Federal Trade Commission

The View from 600 Pennsylvania Avenue: Recent Developments in Law Enforcement and Policy at the Federal Trade Commission

Remarks of Joshua D. Wright*
Commissioner, Federal Trade Commission

at

U.S. Chamber of Commerce
Telecommunications & E-Commerce Committee
Spring Meeting

Washington, D.C.
May 16, 2014

Good afternoon. Thank you very much for the kind introduction. I am pleased to be here today to present keynote remarks for the Spring Meeting of the U.S. Chamber of Commerce's Telecommunications & E-Commerce Committee. I have been informed that this committee is responsible for developing Chamber policy relating to data security and privacy, the Internet and e-commerce, telecommunications, and

* The views stated here are my own and do not necessarily reflect the views of the Commission or other Commissioners. I am grateful to my advisor, Beth Delaney, for her invaluable assistance in preparing these remarks.

broadcasting and mass media. That's quite a portfolio. I am only here for a half hour but I am optimistic – maybe overly so – that I can touch upon many of these topics as well as answer questions that you might have. While I will discuss primarily the Commission's ongoing law enforcement and policy work, I will also give you a sense of my own thinking – as an economist and a lawyer – about useful frameworks and limiting principles, and discuss how my perspective sometimes might be a little different from that of the other Commissioners.

Apple Dissent

Perhaps the best place to start is with the topic of e-commerce. As many of you are probably aware, this past January, the Commission issued an administrative complaint alleging that that Apple, Inc. ("Apple") engaged in "unfair acts or practices" by billing parents and other iTunes account holders for the activities of children who were engaging with software apps likely to be used by children that had been downloaded onto Apple mobile devices.[1] In particular, the Commission took issue with a product feature of Apple's platform that opened a fifteen-minute period during which a user did not need to re-enter a billing password after completing a first transaction with the password. Because Apple did not expressly inform account holders that the entry of a password upon the first transaction triggered the fifteen-minute window during which users could make additional purchases without once again entering the

[1] Complaint, Apple, Inc., F.T.C. File No. 1123108, at para. 28-30 (Jan. 15, 2014).

password, the Commission's complaint alleged that Apple billed parents and other iTunes account holders for the activities of children without obtaining express informed consent.[2]

I respectfully disagreed. In order to deem a practice as unfair, the Commission must show that it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[3] My view of the evidence was that this was a case involving a miniscule percentage of consumers – the parents of children who made purchases ostensibly without their authorization or knowledge. The injury in this case was limited to an extremely small – and arguably, diminishing – subset of consumers.

There was no disagreement that the overwhelming majority of consumers used the very same mechanism to make purchases and that those charges were properly authorized. Indeed, the nature of Apple's disclosures on its platform is an important attribute of Apple's platform and affects the demand for and consumer benefits derived from Apple devices and services. Apple's product design choices, including the nature of these disclosures and its choice to integrate the fifteen-minute window, are a product of considerable investment and innovation, and provide substantial benefits for

[2] *Id.* at para. 4, 20, 28.
[3] 15 U.S.C. § 45(n).

consumers who do not want to experience excessive disclosures or by having to enter passwords every time they make a purchase.

I felt that the Commission, under the rubric of "unfair acts or practices," substituted its own judgment for a private firm's decisions as to how to design its product to satisfy as many users as possible. In my opinion, the consent order basically required Apple to revamp an otherwise indisputably legitimate business practice.

Given the apparent benefits to some consumers and to competition from Apple's allegedly unfair practices, I strongly believe that the Commission should have conducted a much more robust analysis to determine whether the injury to this small group of consumers justified the finding of unfairness and the imposition of a remedy. More generally, as an economist, I strongly believe in the implementation of thorough cost-benefit analyses across many areas of the agency's consumer protection mission, but particularly when the agency uses its unfairness authority, calculates civil penalties, or makes policy recommendations. To that end, it has been one of my priorities to engage the Bureau of Economics in evaluating these matters. As I have mentioned in other contexts,[4] the unique composition of the agency – housing the Bureaus of Competition, Consumer Protection, and Economics – facilitates informed and well-reasoned decision making. I have used my economics background to help identify

[4] Joshua D. Wright, Commissioner, Fed. Trade Comm'n, Remarks at The Economics of Access to Civil Justice: Consumer Law, Mass Torts and Class Actions (Mar. 16, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/293621/140316civiljustice-wright.pdf.

additional areas where the Bureau of Economics can use its expertise to assist the Commission in carrying out its mission to protect consumers.

