Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

EYE ON PRIVACY

MARCH 2014

Welcome

In this month's issue of *Eye on Privacy*, we cover some significant updates from both the U.S. and across the pond, including the potentially significant enforcement of timing provisions in California's data breach notification law, developments regarding the U.S.-EU Safe Harbor in the U.S. and in the EU, a somewhat controversial enforcement action by the FTC regarding Apple's in-app purchase disclosure practices, and new guidance from the UK Information Commissioner's Office for app developers. We also provide a recap of a recent webinar conducted by members of our Brussels privacy team on the status of the new draft EU Data Protection Regulation.

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

Kaiser Foundation Health Plan Settles California Attorney General Charges over Delayed Data Breach Notification

Matthew Staples
Associate, Seattle
mstaples@wsgr.com

Kaiser Foundation Health Plan, Inc. (Kaiser) recently agreed to settle charges brought by California Attorney General Kamala Harris alleging that Kaiser, a component of Kaiser Permanente, the largest health maintenance organization in the U.S., violated California's unfair competition law by taking too long to notify more than 20,000 current and former employees that their personal information had been compromised.[1] The case and its settlement may have significant implications for businesses that suffer data security incidents requiring notification to affected persons.

Complaint and Settlement

In her complaint,[2] Attorney General Harris alleged that Kaiser learned on September 24, 2011, that an external hard drive containing unencrypted Social Security numbers, dates of birth, addresses, and other personal information of Kaiser employees (and, in some cases, spouses and children) was sold to a member of the public at a thrift store. Kaiser secured possession of the drive on December 21, 2011, and commenced a forensic evaluation. The forensic evaluation allegedly revealed over 30,000 Social Security numbers and other unencrypted "employee-related sensitive

Continued on page 2...

[1] The complaint also alleges that Kaiser engaged in unfair competition by "publicly posting and/or displaying the Social Security numbers of 20,539 Californians on an unencrypted hard drive made available to the general public via sale at a thrift store," thereby violating California Civil Code § 1798.85(a)(1).

[2] The complaint in *California v. Kaiser Foundation Health Plan Inc.* (case no. RG14711370) (Cal. Sup. Ct., Alameda Co.), as well as the final judgment and permanent injunction filed on the same day, is available at http://www.wsgr.com/PDFs/Judgment-and-Settlement.pdf.

In This Issue

information" on the drive. Kaiser continued to inventory the drive through mid-February 2012, and notified 20,539 California residents on or about March 19, 2012, that their personal information was compromised in the incident.

Attorney General Harris alleged that Kaiser had sufficient information to identify and notify at least some individuals affected by the breach between December 2011 and February 2012, and that its failure to provide notice in a timely fashion violated California's security breach notification statute. In her complaint, Attorney General Harris sought an injunction to permanently enjoin Kaiser from committing any acts of unfair competition, an order for the company to pay $2,500 for each violation of Section 17200 of the California Business and Professions Code, and recovery of the state's costs for the suit and its investigation of the matter.

Attorney General Harris alleged that Kaiser had sufficient information to identify and notify at least some individuals affected by the breach between December 2011 and February 2012, and that its failure to provide notice in a timely fashion violated California's security breach notification statute

In a stipulated final judgment and permanent injunction entered by the court on February 10, 2014, Kaiser is obligated to provide notices of any future breaches of personal information relating to current or former employees on a "rolling basis" where "feasible and appropriate," with Kaiser needing to provide notice "as soon as reasonably possible after identifying a portion of the total individuals affected by a breach, even if Kaiser's investigation of the breach is ongoing," and "continu[ing] to notify individuals as soon as they are identified, throughout and until completion of Kaiser's investigation of the breach."

Kaiser also agreed to pay $150,000 ($30,000 in civil penalties and $120,000 in attorneys' fees and costs of investigation and prosecution). Further, Kaiser agreed to, within 120 days of the judgment, provide additional training to its employees regarding personnel files, review its email encryption policies and devise a plan for updating those policies as needed, audit its employees' access to employee personal information, and provide a report to the California attorney general's office regarding its audit.

