Bloomberg BNA

Electronic Commerce & Law Report™

VOL. 19, NO. 26 JULY 2, 2014

MOBILE DEVICES

The authors review the Federal Trade Commission's increasing watchfulness over the development of mobile applications from the perspective of consumer data security. They also discuss the impact of the U.S. District Court for the District of New Jersey's decision in *FTC v. Wyndham Worldwide Corp.*, and offer insights on the practical implications for businesses.

Mobile Application Development: The Next Frontier for Government Compliance

BY SETH NORTHROP AND LI ZHU

Mobility is rapidly evolving into a requirement, rather than a luxury, for both mature and emerging companies. Today, consumers expect their personal electronic devices to provide "anytime—anywhere computing" that allows for easy consumption and creation of digital content across different platforms. It is not surprising that global shipments for tablet computers nearly doubled between 2012 and 2013, while shipments for traditional personal computers ("PCs") declined by more than ten percent.[1] All signs indicate that mobile devices, such as tablets and smartphones, are the future of personal computing.

The popularity of mobile devices has created a new market for software designed specifically to run on those devices. These mobile applications, known colloquially as "apps," have become the official channel to drive content and services to consumers. Mobile application downloads are forecasted to approach nearly 268 billion by 2017, corresponding to more than $77 billion in revenue.[2] By then, users are predicted to funnel their personal data to more than 100 applications and services every day, which will track what users say, what they do, and where they go. Nor will data be confined to mobile devices, as applications become integrated in other technologies, such as wearable electronics, home appliances, and even cars. As technology develops, a person's data will be increasingly exposed and exchanged as a commodity on the open market.

To date, mobile application development has largely taken place within the "wild west"—anyone with a computer could, and often did, create his or her own applications. Regulatory scrutiny has increased in response to the whirlwind of activity and the extensive and often commonplace collection of personal data. As companies continue to venture into mobile application development, proper government compliance will require them to keep a close eye on regulatory developments.

[1] GARTNER NEWSROOM, GARTNER SAYS WORLDWIDE PC, TABLET AND MOBILE PHONE SHIPMENTS TO GROW 5.9 PERCENT IN 2013 AS ANYTIME-ANYWHERE COMPUTING DRIVES BUYER BEHAVIOR (June 24, 2013), available at http://www.gartner.com/newsroom/id/2525515.

Seth Northrop and Li Zhu are trial attorneys at Robins, Kaplan, Miller & Ciresi LLP, Minneapolis. They are part of the firm's Global Business and Technology Sourcing practice group, and focus their practices primarily on large-scale disputes involving a variety of technologies.

[2] GARTNER NEWSROOM, *Gartner Says by 2017, Mobile Users Will Provide Personalized Data Streams to More Than 100 Apps and Services Every Day* (Jan. 22, 2014), available at http://www.gartner.com/newsroom/id/2654115.

 ISSN 1098-5190

I. The Federal Trade Commission's Role in Regulating Data Security

The Federal Trade Commission ("FTC") has broad authority to protect consumers from harmful business practices.[3] In recent years, the FTC has increasingly asserted that authority in the context of mobile application developments in two ways. First, it began offering practical recommendations designed to guide companies through the collection of personal data; and second, it has started to initiate enforcement actions where it views application developers have overstepped.

The FTC recently offered tips to mobile application developers about security issues that may expose such information. Because consumer data may be "vulnerable to digital snoops, data breaches, and real-world thieves," the FTC expects application developers to "adopt and maintain reasonable data security practices" for protecting consumer information.[4] The FTC cautioned developers against using a "one-size-fits-all approach" because "[s]ecurity threats and best practices evolve quickly."

The FTC will, however, sometimes take matters into its own hands if its advice goes unheeded. The Federal Trade Commission Act ("FTC Act") prohibits "unfair or deceptive acts or practices in or affecting commerce," and empowers the FTC to enforce the FTC Act. 15 U.S.C. § 45(a). The FTC Act defines "unfair acts or practices" as those that cause or are likely to cause "substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). The FTC is empowered to enforce this prohibition using administrative remedies (in a trial-type proceeding before an administrative law judge) and/or judicial remedies (in a federal court by seeking civil penalties and/or injunctive relief). 15 U.S.C. § 45(b) and 53(b).

The FTC recently cracked down on a number of companies, including those who merely failed to invest the necessary time and resources to secure customer data, even though such inaction was arguably neither "unfair" nor "deceptive."[5] In January 2014 alone, the FTC settled privacy claims with multiple companies claiming to comply with international data privacy standards.[6] The FTC has since resolved actions against others, such as Fandango and Credit Karma, for failing to secure data transmitted through their mobile applications.[7] The FTC has also targeted companies for failing to follow their own published data security policies. For example, the FTC recently settled with Snapchat over allegations that messages sent through Snapchat's application did not disappear as easily as promised.[8] Compliance with advertised security policies is especially relevant to companies doing business in states such as California, where state laws (such as the California Online Privacy Protection Act or "CalOPPA") require businesses that collect personally identifiable information online, to disclose their privacy policies.

