Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

EYE ON PRIVACY

JANUARY 2014

Welcome

Welcome to a new year of exciting privacy developments! In this month's issue of *Eye on Privacy,* we recap some significant developments from the end of last year, including an FTC settlement with an app developer that could impact how the collection and sharing of geolocation information from mobile users needs to be disclosed, a separate FTC settlement with a rent-to-own company accused of enabling computer spying by franchisees, Apple's successful dismissal of an iPhone app class action, and the FTC's first settlement in a mobile "cramming" case. We also take a look at recent studies of the "data broker" industry released by the Government Accountability Office and the Senate Commerce Committee, and examine how developments in this area could end up affecting a broad range of companies that would never consider themselves to be data brokers.

As always, please feel free to e-mail us at PrivacyAlerts@wsgr.com if there are any future topics you'd like to see here.

Lydia Parnes
Partner, Washington, D.C.
lparnes@wsgr.com

FTC Settlement with Flashlight App Requires Extensive Disclosures Outside of the Privacy Policy to Collect and Share Geolocation Information

Tracy Shapiro
Of Counsel, San Francisco
tshapiro@wsgr.com

Michael Wolk
Associate, Palo Alto
mwolk@wsgr.com

The Federal Trade Commission (FTC) announced on December 5, 2013, that Goldenshores Technologies, LLC and its managing member, Erik M. Geidl, agreed to a proposed settlement over claims that Goldenshores, through its "Brightest Flashlight Free" mobile application, violated Section 5(a) of the FTC Act prohibiting unfair or deceptive acts and practices affecting commerce by failing to disclose that the app transmitted user data, including precise geolocation information and persistent identifiers, to third parties such as advertising networks. Under the settlement, Goldenshores must provide just-in-time disclosures outside of the privacy policy and obtain affirmative express consent from users before collecting, using, or disclosing geolocation information. The settlement agreement (referred to here as "the order") was subject to public comment through January 6, 2014. The FTC will now decide whether to reach a final settlement with Goldenshores.

Background

The "Brightest Flashlight Free" is a flashlight app that, according to the FTC, has been listed as a top free application in the Google Play application store and has been downloaded tens of millions of times. The core of the FTC's complaint is that Goldenshores told users that the app would

Continued on page 2...

In This Issue

collect data from their mobile devices, but failed to tell them that the app also transmits such data to various third parties, including advertising networks. According to the FTC, the app transmitted precise geolocation information along with persistent device identifiers that could be used to track a user's location over time—data that the FTC has long categorized as sensitive. The FTC also identified as a law violation the fact that the app gave the illusion of providing a choice regarding data collection, but continued to collect data regardless of the user's selection.

FTC Complaint and Proposed Order

The FTC's complaint asserts that Goldenshores told users in its privacy policy and end-user license agreement (EULA) that the app would collect certain user data, but both of those documents failed to disclose that the app would transmit precise geolocation information and persistent device identifiers to third parties. The failure to disclose this information was deceptive, according to the FTC. It is noteworthy that the FTC did not identify, as a basis for the complaint's deception count, a specific misrepresentation that Goldenshores made to users. Rather, the complaint alleges that the failure to disclose that the app transmits data to third parties—in light of the fact that it told users the app itself would collect user data—is deceptive. The complaint also describes how the app purported to give users the option to "accept" or "refuse" the EULA by selecting the appropriate button, but the app collected information prior to the user making a selection and regardless of the user's choice to accept or reject the EULA. The FTC asserts that creating the impression that users have the option to refuse the terms of the EULA, including terms regarding the collection and use of device data, when users cannot actually prevent the app from collecting their device data is false or misleading. As a part of the settlement, Goldenshores agreed not to collect or transmit geolocation information via mobile applications without clearly and prominently providing a just-in-time notice to users (i.e., immediately prior to the collection of such information, and separate from other documents such as end-user license agreements, privacy policies, and terms of use) and obtaining users' affirmative express consent prior to the collection or transmission of such information. The just-in-time notice must disclose:

1) that such application collects or transmits geolocation information;

2) how geolocation information may be used;

3) why such application is accessing geolocation information; and

4) the identity or specific categories of third parties that receive geolocation information from such application.

Curiously, Goldenshores agreed to delete all information, including persistent identifiers, IP addresses, and precise geolocation data, that the app collected from users, despite the fact that the FTC did not allege that Goldenshores improperly collected such data. The order does not address the user data improperly sent to third parties. Goldenshores also agreed, as is customary in FTC orders, not to engage in future misrepresentations regarding the collection, use, or disclosure of user information.

