amazon attempt to refund customers for unwanted purchases, it also added in-app parental controls and a real-time notification system for all purchases to reduce the chance of these charges happening again and to improve the overall customer experience.[25] As ITIF has argued before, Amazon's efforts to rapidly prototype and update its systems based on consumer feedback is exactly what government regulators should like to see in a well-functioning market.[26] Nevertheless, the FTC complained that these refund processes were "unclear and confusing, involving statements that do not explain how to seek refunds for in-app charges or suggest consumers cannot get a refund for these charges."[27]

This case study offers an example of a company that unintentionally caused harm to some of its consumers, as it created value for others. 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, it should not displace a company's judgment on how best to serve its customers with its own.

Case Study 3: No Harm, Intentional

Path is a social network that lets users share journal entries, photos, and location information with up to 150 of their friends (it originally launched with a 50-friend cap).[28] Started in a San Francisco apartment in 2010, the service has 5 million active daily users and 23 million registered accounts.[29] 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.[30] 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, including geo-location data, from approximately 3,000 preteens without first getting the requisite consent.[31]

In May 2012, Path changed its sign-up process to block children under the age of 13 from its service.[32] Regardless, 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 complaint.[33] (The FTC complaint also included a separate allegation about improperly collecting data from adult users.) Path settled with the FTC and paid an $800,000 civil penalty.[34] It signed a consent decree

agreeing to not misrepresent the extent to which it maintains the privacy and confidentiality of its users' personal information; to delete all information it collected on children under age 13; to create a privacy program; and to obtain independent privacy assessments once every two years for the next two decades.[35]

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. The penalty was substantial given the size of the company (a startup with approximately $40 million in funding at the time).[36] However, had consumers suffered actual harm, a larger penalty would have been appropriate.

Case Study 4: Harm, Intentional

Uber is a ridesharing smartphone application that connects users to a rides-for-hire market. In November 2014, a reporter for BuzzFeed reported that the general manager of Uber New York had tracked her approach to an interview with him (in an Uber vehicle) using the company's "God View" application.[37] This tool shows the location of Uber vehicles and customers who have requested a car, and is widely available to corporate employees, but drivers—who operate as contractors—do not have access. The journalist, Johana Bhuiyan, never authorized being tracked, which violates Uber's stated privacy policy.[38] In the wake of this revelation, Uber subsequently investigated and reprimanded its employee.

Uber has a history of flirting with privacy infractions. Uber was pushed to display its privacy policy in a blog post for the first time (although the company said the policy had always been in effect) when a senior executive suggested at a company dinner that Uber ought to consider hiring an opposition research team to dig up incriminating evidence on Uber's critics in the media.[39] This revelation also led to reports of other possible privacy-policy violations, such as reports that Uber used "God View" at a company party, allowing attendees to view all of the Uber rides taking place in a particular city as well as the silhouettes of waiting Uber users who had used their phones to signal for rides. This use of "God View" was anonymous, but some guests were treated to a viewing that showed them the "whereabouts and movements" of multiple individual New York users, which would again violate Uber's privacy policy.[40]

This example illustrates a situation where a company's employees used their access to company data for non-business-related personal reasons, such as to satisfy their own curiosity. In similar cases, employees could knowingly violate the privacy policies of their employer to track their friends in real-time, survey the movements of ex-lovers, or even electronically spy on the behavior of acquaintances.[41]

If a company is willfully violating its own stated policies while also harming its customers, the FTC can and should take enforcement actions.[42] In this case, the FTC should investigate this incident, and if the allegations prove true, it should work with Uber to make sure its new internal policies and procedures restrict employee access to the personal consumer data it collects, including audit trails, and should levy an appropriate penalty against the company. If the FTC decides the facts merit pursuing a case against Uber, it should seek a penalty that deters lax policies on employee access to customer data for non-business purposes.

CONCLUSION

As regulators, including the FTC, weigh enforcement actions against companies, there are a number of things they should consider. First, intentions matter. As companies race to innovate, mistakes will inevitably happen. Regulators should make sure the punishment fits the crime, or they could chill the kind of risk-taking needed for innovation.