Most recently, the FTC has shown that it will require companies to have reasonable data protection policies in place. Failure to secure such data, according to the FTC, is an "unfair" practice under the FTC Act. By way of example, on April 7, 2014, the United States District Court for the District of New Jersey considered and approved that the FTC's authority under the FTC Act extends to the regulation of data security. *FTC v. Wyndham Worldwide Corp.*, 2014 BL 94785, Civil Action No. 13-1887 (ES) (D.N.J. April 7, 2014) (rejecting defendants' attempt to carve out a data-security exception to the FTC Act in its motion to dismiss). In *Wyndham*, the FTC charged the defendant hospitality businesses with failing to properly secure personal information collected from hotel customers, which allegedly allowed intruders to gain unauthorized access—on three separate occasions—to payment card information from more than 619,000 customer accounts. *Id.* The FTC argued that the defendants failed to employ a number of "commonly-used" and "readily available" data security measures. *Id.*

Once the FTC has a company in its crosshairs, that company is often forced to expend significant resources in the form of compliance costs or even legal fees. For example, the company may be asked to overhaul its data security policies and practices, notify affected customers, hire third-party auditors, and/or subject itself to

---

[3] Nangia, *Caution: your company's biggest privacy threat is ... the FTC*, LEXOLOGY (Apr. 1, 2014), available at http://www.lexology.com/library/detail.aspx?g=0627e8a0-b9c2-4cef-84d0-cf20b272ed91.

[4] Federal Trade Commission, Bureau of Consumer Protection, *Mobile App Developers: Start with Security* (Feb. 2013), available at http://www.business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

[5] Nangia, *supra* note 3. The legislative history reveals, however, that businesses may be guilty of deception if they fail to "follow their stated information practices" as provided on their websites, *Wyndham* (citing Hearing before H. Comm. on Commerce, Subcomm. on Telecomm., 105th Cong., at n.23 (July 21, 1998)).

[6] Federal Trade Commission, *FTC Settles with Twelve Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework* (Jan. 21, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply.

[7] Federal Trade Commission, *Fandango, Credit Karma Settle FTC Charges that They Deceived Customers By Failing to Securely Transmit Sensitive Personal Information: Mobile Apps Placed Credit Card Details, Credit Report Data, Social Security Numbers at Risk* (Mar. 28, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers.

[8] Wortham, *Off the Record in a Chat App? Don't Be Sure*, NEW YORK TIMES (May 8, 2014), available at http://www.nytimes.com/2014/05/09/technology/snapchat-reaches-settlement-with-federal-trade-commission.html?_r=2&utm_content=buffer14fa3&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer.

  ECLR ISSN 1098-5190

continual FTC oversight for twenty years. Further, customers exposed by data security breaches may seek relief on their own in the form of expensive, class action lawsuits. Thus, the recent developments discussed above, among others, present a unique challenge for companies collecting customer information in the digital age.

II. Practical Implications for Businesses

Companies can implement a number of best practices to prevent running afoul of the FTC. First, an organization should review its data collection policies and practices and ask the following questions:

- Is consumer data collected in an efficient way?
- Is consumer data collected in a transparent fashion, with notice provided to the consumer?
- Is consumer data anonymized and periodically wiped to minimize damage if there is an unexpected breach?
- Are there strict standards governing the disclosure of information to third parties?

Importantly, the organization must follow its own data security policy, or risk the FTC characterizing its conduct as "unfair" or "deceptive."

Second, an organization should update its security infrastructure to include "commonly-used" and "readily available" data security measures, such as:

- Implementing restrictions requiring that consumers use complex passwords;
- Preventing servers from using commonly-known default user IDs and passwords;
- Setting up basic firewalls;
- Maintaining a proper inventory of its computers;
- Encrypting highly-sensitive data, such as payment card information, in a form that is not "clear readable text";
- Ensuring that any and all subsidiaries of the organization implement adequate information security policies and procedures before connecting them to the main network;
- Installing updates and security patches for server operating systems;
- Monitoring the network for malware used in previous intrusions; and
- Restricting third-party access to the network. *Id.*

Third, the organization should be aware of industry-specific privacy regulations. For example, organizations providing mobile applications or online services that may be used by children under thirteen, must comply with the Children's Online Privacy Protection Act ("COPPA"). COPPA requires that the organization provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children.[9] The organization must maintain the confidentiality and security of a child's information, and retain the information only as long as is necessary to fulfill the purpose for which it was collected. Other industries such as banking, health care, and education face their own collection of specialized data privacy regulations.

III. Conclusion

The federal court in *Wyndham* acknowledged that "we live in a digital age that is rapidly evolving—and one in which maintaining privacy is, perhaps, an ongoing struggle" that "raises a variety of thorny legal issues that Congress and the courts will continue to grapple with for the foreseeable future." Despite the changing landscape, companies can prepare for the unknown by thinking proactively about data security, and subsequently updating and adhering to best practices. The alternative may, unfortunately, be a costly visit from the FTC.

---

[9] Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions* (revised Apr. 2014), available at http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions#General%20Questions.