Data Security and Privacy – Mobile Applications and Devices

With respect to other recent law enforcement efforts, some of our most interesting and cutting-edge work has been in the examination of the privacy and data security aspects of mobile applications and devices. Last week the Commission announced a settlement with Snapchat, a company that markets a popular mobile app that allows consumers to send and receive photo and video messages known as "snaps."[5] The Commission's action in this case illustrates a straightforward use of our deception authority under Section 5 of the FTC Act to challenge both privacy and data security practices.[6]

Snapchat represented that its app provided a private, short-lived messaging service and claimed that once the consumer-set timer for a viewed snap expired, the snap disappeared forever. The agency's complaint, however, alleged that Snapchat violated Section 5 by misrepresenting the disappearing nature of messages sent through its app. Due to a variety of technical workarounds, the photos and videos did not

[5] Press Release, Fed. Trade Comm'n, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 8, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

[6] An act or practice is deemed deceptive "if there is a misrepresentation, omission, or other practice, that misleads the consumer acting reasonably in the circumstances, to the consumer's detriment." FTC Policy Statement on Deception (1983), *appended* to Final Order, Cliffdale Assocs., Inc. 103 F.T.C. 110, 174 (1984), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

necessarily disappear forever. Although Snapchat became aware of this problem, they continued to misrepresent to consumers that the photos and videos would disappear.

The complaint also alleged that Snapchat misrepresented the amount of personal information that its app would collect through its "Find Friends" function – a feature that allows consumers to find and communicate with friends who use the Snapchat service. Because of the way the user interface worked, there was a clear implication that it only collected the user's mobile phone number to provide this service. However, unbeknownst to users, this feature collected the names and phone numbers of all contacts in a user's mobile device address book. Furthermore, the Commission's complaint alleged that Snapchat misrepresented that it would not collect geolocation information when, in fact, it did.

On the data security front, the complaint charged that despite representing that it "employ[ed] the best security practices," Snapchat failed to provide adequate security.[7] For example, many consumers complained that they had sent snaps to someone under the false impression that they were communicating with a friend. Because Snapchat failed to verify users' phone numbers during registration, these consumers were actually sending their personal snaps to complete strangers who had registered with phone numbers that did not belong to them. Moreover, because of failures in how

[7] Complaint, Snapchat, F.T.C. File no. 1323078, 8 (May 8, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf.

Snapchat implemented its Find Friends feature, hackers were able to compile a database of 4.6 million Snapchat usernames and phone numbers, which could have subjected consumers to costly spam, phishing and other unsolicited communications.

In March, the FTC announced that two companies – Fandango and Credit Karma – agreed to settle charges that they misrepresented the security of their mobile apps when they failed to secure the transmission of millions of consumers' sensitive personal information from their mobile apps.[8] The Fandango Movies app for iOS allows consumers to purchase movie tickets and view show times, trailers, and reviews while the Credit Karma Mobile app for iOS and Android allows consumers to monitor and evaluate their credit and financial status. Both of these cases alleged the same misstep – in designing their mobile apps, both Fandango and Credit Karma disabled a critical default process, known as Secure Sockets Layer (SSL) certificate validation.[9]

By overriding the default validation process, Fandango undermined the security of ticket purchases made through its iOS app, exposing consumers' credit card details,

---

[8] In the Matter of Fandango, LLC, F.T.C. File No. 1323089 (Mar. 28, 2014); In the Matter of Credit Karma, F.T.C. File No. 1323091 (Mar. 28, 2014). *See also*, Press Release, Fed. Trade Comm'n, Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Failing to Securely Transmit Sensitive Personal Information (Mar. 28, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers.