Implications

The FTC has long supported the principle that companies should provide "just-in-time disclosures" to users and obtain their affirmative express consent before accessing precise geolocation information. The FTC called for such enhanced notice and consent in both its 2012 report on privacy, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Privacy Report) and its 2013 report on mobile privacy, *Mobile Privacy Disclosures: Building Trust Through Transparency*. Including this standard in the order continues an FTC trend of modeling order provisions after policy positions the FTC adopted in the Privacy Report. Complying with the order may require Goldenshores to make enhanced disclosures outside of the mobile device operating system permissions, because the operating system permissions may not accommodate the level of detail that the FTC has prescribed regarding the collection, use, and sharing of geolocation information. Consent orders are legally binding only on the respondent, and arguably this provision constitutes "fencing-in relief" (i.e., conduct prohibitions that exceed the conduct alleged to have violated the FTC Act, which the FTC asserts are necessary to ensure that respondents' activities remain "fenced in" the confines of the law). As such, a company's failure to follow this standard does not necessarily constitute a law violation. But FTC consent orders often have the consequence of setting precedent for industry.

The FTC's complaint allegation regarding the collection and transmission of information prior to the time that users are given the opportunity to consent to those practices is particularly relevant to app developers. The initial user experience when an app is opened for the first time can be critical, as some users may elect to delete and never again download an app based on their first impressions. As a result, developers often are faced with the challenge of balancing the presentation of legal disclosures and choice mechanisms with their desire to create a user on-boarding experience that minimizes new-user attrition. This proposed settlement underscores the importance of providing disclosures and obtaining consent at the right time.

GAO and Senate Commerce Committee Release Studies Calling for Increased Oversight and Regulation of "Data Broker" Industry

Emily Schlesinger
Associate, Seattle
eschlesinger@wsgr.com

Edward Holman
Associate, Washington, D.C.
eholman@wsgr.com

In recent years, data-driven marketing has spread across numerous sectors of the economy. While the industry provides many benefits and conveniences for consumers by lowering the cost of products and services and helping businesses better capture customer preferences, privacy advocates and legislators are pushing for increased government regulation over companies known broadly as "data brokers."

As a result of the increased interest in additional regulation, in November 2013, the U.S. Government Accountability Office (GAO) released a detailed report about the data broker industry at the request of Senator Jay D. Rockefeller (D-WV), chairman of the Senate Committee on Commerce, Science, and Transportation (the Commerce Committee). The Commerce Committee released its own report about one month later. These reports, both the product of long-running investigations into the policies and practices of companies involved in online and offline marketing and data collection, provide important insights into the potential challenges facing the industry.

Government Accountability Office Study

On November 15, 2013, the GAO released a study following a year-long investigation of existing federal laws and regulations and several state laws applicable to "data brokers" (also known as "information resellers"),[1] which were broadly defined as "companies that collect and resell information on individuals."[2] The GAO also interviewed representatives of federal agencies, trade associations, consumer and privacy groups, and industry businesses, and reviewed the many approaches advocated to improve consumer data privacy, which range from new legislation to greater self-regulation.[3]

The GAO report identified what it perceived as gaps in the current statutory privacy framework that, in the office's opinion, did not fully address changing technology and marketplace practices, including online tracking, mobile applications, location tracking, and mobile payments. The report also maintained that current law is not aligned with "fair information practice principles" (FIPPs),[4] the principles commonly advocated as a baseline for handling consumer data.

The GAO called for Congress to strengthen the current consumer privacy framework, and recommended focusing on the following issues:

- the adequacy of consumers' ability to access, correct, and control their personal information in circumstances beyond those currently accorded under the Fair Credit Reporting Act (FCRA);
- whether there should be additional controls on the types of personal or sensitive information that may be collected and shared;
- whether changes should be made to the permitted sources and methods for data collection; and
- what privacy controls should be imposed related to new technologies, such as web tracking and mobile devices.[5]

The GAO report identified what it perceived as gaps in the current statutory privacy framework that, in the office's opinion, did not fully address changing technology and marketplace practices, including online tracking, mobile applications, location tracking, and mobile payments

[1] U.S. Government Accountability Office, "Report to the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate: Information Resellers—Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace" (Sept. 25, 2013) (hereinafter "GAO report"), *available at* http://www.gao.gov/assets/660/659769.pdf (last visited Dec. 20, 2013).
[2] GAO report, *supra* note 1 at 1.
[3] *See id.* at 2; *see id.*, Appendix I at 48-51.
[4] *See id.* at 46. Rooted in a 1973 report by the United States Department of Health, Education and Welfare, FIPPs are at the core of the Privacy Act of 1974 and are regularly incorporated into government and business privacy policies. FIPPs include the following core principles: transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing. *See* National Strategy for Trusted Identities in Cyberspace, "Fair Information Practice Principles (FIPPs)," *available at* http://www.nist.gov/nstic/NSTIC-FIPPs.pdf (last visited Dec. 20, 2013).
[5] GAO report, *supra* note 1 at 19, 46-47.

Continued on page 4...

GAO and Senate Commerce Committee . . . *(continued from page 3)*

Notably, the report took no position on how this new legislation should look. It merely presented the pros and cons of enacting a comprehensive, federal-based privacy-law regime to replace the current sector-specific regulations,[6] and noted the challenge of allowing consumer privacy protections without inhibiting commerce.[7]

Senate Commerce Committee Report

About one month later, on December 18, 2013, the Senate Commerce Committee issued its own report on data brokers.[8] This report was released just hours before a Commerce Committee hearing on the same issue.[9]

The Commerce Committee sought answers to the following four questions:

1) What data about consumers does the data broker industry collect?