Analysis

The relevant portion of California's security breach notification statute, California Civil Code Section 1798.82, provides in pertinent part as follows (emphasis added):

> Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. **The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.**

The statute does not provide a more precise meaning of "the most expedient time possible and without unreasonable delay," but California's Office of Privacy Protection has recommended that notice be given within 10 days of an organization's determination that personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[3]

California's Office of Privacy Protection has recommended that notice be given within 10 days of an organization's determination that personal information was, or is reasonably believed to have been, acquired by an unauthorized person

In the complaint, Attorney General Harris stated that while Kaiser commenced notice in or about March 2012, it "could have notified individuals it had identified as affected by the breach as early as December 2011." The company providing notice approximately a month after completing its internal forensic analysis—approximately six months after its

[3] *See* California Office of Privacy Protection, "Recommended Practices on Notice of Security Breach Involving Personal Information," *available at* http://www.dhcs.ca.gov/formsandpubs/laws/priv/Documents/PrivacyProtection.pdf.

initial discovery of the hard drive having been compromised, and approximately four months after obtaining the hard drive—allegedly was not "in the most expedient time possible and without unreasonable delay." The complaint does not address whether Kaiser's evaluation of the hard drive constituted "measures necessary to determine the scope of the breach," but by implication, the position of Attorney General Harris in the complaint appeared to be that even if measures are ongoing to determine the scope of the breach, notice must be provided to those who have been identified at the time. This is consistent with the obligation to provide notification on a "rolling basis" where "feasible and appropriate," as Kaiser agreed to in the stipulated final judgment.

Implications

The *Kaiser* case and settlement are interesting for a number of reasons. First, they address what Attorney General Harris asserts "the most expedient time possible" and "without unreasonable delay" mean under California's security breach notification law. The complaint and its settlement evidence Attorney General Harris's position that notification to affected California residents of security breaches must occur on a rolling basis, as residents can be identified, rather than at the completion of an investigation. This implies a position by the attorney general that the statute's provisions permitting notification to be delayed to accommodate "measures necessary to determine the scope of the breach" do not permit delay of notification to identified individuals whose unencrypted personal information has been confirmed as compromised.

Because breach notification investigations often are fluid, with tentative conclusions sometimes later invalidated by subsequent findings, attempting to comply with the "rolling notification" standard suggested by the complaint and settlement may lead to companies being placed in a difficult position. The California statute, along with most other security breach notification statutes, requires notice not only in the event of unencrypted personal information being acquired by an unauthorized person, but also when it is "reasonably believed to have been" so acquired. Companies might be required to deliver notices to consumers containing information that later turns out to be inaccurate or incomplete. This could require later supplementation or correction of facts. It also could result in "false positives" in which consumers are notified that their personal information was compromised when, as revealed by subsequent investigation, it was not.

This case and its settlement may have bearing on other state regulatory authorities' interpretation of their laws or, potentially, lead to statutory amendments

These factors may necessitate difficult decisions by entities suffering a security breach, or a potential security breach, affecting California residents. Companies that delay providing notice until the completion of an investigation run the risk of potential enforcement by the California attorney general. Companies that rush to provide notice while an investigation is ongoing, in contrast, may be required to provide notification based on limited information, as well as to deliver multiple notices to consumers. This may be expensive, logistically challenging, and confusing to recipients. It also could lead to significant public relations challenges.

Additionally, because nearly all of the 46 state security breach notification statutes use similar timing language,[4] this case and its settlement may have bearing on other state regulatory authorities' interpretation of their laws or, potentially, lead to statutory amendments. California was the first state to enact security breach notification legislation in 2002, with dozens of states quickly following suit over the next few years. More generally, California plays a leading role in the privacy regulatory space, and it would not be surprising to see this case and its settlement have an impact on how other state regulatory authorities interpret the timing requirements of their state breach notification laws over time.

[4] While several U.S. state security breach notification statutes use language similar to the California statute, many of them differ in the precise language used to articulate the notice obligation. For example, some states only require notification "without unreasonable delay," while some require notice "as soon as possible," "as soon as reasonably practicable," "as expeditiously as possible," or in accordance with similar standards. Most permit notice to be delayed in circumstances similar to those set forth in the California law, while some also permit notice to be delayed as necessary to identify affected individuals. Three states—Florida, Ohio, and Vermont—in most cases require notification to be provided no later than 45 days following the discovery or determination of a security breach.

Status of the EU Regulation and the Safe Harbor Framework

Cédric Burton
Associate, Brussels
cburton@wsgr.com

Anna Pateraki
Associate, Brussels
apateraki@wsgr.com

On February 20, 2014, two of our Brussels-based attorneys specializing in European privacy and data security—Cédric Burton and Chris Kuner—presented a webcast titled "Update on EU Data Protection Law," with a particular focus on the U.S.-EU Safe Harbor Framework (Safe Harbor).[1] The following article summarizes the session and includes a few key takeaways.

Update on the Regulation

The webinar provided an update on the current status, gave an overview of the political background, and examined a few likely trends pertaining to the draft EU Data Protection Regulation (Regulation). Particular emphasis was placed on a few select items, such as the one-stop-shop regulator, pseudonymization, and profiling.