[9] To help secure sensitive transactions, mobile operating systems, including iOS and Android, provide app developers with tools to implement the industry standard SSL. If properly implemented, SSL secures an app's communications and ensures that an attacker cannot intercept the sensitive personal information a consumer submits through an app. Instead, the companies' disabling of SSL left their apps vulnerable to "man-in-the-middle" attacks, which allow a third party to intercept any of the information the apps sent or received. This type of attack is especially dangerous on unsecured public Wi-Fi networks at coffee shops, airports and shopping centers, where these apps were intended to be used.

including card number, security code, zip code, and expiration date, as well as consumers' email addresses and passwords. Similarly, Credit Karma's apps for iOS and Android exposed consumers' Social Security Numbers, names, dates of birth, home addresses, phone numbers, email addresses and passwords, credit scores, and other credit report details such as account names and balances.

As with Snapchat, the Commission's enforcement action was based on deception – although Fandango and Credit Karma had assured consumers that they were handling their information securely,[10] both companies failed to perform the basic and widely-available security checks that would have caught the vulnerability.[11]

Before I leave the topic of law enforcement, I just want to briefly mention the use of our unfairness authority in data security cases. In implementing its unfairness authority, the Commission recognizes that in deeming an act or practice as "unfair" it must undertake a cost-benefit analysis[12] – I believe that the proper approach is for the Commission to consider the security deficiencies at issue, the resultant harm to

[10] The Fandango app assured consumers during checkout that their credit card information was stored and transmitted securely. Likewise, Credit Karma assured consumers that the company followed industry-leading security precautions, including the use of SSL to secure their information.
[11] Even after a user warned Credit Karma about the vulnerability in its iOS app, the company failed to test its Android app before launch. As a result, one month after receiving a warning about the issue, the company released its Android app with the very same vulnerability. In addition, Fandango failed to have an adequate process for receiving vulnerability reports from security researchers and other third parties, and as a result, missed opportunities to fix the vulnerability.
[12] FTC Policy Statement on Unfairness (1980), *appended* to Final Order, Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), *available at* http://ftc.gov/bcp/policystmt/ad-unfair.htm.

consumers, if any, and whether there were low-cost steps that would significantly reduce the risk.[13]

The *HTC America* case brought by the Commission in February 2013 illustrates this concept.[14] The Commission charged that mobile device manufacturer HTC failed to employ reasonable and appropriate security practices in the design and customization of the software it developed for its smartphones and tablet computers, introducing security flaws that placed sensitive information about millions of consumers at risk. Among other things, the complaint alleged that HTC failed to provide its engineering staff with adequate security training, failed to review or test the software on its mobile devices for potential security vulnerabilities, failed to follow well-known and commonly accepted secure coding practices, and failed to establish a process for receiving and addressing vulnerability reports from third parties.[15]

Importantly, the unfairness analysis in *HTC America* balanced the gravity and likelihood of risk to consumers against the costs of implementing security measures that would have decreased those risks.

---

[13] *See* J. Howard Beales, III & Timothy J. Muris, Choice or Consequences: Protecting Privacy in Commercial Information, 75 U. CHI. L. REV. 132 (2008).

[14] In the Matter of HTC America, F.T.C. File No. 1223049 (Feb. 22, 2013).

[15] While these failures sound remarkably similar to the charges plead against Fandango and Credit Karma, in the *HTC America* case, the Commission used its Section 5 unfairness authority, in addition to its deception authority, to pursue an enforcement action against HTC for its security shortcomings. Although HTC did make some representations about security in its user manuals for its Android-based mobile devices, these representations did not cover all of the conduct, or all of the devices at issue.

Data Security and Breach Notification Legislation

As you might gather from my overview of the Commission's data security and privacy enforcement actions, this is a critical area with respect to the agency's consumer protection activities. Accordingly, in recent testimony on the Hill, the Commission has reiterated its longstanding call for enactment of "a strong federal data security and breach notification law."[16] The Commission has also recommended that any such legislation could "supplement the agency's existing data security authority by authorizing the Commission to seek civil penalties in appropriate circumstances."[17]

The real question, of course, is what would any such legislation look like? I see from the agenda that your afternoon will probably be devoted, at least in part, to discussing this very issue. To get a sense of the Commission's viewpoint on what proposed legislation should take into consideration, I think a good starting point is to recognize that our past law enforcement work has helped inform the discussion.