2) How specific is the data?

3) How does the data broker industry obtain consumer data?

4) Who buys the data, and how is it used?[10]

The Commerce Committee report adopted a broad definition of "data broker" developed by the Federal Trade Commission (FTC): "[c]ompanies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud."[11] This description, however, leaves significant room for interpretation.[12]

Like the GAO, the Commerce Committee concluded that "[c]urrent federal law does not fully address the use of new technologies"[13] or the incredible increase in the sale and availability of consumer information in the digital age. The report opined that although the FCRA, Health Insurance Portability and Accountability Act (HIPAA), and several other laws protect consumers in certain sector-specific contexts, the tremendous changes in the digital age have left a large gray area unregulated. Furthermore, the committee was highly critical of data brokers, drawing the following broad conclusions about their practices: "(1) Data brokers collect a huge volume of detailed information on hundreds of millions of consumers; (2) Data broker products provide information about consumer offline behavior to tailor online outreach by marketers; and (3) Data brokers operate behind a veil of secrecy."[14]

Like the GAO, the Commerce Committee concluded that "[c]urrent federal law does not fully address the use of new technologies" or the incredible increase in the sale and availability of consumer information in the digital age

This disapproving tone echoed throughout the December 18, 2013, Commerce Committee hearing. Senator Rockefeller had many harsh words for common industry practices, and other committee members gave examples of what they deemed "predatory" marketing activities conducted by financial firms or other companies targeting vulnerable groups such as the impoverished or immigrant populations. They also raised concerns about the practice of scoring individuals based on algorithmic data analysis and serving them with tailored offers based on prior web behavior or demographic data, emphasizing their fears of dynamic pricing.

In response, industry representatives highlighted that data brokers' efforts lower the costs of products and services for consumers, while helping businesses focus on tailoring their offerings to consumer needs—not to mention contributing $156 billion to the American economy. In fact, in recent years, database "profiling" and targeted marketing have become fundamental to the success of almost any business or organization—including the U.S. government itself. These techniques provide crucial tools to ensure the provision of

---

[6] *See generally id.* at 31-34.
[7] *Id.* at 46.
[8] Committee on Commerce, Science, and Transportation—Office of Oversight & Investigations Majority Staff, "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes" (Dec. 18, 2013) (hereinafter "Commerce Committee report"), *available at* http://www.scribd.com/doc/192589947/12-18-13-Senate-Commerce-Committee-Report-on-Data-Broker-Industry (last visited Dec. 19, 2013).
[9] Senate Commerce Committee Hearing, "What Information Do Data Brokers Have on Consumers, and How Do They Use It?" (Dec. 18, 2013), *video archive available at* http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=a5c3a62c-68a6-4735-9d18-916bdbbadf01&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a (last visited Dec. 19, 2013). The hearing panel consisted of the following individuals: Jessica Rich, Director of the FTC's Bureau of Consumer Protection; Pam Dixon, Executive Director of the World Privacy Forum; Dr. Joseph Turow, Professor at the Annenberg School for Communication; Tony Hadley, Senior Vice President of Government Affairs and Public Policy at Experian; and Jerry Cerasale, Senior Vice President of Government Affairs and Public Policy for the Direct Marketing Association.
[10] Commerce Committee report, *supra* note 8 at ii.
[11] *Id.* at 1 (citing Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, at 68 (Mar. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (last visited Dec. 19, 2013)).
[12] *See id.* at 13-21 (describing types of consumer data that brokers collect, maintain, and share); *id.* at 21-28 (describing types of data broker products); *id.* at 28-31 (describing data broker customers).
[13] *Id.* at 10.
[14] *Id.* at ii-iii.

government assistance to those in need, and give important insights into the requests and opinions of constituents. Regardless, rather than being extracted from consumers against their will, the majority of the data being discussed was derived from public records or other publicly available information; in most other cases, customers chose to provide the information directly to businesses by opting into incentive or loyalty-card programs, entering contests, or completing questionnaires.

Importantly, although both the Commerce Committee report and the hearing confirmed the growing divide between the two sides of the debate, neither revealed concrete plans for specific legislation, suggesting only that there must be further fact-finding.

Implications

The perceived gaps in federal and state laws called out in both the GAO report and the Commerce Committee report, as well as the derisive remarks of Senator Rockefeller and others during the recent hearing, suggest that the tension between the data broker industry and its critics will likely grow in the coming months. Moreover, one *crucial* issue has yet to be resolved—the definition of a "data broker." The vague and conclusory descriptions adopted by both the GAO and the Commerce Committee could arguably apply to thousands of different companies since "[e]veryone shares data within the Internet ecosystem."[15] Given the lack of clarity, any company that either collects data or relies upon such collection efforts by others may be impacted by the government's heightened scrutiny in this area.