Timing for the adoption of the Regulation remains uncertain due to the Regulation's complexity and the current political disagreements on key issues. Adoption is currently expected to take place in late 2014 or early 2015 at the earliest, with the Regulation entering into force two years after adoption (but timing may change). The Regulation will have an impact on almost all companies doing business in the EU. Companies targeting EU individuals should strategize now on how to comply with the core principles of the Regulation. Regardless of the final wording, the current core principles included in the Regulation will be reflected in the future EU framework, as the existing draft partly codifies existing practices and interpretations.

Political Background on Safe Harbor

The webinar also discussed the current political context in the EU around data transfers, with a focus on Safe Harbor. Safe Harbor recently has been under scrutiny in the EU following the revelations about law-enforcement access to private company data, and has been criticized at both the EU and national levels:

- At the EU level, the criticisms of Safe Harbor included statements about the lack of enforcement and false claims made by companies regarding their adherence to the Safe Harbor principles.[2] Furthermore, the EU Parliament called for the suspension of Safe Harbor, and a vote on a relevant resolution is expected in March 2014.[3] In parallel, the Council of the EU created and co-chaired with the European Commission an ad hoc EU-U.S Working Group on Data Protection to examine transatlantic data flows.

- At the national level, some regulators (e.g., German data protection authorities) have made strong statements calling for the suspension of Safe Harbor.[4] In addition, there has been some interest in data localization requirements (mandating that data be stored locally) in some Member States.[5]

It is, however, important to keep in mind that only the European Commission has the legal powers to take action (e.g., suspend, freeze, and amend) regarding the U.S.-EU Safe Harbor Framework. Any skepticism from national regulators and the EU Parliament is primarily intended to send a political message, since their statements and resolutions are not legally binding on the European Commission. However, their statements have created bad publicity for Safe Harbor-certified companies and thus have put pressure on EU companies to conduct diligence of the Safe Harbor compliance programs of the U.S. companies with which they do business, or in some cases to even refuse to do business with companies that only rely on Safe Harbor for their data transfers to the United States.

It is important to keep in mind that only the European Commission has the legal powers to take action (e.g., suspend, freeze, and amend) regarding the U.S.-EU Safe Harbor Framework

[1] The slides from the webcast are available at http://www.wsgr.com/eudataregulation/pdf/webcast-0214.pdf.

[2] "Data protection: Claude Moraes calls for suspension of EU-US 'safe companies list,'" S&D press release (Oct. 8, 2013), *available at* http://www.socialistsanddemocrats.eu/newsroom/data-protection-claude-moraes-calls-suspension-eu-us-safe-companies-list, or watch a recording of the hearings, *available at* http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131007-1900-COMMITTEE-LIBE.

[3] "NSA snooping: MEPs table proposals to protect EU citizens' privacy," European Parliament LIBE Committee press release (Feb. 12, 2014), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+IM-PRESS+20140210IPR35501+0+DOC+PDF+V0//EN&language=EN.

[4] *See* resolution of German regulators (Jul. 24, 2013), *available at* http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870.

[5] A. Smale, "Merkel Backs Plan to Keep European Data in Europe," *The New York Times* (Feb. 16, 2014), *available at* http://www.nytimes.com/2014/02/17/world/europe/merkel-backs-plan-to-keep-european-data-in-europe.html?_r=0.

Against this background and following several meetings, the European Commission issued a set of documents aimed at "rebuilding trust in EU-U.S. data flows," including a report on Safe Harbor.[6] This report acknowledges that Safe Harbor is a valid solution for data transfers[7] and includes 13 recommendations on Safe Harbor, some of which are addressed to companies (how best to comply) and others to regulators (how best to enforce). More developments with respect to Safe Harbor are expected in the following months, as the European Commission has committed to work with its U.S. counterparts to reinforce Safe Harbor by the summer of 2014.[8]

The European Commission has shown political will to defend and improve Safe Harbor. Safe Harbor is still a valid mechanism for transferring personal data from the EU to the U.S. and the likelihood of seeing this agreement repealed is low, although some changes may come in the future. However, increased scrutiny from U.S. and EU regulators is expected and companies that are Safe Harbor-certified or are planning to become certified should make sure they comply with the Safe Harbor principles.