For example, in conjunction with settling our 50th data security case, the Commission issued a statement in January setting forth some of the guiding principles behind our data security program. As that statement recognized, the touchstone of the agency's approach to data security is reasonableness: a company's data security

[16] Prepared Statement of the Federal Trade Commission on Emerging Threats in the Online Advertising Industry Before the Committee on Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations, United States Senate, 13 (May 15, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/309891/140515emergingthreatsonline.pdf [hereinafter *Homeland Security Testimony*].

[17] *Id.* at 14.

measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.[18]

The Commission's testimony on data security has mirrored these concepts: despite the threats posed by data breaches, many companies continue to underinvest in data security. By way of example, many of the agency's settlements have shown that some companies fail to take even the most basic security precautions.[19]

From my perspective, and speaking only for myself, I find this articulation to be a fine starting point. However, as you would imagine, I believe that it is just that – and before any specific recommendations can be endorsed, I would need to look carefully at the costs and benefits of the proposals.

The Internet of Things, Big Data, and Data Brokers

I would like to conclude my remarks today by spending a few minutes on the topic of "Big Data." For purposes of this discussion, I am going to include within Big Data, the issue of data brokers and the general concept of the Internet of Things. As you are probably already aware, this is another area in which the Commission has taken great interest.

---

[18] Commission Statement Marking the Commission's 50th Data Security Settlement (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[19] *Homeland Security Testimony*, *supra* note 16, at 12.

As general matter, the Commission began looking at issues related to data collection about two decades ago. Most of that early work was related to the Fair Credit Reporting Act, but with the advent of the Internet, the Commission's focus on data collection and use has shifted to a broader view. In order to stay informed and abreast of the latest developments, the Commission regularly conducts workshops and conferences. For example, in December 2012, the agency hosted a workshop, entitled The Big Picture: Comprehensive Online Data Collection, to explore the practices and privacy implications of comprehensive collection of data about consumers' online activities.[20] In December 2012, the Commission initiated a study of data broker practices by issuing 6(b) Orders to nine data brokers seeking information about their information collection and use practices.[21] This upcoming September, the Commission will examine the potential effects of "Big Data" on American consumers at a workshop entitled, Big Data: A Tool for Inclusion or Exclusion?[22]

With regard to policy development, this is an area that I think can really benefit from the rigorous study of consumer preferences, behavior, and potential risks. These

---

[20] *See* Press Release, Fed. Trade Comm'n, FTC to Host Workshop to Explore Practices and Privacy Implications of Comprehensive Collection of Internet Users Data (Oct. 15, 2012), *available at* http://www.ftc.gov/news-events/press-releases/2012/10/ftc-host-workshop-explore-practices-privacy-implications.

[21] Press Release, Fed. Trade Comm'n, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), *available at* http://www.ftc.gov/news-events/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data.

[22] Press Release, Fed. Trade Comm'n, FTC to Examine Effects of Big Data on Low Income and Underserved Consumers at September Workshop (Apr. 11, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/04/ftc-examine-effects-big-data-low-income-underserved-consumers.

factors should be evaluated within the traditional cost-benefit analysis. I believe it is critical to understand the potential outcome of any proposed course of action to "protect consumers" before making specific recommendations.

By way of example, in enacting statutes such as the Fair Credit Reporting Act, Congress undertook efforts to balance the benefits of information collection and sharing (fair and accurate credit reporting is beneficial to both businesses and consumers) against the costs of such information collection and sharing (potential risks to confidentiality, accuracy, relevancy and appropriate use). In doing so, Congress carefully articulated the types of information to be protected, limited the use and access to such information, and provided certain consumer protections relating to the accuracy of and the ability to dispute and correct such information. I would be wary of extending FCRA-like coverage to other uses and categories of information without a robust balancing of the benefits and costs associated with such requirements.

Thank you very much for your time. I am happy to take some questions.