In December 2012, the FTC opened its own inquiry into the privacy implications of the industry's collection and use of consumer data, the findings of which are expected to be released in early 2014 and may only further muddy the waters.[16] In the past, FTC Commissioner Julie Brill has promoted a "one-stop shop" for consumers to access their information in an effort she has dubbed "Reclaim Your Name";[17] the forthcoming report will probably continue to stress the Commissioner's view that heightened industry regulation is needed.[18] It is also possible that the FTC could propose a legislative recommendation to give itself broader authority over data brokers or call for more self-regulatory efforts.

Given the lack of clarity, any company that either collects data or relies upon such collection efforts by others may be impacted by the government's heightened scrutiny in this area

Whether through comprehensive federal and state legislation or more restrictive self-regulation, one thing is clear—privacy advocates and lawmakers seem intent on imposing a greater degree of regulation on this industry. But until a definitive definition of what constitutes a "data broker" exists, any company involved in the collection and use of consumer data (particularly data obtained from, or provided to, third parties) could feel the effects and should track this issue closely.

---

[15] *See* Testimony of Thomas Hadley, Senior Vice President of Government Affairs and Public Policy at Experian, Committee Hearing, *supra* note 9.

[16] *See* Press Release, *supra* note 10.

[17] Julie Brill, FTC chairman, "Reclaim Your Name—Keynote Address at the 23rd Computers Freedom and Privacy Conference," at 10-11 (June 26, 2013), *transcript available at* http://www.ftc.gov/sites/default/files/documents/public_statements/reclaim-your-name/130626computersfreedom.pdf (last visited Dec. 20, 2013).

[18] In 2012, the FTC published a report calling for greater transparency among data brokers, and asking Congress to give consumers the right to access information these firms hold about them. *See* FTC report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at 30 (Mar. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (last visited Dec. 20, 2013). Although the report covered many different issues, the FTC specifically called on data brokers to increase transparency for consumers by creating a centralized website where they could identify themselves and disclose how they collect and use data, as well as details about the choices that data brokers provide consumers about their own information.

National Rent-to-Own Company Settles FTC Charges of Enabling Computer Spying by Franchisees

Matthew Staples
Associate, Seattle
mstaples@wsgr.com

On October 22, 2013, the Federal Trade Commission (FTC) announced a proposed settlement of a case against Aaron's, Inc., a national rent-to-own retailer with more than 1,800 locations in 48 states, having alleged that Aaron's knowingly played a direct and vital role in its franchisees' installation and use of software on rental computers that secretly monitored consumers.

The FTC alleged, among other things, that the software used by Aaron's franchisees[1] was used on rented computers to surreptitiously track consumers' locations, use computers' webcams to take photographs of consumers inside their homes, take screen shots of computer users' activities on the computers, use false registration screens to collect personal information, and record keystrokes on the computers in order to capture login credentials for email, financial, and social media accounts. In many instances, Aaron's franchisees did not obtain consent from their rental customers and did not disclose to them or the rental computers' users that the software was installed and could be used to track consumers' locations and to remotely spy on their activities.

The FTC brought the enforcement action against Aaron's, a franchisor, despite the alleged violations being committed by its franchisees, for several reasons. According to the FTC:[2]

- Aaron's facilitated its franchisees' installation and use of the software and provided its franchisees with the technical capacity to access and use the software. To use and activate the software, franchisees were required to obtain corporate email accounts provided by Aaron's. Email messages were routed through Aaron's corporate headquarters and stored on servers owned, controlled, and maintained by Aaron's. Aaron's also gave franchisees instructions on how to install and use the software, and in many instances gave franchisees permission to access the software vendor's website using Aaron's network.
- Aaron's senior management and personnel responsible for the franchisees knew that the franchisees were using the spying software without notifying consumers.
- Aaron's IT personnel were aware that the company's server space was being used to store email messages sent using the software, as well as of the contents of those email messages.

> The FTC alleged that the actions of Aaron's in permitting and participating in the gathering and storage of private and confidential information about consumers caused or was likely to cause substantial harm to consumers

The FTC alleged that the actions of Aaron's in permitting and participating in the gathering and storage of private and confidential information about consumers caused or was likely to cause substantial harm to consumers, and that this injury could not reasonably be avoided and was not outweighed by countervailing benefits to consumers or competition. Accordingly, the FTC alleged that the company's practices constituted unfair acts or practices in violation of Section 5 of the FTC Act.

Settlement

Aaron's agreed to the terms of a proposed settlement, including numerous remedies. As part of the proposed settlement, which would remain in effect for at least 20 years, Aaron's must:

- not use monitoring technology on computers rented to consumers to collect data from or about consumers (other than with notice to and consent from a consumer, or in connection with a request for technical support initiated by a consumer, where Aaron's uses the data for no other purpose);[3]
- not use geolocation tracking technology in any rented consumer product without providing clear and prominent notice to, and obtaining affirmative consent from, the consumer at the time the product is rented, including the installation of a clear and prominent icon on the computer on which the technology is installed that, when clicked, provides specified categories of disclosures about the geophysical location tracking