Five Key Takeaways About Safe Harbor

1. Under the existing law, Safe Harbor is a valid legal mechanism for EU-U.S. data transfers and will likely stay.

Increased scrutiny from U.S. and EU regulators is expected and companies that are Safe Harbor-certified or are planning to become certified should make sure they comply with the Safe Harbor principles

2. A few improvements to Safe Harbor are expected to become effective in the second half of 2014 or later.

3. Enforcement of Safe Harbor in the U.S. is increasing. As also reported in this newsletter, the FTC reached settlements with 13 companies earlier this year for falsely claiming compliance with Safe Harbor.

4. If your business is being pressured by your EU customers about Safe Harbor, be ready to explain that you take compliance with EU privacy laws seriously and be prepared to demonstrate how your company complies with the Safe Harbor principles.

5. Review the European Commission's recommendations for Safe Harbor-certified companies and decide how best to implement them. Being proactive will help increase trust in your organization.

For more information on this topic, please contact any of the attorneys on our Brussels-based EU privacy and data security team.

A recording of our webcast is located at http://peach.wsgr.com/store/seminar/seminar.php?seminar=25407. The webcast slides may be viewed at http://www.wsgr.com/eudataregulation/pdf/webcast-0214.pdf.

---

[6] "EC Communication on the functioning of the Safe Harbor from the perspective of EU citizens and companies established in the EU," *available at* http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

[7] "Restoring Trust in EU-U.S. data flows - Frequently Asked Questions," EC press release (Nov. 27, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

[8] Joint Press Statement following the EU-US-Justice and Home Affairs Ministerial Meeting (Nov. 18, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-1010_en.htm.

FTC Steps Up Enforcement of Safe Harbor Compliance Claims

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

Joe Molosky
Associate, Washington, D.C.
jmolosky@wsgr.com

The Federal Trade Commission's (FTC's) enforcement actions for claims of compliance with Safe Harbor privacy frameworks by U.S. companies have increased significantly over the past few months. In the first two months of 2014 alone, the FTC announced settlements with 13 U.S. companies over allegations that the companies falsely claimed they held current certifications under the U.S.-EU Safe Harbor Privacy Framework.[1] The FTC's focus has not been limited to the EU framework, as three of the settlements include claims that the companies falsely represented holding current certifications under the U.S.-Swiss Safe Harbor Privacy Framework.

Background

The Safe Harbor privacy frameworks are voluntary self-certification programs developed by the U.S., EU, and Switzerland to reconcile the different approaches to privacy in those areas. The frameworks provide a method for U.S. organizations to comply with the EU's Directive on Data Protection and the Swiss Federal Act on Data Protection when transferring personal information from the EU and Switzerland to another country. In order to hold a current certification, a company must certify on an annual basis that it complies with the seven Safe Harbor Privacy Principles: notice, choice, onward transfer, access, security, data integrity, and enforcement. The FTC enforces compliance with the frameworks in two ways. First, the FTC enforces statements made by organizations regarding the status of their certification, which have been the focus of the recent enforcement actions. Second, the FTC enforces the promises made by organizations in order to obtain certification, which have resulted in significant settlements in prior years, most recently with Myspace in 2012.[2]

The FTC alleged that the companies published statements, privacy policies, and Safe Harbor certification symbols on their websites that stated or implied that the companies held current certifications. The FTC alleged that these statements were deceptive under Section 5 of the FTC Act because although the companies represented that they held current Safe Harbor certifications, in reality they had not self-certified for a period of time and did not hold current certifications at the time of the representations. The companies involved represent a wide range of industries, including professional sports teams, an accounting firm, IT service providers, and a children's online entertainment company.

Settlements

In their settlement agreements with the FTC, the companies agreed to refrain from misrepresenting the extent to which they are a member of, adhere to, comply with, are certified by, are endorsed by, or otherwise participate in any privacy or data security program sponsored by the government or any other self-regulatory or standard-setting organization.[3] The agreements, which also include reporting requirements, are effective for 20 years from the date of issuance.

Implications

The investigations and settlements are significant, as they demonstrate the FTC's perhaps renewed focus on enforcing the Safe Harbor frameworks in the face of criticism from the European Commission.[4] Partially in response to reports of law enforcement access to personal information, on November 27, 2013, the European Commission published a set of recommendations regarding the U.S.-EU Safe Harbor Framework and questioned the enforcement of the framework by U.S. authorities. The FTC defended past enforcement of the frameworks by U.S. authorities, but the recent settlements demonstrate an additional focus on the area, especially statements of certification under the frameworks.

Businesses that include statements regarding Safe Harbor certification in their privacy policies or websites should ensure that they have met the certification requirements, including compliance with the seven Safe Harbor Privacy Principles, and establish a process for ensuring that their certification remains up-to-date. Reviewing an organization's Safe Harbor certification statements also presents a prime opportunity to ensure that any other public privacy or data security representations are clear, reflect current practices, and comply with applicable state and federal privacy policy requirements.