Second, huge fines for these mistakes may actually leave consumers worse off. If regulatory agencies levy massive fines for unintentional actions, or for actions that cause little to no harm (or both), companies will focus less on releasing safe, useful products and services for consumers, and more on legal fees and internal audits that slow down the pace of innovation but protect them from lawsuits. In addition, this may discourage transparency, because the takeaway for many companies will be that they are better off not fully disclosing details about their practices to customers out of fear that this information could be used against them in the future. They may also be deterred from releasing new products and services until their lawyers have signed off on everything. This would deprive consumers of the rapidly developing services and technologies that characterize the Internet age, and also limit global competitiveness in the Internet industry. Plus, every dollar transferred to government is one less that can be invested in innovation.

Third, overzealous regulatory judgments and penalties can limit national competitiveness and jobs, especially in fast-paced, innovation-based industries that constitute the core competitive advantage in developed nations like the United States. There is a growing "race for global innovation advantage" as nations around the globe seek to gain advantage by attracting these high-paying jobs to their borders.[43] Overly stringent regulatory judgments by U.S. regulatory agencies like the FTC not only limit U.S. tech firms' competitiveness, but also, as noted above, provide convincing justification to foreign governments that are intent on hobbling U.S. tech firms.

Fourth, regulators should not attempt to overrule a company's judgment about how best to serve its own customers. In cases where a company is trying to adapt to its consumers' needs and has caused relatively little or even no consumer harm, regulators should not try to micromanage the situation. As the above Amazon example illustrates, companies often are more than willing to self-correct their mistakes and adjust their business practices to correct unintended harms and bring added benefits to their customers.

Finally, regulatory agencies should recognize that consent decrees act as de facto law and should be careful with their use of such punitive schemes. By forcing companies into consent decrees, instead of using their own rulemaking authority or waiting for Congress to act, regulatory agencies often circumvent the democratic process and decrease transparency in rulemaking. Consent decrees, such as the ones the FTC has entered into with companies like Facebook, Twitter, and Google, reflect the agreement of only two parties, not all stakeholders. This type of regulation is dealt with on a case-by-case basis, ostensibly because Congress usually does not give regulatory agencies authority for broad-based regulation. Yet it still can have far-reaching effects. When a consent decree is created, all businesses in the same sector usually take heed of the results and mend their practices to fit the precedents set by the consent decree. These types of 20-year agreements can confine

companies to stagnant business practices and deter them from taking risks lest they be subject to steep federal fines. At times, consent decrees can create greater barriers for new entrants by subjecting them to costly, cumbersome, and complex de facto regulations under threat of potential lawsuits, entrenching established interests and even paradoxically harming competition in the marketplace. A better approach is for regulatory agencies to establish clear rules through their public processes and then take action against any company that knowingly violates them. Regulators can also use these concrete rules to target companies that knowingly harm consumers. The framework discussed in this report can help regulators draw those distinctions.