[1] The software was the subject of related FTC actions earlier in 2013 against the software's manufacturer, Designerware LLC, as well as several rent-to-own stores, including Aaron's franchisees, that used it. Information regarding those related FTC actions is available at http://www.ftc.gov/news-events/press-releases/2013/04/ftc-approves-final-order-settling-charges-against-software-and.
[2] The FTC's complaint against Aaron's is available at http://www.ftc.gov/sites/default/files/documents/cases/131022aaronscmpt.pdf.
[3] These, along with most obligations in the settlement, are limited to the actions of Aaron's and its franchisees in connection with "covered rent-to-own transactions," defined as any transaction where a consumer enters into an agreement for the purchase or rental of any consumer product where the consumer's contract or rental agreement provides for payments over time with options to purchase the product.

technology and how collected information is used and disclosed (with exceptions only for (i) activating monitoring technology in response to the potential theft of a rented item, and (ii) in connection with a request for technical support initiated by a consumer, where Aaron's uses the data for no other purpose);

- refrain from engaging in any false representations to consumers or deception regarding the collection of personal information through a rented computer by way of any notice, prompt screen, or other software application appearing on the screen of any computer;

- refrain from any misrepresentations regarding the extent to which Aaron's maintains and protects the security, privacy, or confidentiality of any data or information from or about a consumer;

- not use data gathered by practices prohibited by the settlement to collect consumer debts;

- delete or destroy data collected using practices prohibited by the settlement;

- require its franchisees to refrain from using, and to destroy, any data collected using methods that do not comply with the settlement;

- prohibit its franchisees from engaging in various other actions that would be inconsistent with those practices Aaron's agreed to abstain from in the settlement, and to monitor and enforce franchisees' compliance; and

- engage in related recordkeeping, reporting, and notification obligations.

Implications

The Aaron's settlement has significant implications. First, it illustrates the need for companies that use technologies that monitor consumers' activities, including those that capture geolocation information, to evaluate carefully the means by which they notify affected consumers of their practices and obtain consent.

Second, the settlement has significant implications for franchisors, franchisees, and others doing business under similar arrangements. The FTC did not allege that Aaron's itself used the accused software in any of its company-owned stores, and it appears that no such use occurred. The company's practices still were challenged, though, due to it knowing about its franchisees' practices and, in some cases, facilitating those franchisees' use of the invasive technology. The FTC's pursuit of Aaron's in these circumstances, along with the settlement obligating Aaron's to engage in monitoring and oversight of its franchisees, may be instructive for franchisors and similarly situated companies.

The settlement has significant implications for franchisors, franchisees, and others doing business under similar arrangements. The FTC did not allege that Aaron's itself used the accused software in any of its company-owned stores, and it appears that no such use occurred.

Aaron's and certain of its franchisees also face multiple putative class action lawsuits in numerous jurisdictions relating to the conduct challenged by the FTC. These lawsuits, pending as of this writing, further underscore the potential risks presented by such conduct.

Tip

"Do Not Track" Signals – Do you know how your website collects and uses personal information? California law changed on January 1, 2014. Are you ready?

California Federal Judge Grants Summary Judgment to Apple, Dismissing Consumers' iPhone App Class Action

Emily Schlesinger
Associate, Seattle
eschlesinger@wsgr.com

On November 25, 2013, Judge Lucy Koh of the U.S. District Court for the Northern District of California granted summary judgment for defendant Apple, Inc., dismissing claims by a class of plaintiffs claiming that they had detrimentally relied on Apple's misrepresentations to purchase and use their iPhones and other devices in violation of California consumer protection laws.[1] After nearly three years of litigation, Judge Koh ultimately determined that the plaintiffs lacked standing to pursue their claims because they did not establish a genuine issue of material fact that they "actually relied" on Apple's statements that it had adhered to the company privacy policy.[2]

Litigation Background

In December 2010, *The Wall Street Journal* published a highly publicized article discussing the ability of Apple and Android mobile applications ("apps") to "track" their users.[3] Soon after the story broke, a group of plaintiffs sued Apple, arguing that the company had approved apps for the iPhone and iPad that intercepted users' personal information and tracked their habits without authorization in violation of federal and state law. In August 2011, 18 other putative class actions were consolidated with the original case in multidistrict litigation before Judge Koh.[4]

The consolidated complaint brought claims on behalf of two putative nationwide classes—an "iDevice Class" and a "Geolocation Class." The iDevice Class consisted of all people in the United States who had purchased an iPhone and downloaded free apps in the previous three years. The plaintiffs claimed that class members had been damaged because Apple could not safeguard their personal information as represented in Apple's privacy policy. Examples of the information allegedly collected from the plaintiffs included (among other things) their geolocation, the unique device identifier (UDID) assigned to their iPhones, the personal name assigned to their devices, and their app-specific activity.[5] Also, despite Apple's claims to the contrary, the plaintiffs opined that the foregoing information was not anonymized, and therefore could be linked to an individual user. The Geolocation Class consisted only of those iPhone purchasers who switched off the "Location Services" setting on their iPhones, which they believed would prevent their iPhone from storing information about their physical location and transmitting that information to Apple.

