Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

EYE ON PRIVACY

SEPTEMBER 2013

Welcome

It's hard to believe that Summer is already over! In this month's issue of Eye on Privacy, we recap some significant developments since our last issue in May, including new state social media credential laws, FCC activity regarding personal information on mobile devices, the FTC's continued push on potential FCRA violators, and Delta's privacy litigation with the California Attorney General. We also provide a thorough discussion of the Digital Advertising Alliance's guidance on the application of its self-regulatory principles to mobile, and recent decisions and a significant upcoming change to the Telephone Consumer Protection Act.

Also, we have some upcoming webinars in the works on significant privacy developments, so please keep an eye on our events page for further announcements.

As always, please feel free to send us a note at PrivacyAlerts@wsgr.com if you have any suggestions for future article topics.

Lydia Parnes

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

Digital Advertising Alliance Releases Guidance on the Application of Its Self-Regulatory Principles to the Mobile Environment

New Self-Regulatory Guidance Joins Other Privacy and Transparency-Related Considerations for Participants in the Mobile Ecosystem

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

Tonia Klausner
Partner, New York
tklausner@wsgr.com

Matthew Staples
Associate, Seattle
mstaples@wsgr.com

On July 24, 2013, the Digital Advertising Alliance (DAA), comprised of the largest media and marketing trade associations in the U.S., released new guidance regarding mobile and other devices (Mobile Guidance).[1] The Mobile Guidance explains how the DAA's existing Self-Regulatory Principles for Online Behavioral Advertising (OBA Principles)[2] and Self-Regulatory Principles for Multi-Site Data (MSD Principles)[3] (together, the DAA Principles) apply to companies operating in the mobile ecosystem. It sets forth specific

Continued on page 2...

[1] Digital Advertising Alliance, "Application of Self-Regulatory Principles to the Mobile Environment," 2013, available at http://www.aboutads.info/DAA_Mobile_Guidance.pdf.

[2] Digital Advertising Alliance, "Self-Regulatory Principles for Online Behavioral Advertising," 2009, available at http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf.

[3] Digital Advertising Alliance, "Self-Regulatory Principles for Multi-Site Data," 2011, available at http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

In This Issue

Digital Advertising Alliance Releases Guidance on the Application of Its Self-Regulatory Principles to the Mobile Environment ..... Page 1-5

TCPA Update: Recent Decisions and Significant Upcoming Change to TCPA Rules ..... Page 6-7

Employee Social Media Accounts Protected Under New Laws ..... Page 8

FCC Actions Clarify that Mobile Data Security Rules Apply to Data on Devices ..... Page 8-10

Policing Privacy: Undercover FTC Staff "Test-Shop" Data Brokers to Identify FCRA Violators ..... Page 10-12

Delta Wins Dismissal of California AG Mobile App Privacy Action ..... Page 13-14

requirements for the collection and use of precise location information, as well as two new categories of data: "cross-app data" and "personal directory data."

By articulating clear obligations for companies with respect to these types of data, the Mobile Guidance represents a milestone for the mobile advertising industry, which has been debating how to provide adequate notice and choice to consumers for quite some time. Noncompliance ultimately will be subject to the Online Interest-Based Advertising Accountability Program, operated by the Council of Better Business Bureaus.[4] Participants in the mobile ecosystem—including app developers, analytics companies, ad networks, app platform providers, and providers of devices and related services—should evaluate their practices in light of the Mobile Guidance.

The Mobile Guidance arrives amid a crowded landscape of recent developments relating to privacy and transparency in the mobile context. It follows sets of best practices for the mobile space set forth by the Federal Trade Commission (FTC) in February 2013 and by California Attorney General Kamala Harris in January 2013. It also joins the draft Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices, developed through the multistakeholder process convened by the National Telecommunications and Information Administration (NTIA) regarding mobile app transparency, and temporarily "frozen" for use in testing by participating organizations on July 25, 2013.[5] The FTC's and California Attorney General Harris' recommendations, together with the NTIA's short-form notice code of conduct, once finalized, will join the Mobile Guidance in presenting several privacy- and transparency-related considerations for participants in the mobile space.