ENDNOTES

1. These include the Consumer Financial Protection Bureau, Consumer Product Safety Commission, Federal Aviation Administration, Federal Communications Commission, Federal Trade Commission, Financial Industry Regulatory Authority, Food and Drug Administration, and the National Highway Traffic Safety Administration.
2. Daniel Castro, "Latest Privacy Kerfuffle Shows Limits of Proposed Privacy Legislation," *Innovation Files*, February 21, 2012, http://www.innovationfiles.org/latest-privacy-kerfuffle-shows-limits-of-proposed-privacy-legislation/.
3. Julia Angwin and Jennifer Valentino-Devries, "Google's iPhone Tracking," *Wall Street Journal*, February 17, 2012, http://www.wsj.com/news/articles/SB10001424052970204880404577225380456599176.
4. Ibid.
5. Ibid.
6. Ibid.
7. "Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser," *Federal Trade Commission*, August 9, 2012, http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.
8. Amanda Holpuch, "Apple to pay $32.5m over practice that let children make in-app purchases," *The Guardian*, January 15, 2014, http://www.theguardian.com/technology/2014/jan/15/apple-practice-children-make-in-app-purchases.
9. Daniel Castro and Alan McQuinn, "The Economic Costs of the European Union's Cookie Notification Policy," *The Information Technology and Innovation Foundation*, November 2014, pg. 1-2, http://www2.itif.org/2014-economic-costs-eu-cookie.pdf.
10. Daniel Castro, "Latest Privacy Kerfuffle Shows Limits of Proposed Privacy Legislation," *Innovation Files.*
11. Ibid.
12. Julia Angwin, "Google, FTC Near Settlement on Privacy," *Wall Street Journal*, July 10, 2012, http://www.wsj.com/news/articles/SB10001424052702303567704577517081178553046.
13. Julia Angwin and Jennifer Valentino-Devries, "Google's iPhone Tracking," *Wall Street Journal.*
14. Ibid.
15. Daniel Castro, "Whatever happened to 'No harm no foul'?" *Innovation Files, July 10, 2012,* http://www.innovationfiles.org/whatever-happened-to-no-harm-no-foul/.
16. Eric Engleman, "Amazon.com's 1-Click patent confirmed following re-exam," *Bizjournals*, March 10, 2010, http://www.bizjournals.com/seattle/blog/techflash/2010/03/amazons_1-click_patent_confirmed_following_re-exam.html.
17. "FTC Alleges Amazon Unlawfully Billed Parents for Millions of Dollars in Children's Unauthorized In-App Charges," *Federal Trade Commission,* July 10, 2014, http://www.ftc.gov/news-events/press-releases/2014/07/ftc-alleges-amazon-unlawfully-billed-parents-millions-dollars.
18. Greg Bensinger, "FTC Sues Amazon Over In-App Purchases by Children," *Wall Street Journal*, July 10, 2014, http://www.wsj.com/articles/ftc-sues-amazon-over-in-app-purchases-by-children-1405012533, Cecilia King, "FTC sues Amazon over children's in-app purchases," *Washington Post*, July 10, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/10/ftc-sues-amazon-over-childrens-in-app-purchases/, and "FTC Alleges Amazon Unlawfully Billed Parents for Millions of Dollars in Children's Unauthorized In-App Charges," *Federal Trade Commission.*
19. "FTC Alleges Amazon Unlawfully Billed Parents for Millions of Dollars in Children's Unauthorized In-App Charges," *Federal Trade Commission.*
20. Ibid.
21. 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, 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, http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/02/the-ftc-just-scored-a-victory-in-its-suit-against-amazon/.