> Judge Koh ultimately determined that the plaintiffs lacked standing to pursue their claims because they did not establish a genuine issue of material fact that they "actually relied" on Apple's statements that it had adhered to the company privacy policy

After a year of heated motion practice[6] and the dismissal of the initial complaint for lack of standing,[7] the plaintiffs filed their Third Amended Complaint (TAC) on October 4, 2012.[8] The TAC only alleged claims under California's Consumers Legal Remedies Act (CLRA)[9] and California's Unfair Competition Law (UCL).[10]

---

[1] Order Granting Defendant's Motion for Summary Judgment, *In re iPhone Application Litig.*, No. 5:11-md-02250-LHK (N.D. Cal. Nov. 25, 2013).
[2] *Id.* at 13.
[3] *See* Scott Thurm and Yukari Iwatani Kane, "Your Apps are Watching You: A WSJ Investigation finds that iPhone and Android apps are breaching the privacy of smartphone users," *The Wall Street Journal* (Dec. 27, 2010), *available at* http://online.wsj.com/news/articles/SB10001424052748704694004576020083703574602?cb=logged0.33890537178219793 (last visited Dec. 8, 2013).
[4] Consolidation and Transfer Order, *In re iPhone Application Litig.*, No. 5:11-md-02250-LHK (N.D. Cal. Aug. 25, 2011).
[5] *See* TAC ¶ 2.
[6] The initial consolidated complaint alleged claims under the Stored Communications Act, Computer Fraud and Abuse Act, and Wiretap Act, as well as claims of violations of the plaintiffs' right to privacy, negligence, trespass, and conversion under California common law. The complaint also asserted claims against mobile advertising and analytics services Admob, Inc., Flurry, Inc., AdMarvel, Inc., Google, Inc., and MediaLets, Inc. ("Mobile Advertising Defendants"), arguing that they had "collected" supposedly "personal information" from the plaintiffs' devices for purposes unrelated to the "functionality of those devices," or the apps on them. However, in June 2012, Judge Koh dismissed the Mobile Advertising Defendants, and the plaintiffs proceeded against Apple on the only two remaining claims. *See* Order Granting in Part, and Denying in Part, Defendants' Motion to Dismiss, *In re iPhone Application Litig.*, No. 5:11-md-02250-LHK (N.D. Cal. June 12, 2012).
[7] Apple successfully moved to dismiss the plaintiffs' initial consolidated complaint on the basis that the plaintiffs lacked Article III standing because Apple's allegedly unlawful conduct did not cause them any actual injury. *See* Order Granting Defendants' Motion to Dismiss for Lack of Article III Standing with Leave to Amend, *In re iPhone Application Litig.*, No. 5:11-md-02250-LHK (N.D. Cal. Sept. 20, 2011). The dismissal cast doubt on the plaintiffs' theory that the collection of personal information itself created a particularized injury for the purposes of Article III standing and demanded more concrete allegations. When the plaintiffs filed their First Amended Complaint, Apple again argued that they lacked standing; however, this time, Judge Koh denied the motion and allowed the plaintiffs to proceed on two of their claims. *See* Order Granting in Part, and Denying in Part, Defendants' Motion to Dismiss, *In re iPhone Application Litig.*, No. 5:11-md-02250-LHK (N.D. Cal. June 12, 2012) at 10-11. Judge Koh explained that the plaintiffs had "articulated additional theories of harm," and "actual injury," including "diminished and consumed iDevice resources," "increased, unexpected and unreasonable risk to the security of personal information," and "detrimental reliance on Apple's representations" regarding privacy protections offered to app users. *See id.*
[8] Third Amended Complaint, *In re iPhone Application Litig.*, No. 5:11-md-02250-LHK (N.D. Cal. Oct. 4, 2012).
[9] Cal. Civil Code § 1750, *et seq.*
[10] Cal. Bus. & Prof. Code § 17200, *et seq.*

The Plaintiffs' Claims Against Apple

Apple's iPhones and devices are composed of the hardware and the mobile operating system firmware known as iOS. According to the plaintiffs, Apple designed the iOS environment to easily transmit iPad and iPhone users' personal information to third parties that would allegedly collect and analyze that data without users' detection or consent. The crux of the plaintiffs' claims was that the plaintiffs were deceived into buying iOS devices and that the devices were overvalued (due to privacy deficiencies) and did not function as represented.

The plaintiffs also argued that the personal information being transmitted through the apps was not adequately protected despite the claims Apple made when the plaintiffs purchased their devices, and that Apple collected location data from its users even when the "Location Services" setting was turned off.[11] Further, the plaintiffs asserted that due to Apple's conduct, the resources of their Apple devices—including iDevice storage, battery life, and bandwidth—were consumed and diminished without their permission. They claimed that if they had known of their devices' "actual characteristics," they would not have purchased them, or would have demanded a lower price.[12]

The crux of the plaintiffs' claims was that the plaintiffs were deceived into buying iOS devices and that the devices were overvalued (due to privacy deficiencies) and did not function as represented

The Court's Findings

After months of discovery and numerous depositions, Apple moved for summary judgment in May 2013, asserting that the plaintiffs lacked Article III standing, as well as standing under both the CLRA and the UCL.[13] They also asserted that the plaintiffs failed to create a genuine issue of material fact concerning their standing. Judge Koh agreed.