---

[1] http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply; http://www.ftc.gov/news-events/press-releases/2014/02/ftc-settles-childrens-gaming-company-falsely-claiming-comply.

[2] Agreement Containing Consent Order, In the Matter of Myspace LLC, No. 102 3058, http://www.ftc.gov/sites/default/files/documents/cases/2012/05/120508myspaceorder.pdf.

[3] *See e.g.*, Agreement Containing Consent Order, In the Matter of DataMotion, Inc., No. 142 3023, http://www.ftc.gov/sites/default/files/documents/cases/140121datamotionagreement.pdf; Agreement Containing Consent Order, In the Matter of Fantage.com, Inc., No. 142 3026, http://www.ftc.gov/system/files/documents/cases/140107fantageagree.pdf.

[4] *See* Stephen Gardner, "U.S. Officials Respond to EU Concerns over Safe Harbor Data Transfer Program," Bloomberg BNA (Dec. 16, 2013), http://www.bna.com/us-officials-respond-n17179880742/.

Apple Agrees to Refund at Least $32.5 Million to Settle FTC Complaint Alleging That It Charged Kids' In-App Purchases Without Parental Consent

Emily Schlesinger
Former Associate, Seattle

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

On January 15, 2014, the Federal Trade Commission (FTC) announced that Apple, Inc. had agreed to pay a minimum of $32.5 million in full refunds to consumers to settle allegations that the company was billing customers for purchases that children made from the company's App Store without parental consent.[1] According to the FTC, since at least 2011, thousands of children had unwittingly racked up significant App Store charges without their parents' knowledge because the company's billing procedures allowed users to incur unlimited in-app charges for a 15-minute window after downloading new software onto a device.[2]

The billing issue gained public attention when *The Washington Post* ran a February 2011 story on the topic.[3] Apple quickly responded by upgrading its operating system to require users to submit an iTunes password to make purchases on newly downloaded apps. However, even after the company required users to enter passwords to make in-app purchases, the users' accounts remained open for additional purchases for 15 minutes before the password window expired, and the request-for-password pop-up often did not explain that a parent was about to authorize a purchase.[4] A putative class action lawsuit followed a month later, and the parties entered into a settlement in June 2013, with the company agreeing to offer iTunes credits or cash refunds to parents for children's unintended in-app charges.[5] However, the class action settlement did not require the company to make changes to its systems to ensure that consumers were notified that reentering their usernames and passwords to make in-app charges effectively authorized a 15-minute window during which subsequent charges could be made.

The FTC's Complaint

According to the FTC's complaint, Apple's App Store offers hundreds of mobile applications ("apps"), including a category of "Games," some of which are specifically subcategorized as intended for "Family" or "Kids."[6] Although several apps are identified as "Free," the company may still charge account holders for certain user activities within those apps; these are known as "in-app charges."[7] Such charges, which are often included in apps targeting children, can range from $0.99 to $99.99, and the company sets no limits on their purchase.[8]

The installation of a new app on a device prompts a user to enter his iTunes username and password.[9] But, according to the FTC,

> According to the FTC, since at least 2011, thousands of children had unwittingly racked up significant App Store charges without their parents' knowledge because the company's billing procedures allowed users to incur unlimited in-app charges for a 15-minute window after downloading new software onto a device

during the 15-minute period following installation, Apple did not properly display a second password prompt before users could incur in-app charges.[10] As a result, children

[1] *See* FTC Release, "Apple Inc. Will Provide Full Consumer Refunds of At Least $32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent—Company Also Will Modify its Billing Practices Under FTC Settlement" (Jan. 15, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million (last visited Mar. 6, 2014).

[2] *See* Cecilia Kang, "In-app purchases in iPad, iPhone, iPod kids' games touch off parental firestorm," *The Washington Post* (Feb. 8, 2011), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2011/02/07/AR2011020706073_pf.html (last visited Mar. 6, 2014).

[3] *See id.*

[4] *See* Statement of Chairwoman Edith Ramirez & Commissioner Julie Brill, *In the Matter of Apple Inc.*, FTC File No. 1123018 (Jan. 15, 2014) (hereinafter "Ramirez & Brill statement") (noting that "for well over two-and-a-half years after [Apple added a password prompt to the in-app purchase sequence in March 2011], the password prompt has lacked any information to signal that the account holder is about to open a 15-minute window in which unlimited charges could be made in a children's app").