22. "Set Parental Controls for In-App Purchases," *Amazon*, accessed December 11, 2014, http://www.amazon.com/gp/help/customer/display.html?nodeId=201357720, and Andrew C. DeVore, "Amazon Letter to FTC," *Scribd.*
23. Grant Gross, "Amazon allowed kids to spend millions on in-app purchases, FTC says," *IT World*, July 10, 2014, http://www.itworld.com/article/2696340/it-management/amazon-allowed-kids-to-spend-millions-on-in-app-purchases--ftc-says.html.
24. Ibid.
25. "Set Parental Controls for In-App Purchases," *Amazon*, accessed Dec. 11, 2014, and Andrew C. DeVore, "Amazon Letter to FTC," *Scribd.*
26. Daniel Castro, "The FTC should reward, not penalize, companies that innovate in good faith," *The Hill*, July 11, 2014, http://thehill.com/blogs/pundits-blog/economy-budget/211721-the-ftc-should-reward-not-penalize-companies-that-innovate.
27. "FTC Alleges Amazon Unlawfully Billed Parents for Millions of Dollars in Children's Unauthorized In-App Charges," *Federal Trade Commission.*
28. Ellis Hamburger, "Path is back with a new messaging app that can talk to people and places," *The Verge*, June 20, 2014, http://www.theverge.com/2014/6/20/5827452/path-is-back-path-talk-messaging-app-acquires-talkto-unlimited-friends-list-dave-morin.
29. "Who We Are," *Path*, accessed December 18, 2014, https://path.com/about, and Harrison Weber, "Path has just 5 million daily active users globally," *Venture Beat*, September 10, 2014, http://venturebeat.com/2014/09/10/path-has-just-5-million-daily-active-users-globally/.
30. Kipp Bodnar, "How Path is Making 'Small' the New 'Big' in Social Media," *HubSpot*, January 5, 2012, http://blog.hubspot.com/blog/tabid/6307/bid/30493/How-Path-is-Making-Small-the-New-Big-in-Social-Media.aspx.
31. "United States of America, Plaintiff, v. Path, Inc., Defendant," *Federal Trade Commission*, February 1, 2013, http://www.ftc.gov/enforcement/cases-proceedings/122-3158/path-inc.
32. Om Malik, "Path reaches settlement with FTC, agrees to pay $800,000 fine for COPPA violations," *Gigaom*, February 1, 2013, https://gigaom.com/2013/02/01/path-reaches-settlement-with-ftc-agrees-to-pay-800000-fine-for-coppa-violations/.
33. Ibid.
34. "United States of America v. Path, Inc.," *Federal Trade Commission*, February 8, 2013, http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.
35. "United States of America v. Path, Inc.," *Federal Trade Commission*, and Jessica Guynn, "Mobile social networking app Path settles with FTC for $800,000," *Los Angeles Times*, February 1, 2013, http://articles.latimes.com/2013/feb/01/business/la-fi-tn-ftc-path-settlement-20130201.
36. Darrell Etherington, "Path Settles With FTC Over Privacy Row, Will Pay $800K and Establish New Privacy Program Including Outside Audits," *TechCrunch*, February 1, 2013, http://techcrunch.com/2013/02/01/path-settles-with-ftc-over-privacy-row-will-pay-800k-and-establish-new-privacy-program-including-outside-audits/.
37. Chanelle Bessette, "Does Uber Even Deserve Our Trust?" *Forbes*, November 25, 2014, http://www.forbes.com/sites/chanellebessette/2014/11/25/does-uber-even-deserve-our-trust/.
38. Don Reisinger, "Uber's 'God View' under scrutiny as spotlight intensifies on its practices," *CNET*, November 19, 2014, http://www.cnet.com/news/god-view-under-spotlight-as-uber-investigation-intensifies/, and Uber's Data Privacy Policy," *Uber*, November 17, 2014, http://blog.uber.com/privacypolicy.
39. Ben Smith, "Uber Executive Suggests Digging Up Dirt On Journalists," *BuzzFeed*, November 17, 2014, http://www.buzzfeed.com/bensmith/uber-executive-suggests-digging-up-dirt-on-journalists, Johana Bhuiyan and Charlie Warzel, "'God View': Uber Investigates Its Top New York Executive For Privacy Violations," *BuzzFeed*, November 18, 2014, http://www.buzzfeed.com/johanabhuiyan/uber-is-investigating-its-top-new-york-executive-for-privacy, and "Uber's Data Privacy Policy," *Uber.*
40. Kashmir Hill, "'God View': Uber Allegedly Stalked Users For Party-Goers' Viewing Pleasure (Updated)," *Forbes*, October 3, 2014, http://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/.

41. Charlie Warzel, "We Asked 29 Tech Companies If Their Employees Can Access Your Personal Data," *BuzzFeed*, December 14, 2014, http://www.buzzfeed.com/charliewarzel/we-asked-29-tech-companies-if-their-employees-can-access-you.
42. Julian Hattem, "Uber ignites new privacy fight," *The Hill*, November 11, 2014, http://thehill.com/policy/technology/225071-uber-ignites-new-privacy-fight.
43. Robert Atkinson and Stephen Ezell, *Innovation Economics: The Race for Global Advantage* (New Haven: Yale University Press, 2012).

ACKNOWLEDGEMENTS

The authors wish to thank the following individuals for providing input to this report: Rob Atkinson, Jean Cornell, Randolph Court, Alex Key, and Sue Wunder. Any errors or omissions are the authors' alone.

ABOUT THE AUTHORS

Daniel Castro is a Senior Analyst with the Information Technology and Innovation Foundation and Director of the Center for Data Innovation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

Alan McQuinn is a Research Assistant with the Information Technology and Innovation Foundation. Before joining ITIF, Mr. McQuinn was a telecommunications fellow for Congresswoman Anna Eshoo and an intern for the Federal Communications Commission in the Office of Legislative Affairs. He got his B.S. in Political Communication and Public Relations for the University of Texas at Austin.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a Washington, D.C.-based think tank at the cutting edge of designing innovation strategies and technology policies to create economic opportunities and improve quality of life in the United States and around the world. Founded in 2006, ITIF is a 501(c) 3 nonprofit, non-partisan organization that documents the beneficial role technology plays in our lives and provides pragmatic ideas for improving technology-driven productivity, boosting competitiveness, and meeting today's global challenges through innovation.

FOR MORE INFORMATION, VISIT WWW.ITIF.ORG.