Actual reliance is an "essential" element to establishing standing under Article III, the CLRA, and the UCL, but according to Judge Koh, the plaintiffs had not shown that they had "actually relied on Apple's alleged misrepresentations regarding data collection and privacy to their detriment."[14] She explained that although the plaintiffs each alluded to "a vague 'understanding'" of Apple's privacy policies,[15] none of them had "present[ed] evidence that he or she even saw, let alone read and relied upon, the alleged misrepresentations contained in the Apple Privacy Policies, S[oftware Licensing Agreements (SLAs)], or App Store Terms and Conditions, either prior to purchasing his or her iPhone, or any time thereafter."[16] It did not help the plaintiffs' case that their testimony (and that of their putative class members) repeatedly undermined their own arguments—many of them could not "recall" what they read when buying the device in question, or stated that they did not rely on anything other than online reviews when buying their iOS product.

Judge Koh also rejected the plaintiffs' position that their agreement to Apple's terms of service served as an implicit agreement to the terms of the company's privacy policy

Judge Koh also rejected the plaintiffs' position that their agreement to Apple's terms of service served as an implicit agreement to the terms of the company's privacy policy. She reasoned that "[t]he mere fact that plaintiffs had to scroll through a screen and click on a box stating that they agreed with the Apple Privacy Policy in July 2010 does not establish, standing alone, that plaintiffs actually read the alleged misrepresentations contained in that privacy policy, let alone that these misrepresentations subsequently formed the basis for plaintiffs' 'understanding' regarding Apple's privacy practices."[17] Further, Judge Koh expressed concern that the plaintiffs had filed declarations that endeavored to contradict their prior deposition testimony acknowledging that they had not read Apple's alleged misrepresentations.[18] In short, she found that the "[p]laintiffs' repeated failure to provide any evidence to

[11] An April 2011 article in *The Wall Street Journal* led to these allegations; the article stated that newspaper testing showed that even when iPhones' "Location Services" were turned "off," location data was still stored on Apple's devices, and collected "rather inaccurate location readings." Jennifer Valentino-Devries, "IPhone Stored Location in Test Even if Disabled," *The Wall Street Journal* (Apr. 25, 2011), *available at* http://online.wsj.com/news/articles/SB10001424052748704123204576283580249161342 (last visited Dec. 8, 2013). Apple later attributed this data collection to a "software bug" that was resolved with the release of a new iOS version. *See* Nick Bilton, "Apple Updates Software to Fix Problems with Collecting Location Data," *The New York Times* (May 4, 2011), *available at* http://bits.blogs.nytimes.com/2011/05/04/apple-ios-software-release-fixes-location-bug/ (last visited Dec. 8, 2013).

[12] TAC ¶ 5.

[13] Defendant Apple, Inc.'s Motion for Summary Judgment, *In re iPhone Application Litig.*, No. 5:11-md-02250-LHK (N.D. Cal. May 17, 2013).

[14] Order Granting Defendants' Motion for Summary Judgment, *supra* note 1 at 13 ("For the Plaintiffs' harm to be 'fairly traceable' to Apple's misrepresentations, . . . Plaintiffs must have actually seen the misrepresentations and taken some action based on what they saw—that is, Plaintiffs must have actually relied on the misrepresentations to have been harmed by them").

[15] *Id.* at 19.

[16] *Id.* at 16.

[17] *Id.* at 26.

[18] *Id.* at 18-19 (noting that "attempting to create a genuine issue of material fact by submitting an affidavit contradicting one's own prior deposition testimony is generally disfavored").

Continued on page 10...

support the theory that they must have read or seen the alleged misrepresentations in Apple's Privacy Policy strengthens the Court's conclusion that Plaintiffs have not met their burden to demonstrate standing."[19]

Implications

The decision—which marks the definitive end of a lengthy legal battle between Apple and consumers—is noteworthy for a couple of reasons.

> The ruling strongly suggests that in order to meet the rigorous standing requirements necessary to proceed under the CLRA or UCL, litigants must do far more than assume that someone relied on a company's privacy policy

First, the ruling strongly suggests that in order to meet the rigorous standing requirements necessary to proceed under the CLRA or UCL, litigants must do far more than assume that someone relied on a company's privacy policy. According to Judge Koh, each plaintiff must point to specific facts "indicating that [he or she] actually saw the misrepresentations," as well as facts that those misrepresentations were "substantial factors" when he or she bought a device. As such, plaintiffs moving forward on such claims would need to have established a thorough record of their diligence prior to making a purchase—and such cumbersome "pre-litigation" planning is highly unlikely.