[5] *See* Home Page of the *In re Apple In-App Purchase Litigation* Settlement website, No. 5:11-cv-01758 (N.D. California), *available at* https://www.itunesinapppurchasesettlement.com/CAClaimForms/AIL/Home.aspx (last visited Mar. 6, 2014).

[6] FTC Complaint, *In the Matter of Apple, Inc.*, *available at* http://www.ftc.gov/sites/default/files/documents/cases/140115applecmpt.pdf (hereinafter "complaint") at ¶ 6.

[7] *Id.* ¶ 22.

[8] *Id.* ¶ 7.

[9] *See id.* ¶¶ 11-13 (describing the app-installation process).

[10] *Id.* ¶ 16.

Continued on page 8...

made in-app charges without their parents' knowledge simply by pressing the "Buy" button repeatedly on certain apps during that 15-minute window.[11] Also, the company's stated policy is that "all App Store transactions are final," and to the extent that a parent actually discovers any unauthorized charge made by his child, the company's refund process is prohibitively "cumbersome."[12]

The FTC alleged that the company's billing procedures violated Section 5 of the FTC Act because consumers were not properly alerted that entering a username and password combination to purchase an in-app item also approved *any* further purchases for an additional 15-minute window without requiring further authorization.[13] Moreover, the FTC seemed to find fault with the fact that the company had not revised its procedures to *fully resolve* the issue after receiving "at least tens of thousands of complaints related to unauthorized in-app charges by children" beginning as early as March 2011.[14]

> The consent decree, which lasts for 20 years, with audit rights lasting for five years, requires the company to implement several new measures in its billing practices by March 31, 2014

Terms of Settlement

The consent decree, which lasts for 20 years, with audit rights lasting for five years, requires Apple to implement several new measures in its billing practices by March 31, 2014.[15] These steps include:

- providing clear and conspicuous notice of all material information related to billing, including details about future purchases that can be made after the consumer enters his or her password; [16]
- obtaining users' express, informed consent for *all* in-app charges; and
- allowing consumers to revoke consent to prospective in-app charges at any time.[17]

The consent decree also requires the company to provide full refunds to all account holders it billed for unauthorized in-app charges made by minors by:

- providing electronic notice to any account holders who have made in-app purchases since March 2011, explaining that refunds are available and describing the proper procedure to obtain them;[18] and
- refunding the full purchase price of the in-app charge in question within 14 days to any eligible consumer who requests it.[19]

> Notably, the company must pay a minmum of $32.5 million in refunds. Further, if it receives less than $32.5 million in consumer requests within the first 12 months of the consent decree, it must remit any balance of the $32.5 million to the FTC.

Notably, the company must pay a minimum of $32.5 million in refunds. Further, if it receives less than $32.5 million in consumer requests within the first 12 months of the consent decree, it must remit any balance of the $32.5 million to the FTC.[20]

Commissioner Wright's Dissent

FTC commissioners voted 3-1 in favor of the deal,[21] with Commissioner Joshua T. Wright issuing a lengthy dissent.[22] Commissioner Wright opined that because the harm involved a "miniscule percentage of

---

[11] *Id.*

[12] *Id.* ¶ 27.

[13] *See* 15 U.S.C. § 45(a) and (n).

[14] Complaint, *see supra* note 6, ¶ 24.

[15] *See* Agreement Containing Consent Order, *available at* http://www.ftc.gov/sites/default/files/documents/cases/140115appleagree.pdf (last visited Mar. 6, 2014) (hereinafter, "consent order") at Parts IV & VII.

[16] *See id.* at ¶ 5 & Part I. "Express, informed consent" is specifically defined as an "affirmative act communicating authorization of an in-app charge (such as entering a password)," made directly before an in-app activity for which a consumer is billed, and a "clear and conspicuous disclosure of material information about the charge." *Id.* at 3, ¶ 5.

[17] *Id.* at Part I.

[18] *Id.* at Part II.F.

[19] *Id.* at Part II.

[20] *Id.* at Part II.D.

[21] Apple Inc.; Analysis of Proposed Consent Order to Aid Public Comment, Fed. Register/Vol. 79, No. 15, File No. 112 3108 (Jan. 23, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/federal_register_notices/2014/01/140123appleanalysisfrn.pdf (last visited Mar. 6, 2014). Commissioner Maureen K. Ohlhausen joined the majority, but issued her own separate statement. *See* Statement of Commissioner Maureen K. Ohlhausen, *available at* http://www.ftc.gov/public-statements/2014/01/statement-commissioner-maureen-k-ohlhausen (last visited Mar. 6, 2014) (hereinafter "Ohlhausen statement").

[22] Dissenting Statement of Joshua T. Wright, *available at* http://www.ftc.gov/public-statements/2014/01/dissenting-statement-commissioner-joshua-d-wright (last visited Mar. 6, 2014) (hereinafter "dissent").

consumers" when compared to the total number of apps downloaded from the App Store, any alleged injury was "insubstantial."[23] The majority disagreed, explaining that the size of the company and the volume of its App Store business were not proper factors in the analysis: "[T]he FTC Act does not give a company with a vast user base and product offerings license to injure large numbers of consumers or inflict millions of dollars of harm merely because the injury affects a small percentage of its customers or relates to a fraction of its product offerings."[24]

Commissioner Wright also argued that the decision would stifle innovation by requiring a company like Apple to try to anticipate "*all* the things that might go wrong" when it developed a new product, which would be "prohibitively costly" and likely "impossible."[25] However, the majority countered that the company's actions were not "unfair" because it had failed "to anticipate *all* things that might go wrong," but rather, because it repeatedly failed to fix a significant billing issue about which it was "well aware" in 2011.[26]

Implications

The settlement is the first punishment the FTC has handed to a tech platform over the handling of children's apps. It demonstrates the growing public and government concern over whether companies are providing parents with the appropriate information and tools to properly supervise their children's online activities.

> Companies operating in the mobile sphere should always obtain express consent before billing a consumer for any charge, and should provide "just-in-time disclosures" outside of the terms of the service or privacy policy for material information

The settlement also reinforces the FTC's long-held principle that companies must fully disclose to consumers all material details to a transaction, and it reemphasizes that disclosures in a company's terms of service or privacy policy may not be sufficient.[27] To avoid following in Apple's footsteps, companies operating in the mobile sphere should always obtain express consent before billing a consumer for any charge, and should provide "just-in-time disclosures" outside of the terms of the service or privacy policy for material information.

Importantly, companies should take heed that good intentions and remediation efforts may be immaterial to the FTC. The majority stressed that regardless of Apple's "intent," its failure to properly disclose the details of the 15-minute window was enough to constitute a law violation.[28] Moreover, the fact that the company began trying to fix the issue in March 2011 and had already agreed to refund certain consumers their money in the context of related class action litigation did not stop the FTC from asking the company to pay an additional hefty fee and ensure that its processes met the agency's standards.

---

[23] *Id.* at 5; *see id.* at 5-8.

[24] Ramirez & Brill statement, *supra* note 4 at 3.

[25] *Id.* at 15.

[26] *Id.*; *see also* Ohlhausen statement, *supra* note 21 at 1-2 (noting that the action would not "chill an iterative approach to software development" or "unduly burden the creation of complex products").

[27] The majority noted that the company's disclosure of the 15-minute window in its Terms and Conditions was not sufficient to provide consumers with adequate notice. *See* Ramirez & Brill statement, *supra* note 4 at 4.

[28] *Id.* at 2 & n.4.

UK Information Commissioner's Office Issues Guidance for App Developers

Cédric Burton
Associate, Brussels
cburton@wsgr.com

Anna Pateraki
Associate, Brussels
apateraki@wsgr.com

In December 2013, the United Kingdom's Information Commissioner's Office (ICO) issued "Privacy in mobile apps – Guidance for app developers."[1] According to the ICO, the guidance is not only relevant for apps used on mobile devices such as smartphones and tablets, but also for "other devices using similar app technology, for instance living-room devices such as smart TVs or games consoles."

The guidance is addressed to organizations developing apps for the UK market,

> The guidance addresses key EU privacy issues and may be useful for any organization developing apps for individuals located in the European Union

regardless of their location. However, it addresses key EU privacy issues and may be useful for any organization developing apps for individuals located in the European Union (EU). In addition, the ICO guidance should be read together with the opinion on mobile apps issued by the Article 29 Working Party (the body of European data protection regulators) in March 2013, a summary of which we have provided in a previous WSGR Alert.[2] Listed below are the key takeaways and recommendations from the guidance.

Takeaways and Recommendations

1. Unique device identifiers can be personal data: Under EU data protection law, personal data is interpreted broadly and may include information that is not limited to traditional identifiers such as an individual's name or photograph. According to the ICO, "a good example in the mobile environment would be a unique device identifier such as an IMEI number: even though this does not name the individual, if it is used to treat individuals differently it will fit the definition of personal data." The ICO notes that when an app developer is uncertain about whether the data is personal, it would be simpler to treat it as personal from the start.