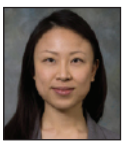
Moreover, this is one of the few major privacy class actions to have been dismissed *after* discovery rather than on a motion to dismiss. Thus, it provides additional guidance to defense lawyers considering whether to settle or fight a putative privacy class action. Specifically, Judge Koh's decision suggests that defendants in privacy disputes have serious ammunition to raise a standing argument if a plaintiff can point to nothing substantive to show his or her reliance on a company's alleged misrepresentations when buying the company's product. Because most consumers do not maintain detailed records of their research before purchasing products like smartphones or mobile apps, "evidentiary support" may wind up being the fatal blow to a plaintiff's complaint in future cases.

> The decision suggests that defendants in privacy disputes have serious ammunition to raise a standing argument if a plaintiff can point to nothing substantive to show his or her reliance on a company's alleged misrepresentations when buying the company's product

[19] *Id.* at 27.

FTC Settles First Mobile "Cramming" Case

Suzanne Bell
Partner, Palo Alto
sbell@wsgr.com



Sharon Lee
Associate, Palo Alto
shlee@wsgr.com

In November 2013, the Federal Trade Commission (FTC) obtained a monetary judgment of more than $11 million in aggregate against Wise Media, LLC, its CEO, its owner, and an entity holding Wise Media funds, as well as a permanent injunction prohibiting Wise Media, its CEO, and its owner from placing charges on any person's telephone bill or assisting anyone else in doing so. The FTC alleged in its complaint that Wise Media had engaged in deceptive and unfair acts and practices in violation of Section 5(a) of the FTC Act by representing that consumers were obligated to pay charges for Wise Media's text message-based services that Wise Media caused to be placed on their mobile phone bills, without obtaining their express informed consent. The practice of placing unauthorized third-party charges on consumers' phone bills is known as "cramming."

Background

According to the FTC, Wise Media provided subscription services that included periodically sending text messages with love tips, horoscope alerts, and similar information. Each subscription cost $9.99 per month with automatic monthly renewal.

The complaint alleged that Wise Media provided these services to consumers and charged them without obtaining their express informed consent. As described in the complaint, consumers received text messages suggesting that they were subscribed to these services, and they often ignored what appeared to be a spam text. Even if consumers responded by text indicating that they did not want Wise Media services, they were still charged for those services. In contrast, the FTC described "double opt-in" verification as standard industry practice for merchants that offer consumers the ability to order and purchase by text message, with the charge appearing on the consumers' mobile phone bills. According to the complaint, "double opt-in" verification is a process in which the merchant requires the consumer to take two steps to confirm a purchase.

The FTC alleged that Wise Media used the billing mechanisms of mobile phone companies to cause charges for Wise Media services to be included on consumers' mobile phone bills with abbreviated descriptions that did not always identify Wise Media as the source of the charge. According to the FTC, most consumers paid their mobile phone bills without noticing these charges, and even for consumers who noticed these charges, it was difficult to dispute them: Not only was it challenging to find phone numbers for Wise Media, but Wise Media representatives claimed they would refund charges and did not, or consumers were unable to obtain refunds for all of the months charged.

The complaint stated that phone companies had refunded to consumers substantial percentages of Wise Media's charges, with certain phone companies warning and terminating Wise Media over its excessive refund rates. In addition, the complaint alleged that Wise Media received numerous complaints from consumers and the Better Business Bureau, but nonetheless had made millions since beginning operations in 2011.

Settlements

In addition to requiring payment of more than $11 million in aggregate, the settlements include permanent injunctions and orders against Wise Media, its CEO, and its owner. They prohibit these defendants from placing charges on any person's telephone bill or assisting anyone else in doing so. The settlements also prohibit these defendants from representing that a consumer is obligated to pay for goods or services or otherwise cause any charges to be billed to a consumer's account unless prior to the charge, the consumer has provided express verifiable consent to be charged and all material terms of the billed purchase have been disclosed. These material terms include the number and amount of each charge and the account to which each charge will be billed.

Conclusion

These settlements are a reminder that the FTC is continuing to actively monitor the mobile payment space. In its March 2013 staff report, *Paper, Plastic...or Mobile?: An FTC Workshop on Mobile Payments*,[1] the FTC expressed concern that when disputes arise regarding mobile phone billing, consumers' recourse is their agreements with or the goodwill of mobile carriers instead of statutory or regulatory protection.[2] Companies using mobile payments should consider how to best obtain consumer consent for any charges and use methods that are at least in line with industry standards.

---

[1] FTC Workshop, "Paper, Plastic...or Mobile?: An FTC Workshop on Mobile Payments" (March 2013), staff report available at http://www.ftc.gov/opa/2013/03/mobilepymts.shtm.

[2] For our coverage of the FTC's March 2013 staff report, *Paper, Plastic...or Mobile?: An FTC Workshop on Mobile Payments*, please see our WSGR Alert at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-mobile-payment-industry.htm.

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

650 Page Mill Road, Palo Alto, California 94304-1050 | Phone 650-493-9300 | Fax 650-493-6811 | www.wsgr.com

Austin Beijing Brussels Georgetown, DE Hong Kong Los Angeles New York Palo Alto San Diego San Francisco Seattle Shanghai Washington, DC