2. Who is the data controller?: Under EU data protection law, data controllers are those that define the purposes and the means of the processing. They are generally responsible for ensuring compliance with data protection law (including filing a registration with ICO and responding to subject access requests), even if they contract out tasks such as hosting. For example, apps such as social media and advertisement-funded games (that decide how personal data is handled) will likely be data controllers. App developers are unlikely to be data controllers if the app code runs solely on a mobile device but does not collect or transfer data elsewhere.

> When designing the app, the ICO suggests considering the data types the app might access, collect, or transmit, and how these could affect a user of the app

According to the ICO, when developing an app on behalf of a client, "you may well not be a data controller," but rather a data processor. "If this is the case, expect the client to insist on a written contract which covers appropriate security measures."

3. Minimum data necessary: Apps should not collect and process more data than the minimum necessary to perform the tasks of the app. According to the ICO, "collecting data just in case you may need it in the future is bad practice, even when the user has consented," and it also increases the risks of accidental loss or misuse of the data. When designing the app, the ICO suggests considering the data types the app might access, collect, or transmit, and how these could affect a user of the app. In addition, "you should aim to use the least privacy-intrusive data possible." For example, ensure that a

[1] "Privacy in mobile apps - Guidance for app developers," UK ICO, *available at* http://ico.org.uk/for_organisations/data_protection/topic_guides/online/~/media/documents/library/Data_Protection/Detailed_specialist_guides/privacy-in-mobile-apps-dp-guidance.pdf, December 2013.

[2] "European Regulators Issue Opinion on Mobile Apps," WSGR Alert, *available at* http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-EU-mobile-apps.htm, March 22, 2013.

social media app by default strips out unnecessary metadata (e.g., creation date, location) from each image before uploading it. If an app uses GPS-location services to recommend activities near the user's location, design the app so that the device itself functions in the town closest to the user's location, thus avoiding the need to send exact GPS coordinates of the user's location back to the central server. Users who want results based on their accurate location can change the default behavior. Finally, users should be able to permanently delete their personal data and any account they may have set up.

4. Privacy policies: Users of the app must be properly informed about what will happen to their personal data if they install and use the app. However, it may be inconvenient for users to be presented with a lengthy privacy policy or numerous prompts. The ICO encourages alternative ways to provide information on a device with a small screen and a touch-based interface, such as the ones described in ICO's "Privacy notice code of practice." Furthermore, the ICO flags the following important points:

    - Use plain English
    - Use language appropriate to the audience (e.g., children)
    - Be transparent about which data the app wants and why
    - Make the privacy information available as soon as practicable, ideally before the user downloads the app (e.g., via the app store or a link to the privacy policy)
    - Use just-in-time notifications or other alert systems for more intrusive data (e.g., GPS location) or unexpected processing (e.g., uploading data to the Internet)

> The guidance is a practical example of how to implement the "privacy by design" and "privacy by default" principles that are supported by EU regulators and will most likely be included in the upcoming EU Data Protection Regulation

    - Use a "layered" approach (e.g., first present a summary of important points, including more detail that is readily available), if appropriate

5. Give users feedback and control: Users should be allowed to make meaningful decisions. The ICO recommends that rather than giving users a single "all or nothing" choice, give users a granular choice where possible. This includes allowing users to easily review and change their decisions after the app is installed and used (e.g., menu and settings, privacy-friendly defaults). In addition, if geolocation services are running in the background, consider using clear and recognizable icons to indicate that this is occurring and, where necessary, include an option to stop.

6. Keep the data secure: The ICO suggests ensuring that passwords are "appropriately salted and hashed on any central server." In addition, the ICO suggests using "encrypted connections to ensure security of the data in transit, using SSL/TLS for instance," especially where this incudes "transmitting usernames, passwords and any particularly sensitive information, including device IDs or other unique IDs." However, for transmitting or storing data, the ICO suggests using "tried and tested cryptographic methods, rather than implementing your own cryptography." Furthermore, "be particularly careful if your app accesses data from other apps or locations." Finally, "pay attention to vulnerabilities which are more relevant in a mobile apps environment" (e.g., inter-app injection flaws, failure to properly check SSL/TLS certificates).

Conclusion

The ICO guidance shows the need to consider privacy implications early on in the app development phase. It is a practical example of how to implement the "privacy by design" and "privacy by default" principles that are supported by EU regulators and will most likely be included in the upcoming EU Data Protection Regulation. The underlying message of the guidance is to take privacy into account at an early stage; this will help your app be compliant in the UK and other EU countries.

Tip

Forensic preservation and scene preservation can dramatically lower the costs of security incident investigation and remediation.

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