Background

In July 2009, the DAA published the OBA Principles, the online advertising industry's effort to establish standard business practices concerning the collection of information about people's online behavior across websites and its use in online behavioral advertising (OBA).[6] They consist of seven principles, most notably requirements of clear notice to consumers about the collection and use of data for OBA purposes, and consumer choice regarding whether such data can be used for OBA.[7] In 2011, the DAA expanded its self-regulatory program to cover "multi-site data," which is all data collected from particular computers or devices regarding web viewing over time and across unaffiliated websites, and not just that collected for OBA purposes.[8]

Mobile Guidance

The Mobile Guidance provides direction regarding how the DAA Principles apply within the mobile website and app environments. In particular, the Mobile Guidance:

- makes clear that the DAA Principles apply in the mobile context and elaborates on how they apply;
- explains how the DAA Principles apply to data collected on a particular device regarding app use over time and across non-affiliate applications (cross-app data)[9];
- explains how the DAA Principles apply to data about the physical location of a device that is sufficiently precise to locate a specific individual or device (precise location data); and
- explains how the DAA Principles apply to the collection, use, and disclosure of calendar, address book, phone/text log, or photo/video data created by a consumer that is stored on or accessed through a device (personal directory data).

The Mobile Guidance sets out responsibilities for first parties and third parties. A "first party" is an entity that owns or has control over an app with which a consumer interacts, as well as the entity's affiliates. An entity is a "third party" to the extent that it collects cross-app data or precise location data from or through a non-affiliate's application, or collects personal directory data from a device.[10]

Application of Self-Regulatory Principles Across Channels

The Mobile Guidance first emphasizes that the DAA Principles apply consistently across all channels, regardless of the type of computer or device involved.[11] In commentary, however, the DAA acknowledges the technical limitations of different types of

---

[4] Only after the DAA's choice mechanism for cross-app data is operational, and after an implementation period, will companies face DAA accountability mechanisms with respect to cross-app data, precise location data, and personal directory data. For information about the Interest-Based Advertising Accountability Program, see http://www.bbb.org/us/interest-based-advertising/.

[5] The NTIA's published Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices is available at http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf. The draft code has been released for purposes of user testing by participating companies, but has not yet been finalized.

[6] OBA is the collection of data from a particular computer or device regarding web-viewing behaviors over time, and across unaffiliated websites, for the purpose of using such data to predict user preferences or interests to deliver advertising to that computer or device based on those inferred preferences or interests. For example, through OBA, a consumer shopping online for baseball tickets might receive targeted ads on other, unaffiliated websites about baseball tickets or about other products that those shopping for baseball tickets may tend to be interested in (e.g., sports magazines).

[7] Digital Advertising Alliance, "Self-Regulatory Principles for Online Behavioral Advertising," 2009, available at http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf; Digital Advertising Alliance, "Self-Regulatory Principles for Online Behavioral Advertising Implementation Guide," 2010, available at http://www.aboutads.info/resource/download/OBA%20Self-Reg%20Implementation%20Guide%20-%20What%20Everyone%20Needs%20to%20Know.pdf.

[8] For additional information on the MSD Principles, please see our WSGR Alert at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-online-advertising-data-collection.htm.

[9] Cross-app data also includes unique values assigned or attributed to a device, or a unique combination of characteristics associated with a device, where combined with cross-app data. It does not include (i) precise location data, (ii) personal directory data, (iii) data that has been de-identified in accordance with the Mobile Guidance, or (iv) data that is collected across unaffiliated apps but is not associated or combined across such apps.

[10] In situations where it is clear that the consumer is interacting with a portion of an app that is not an ad and is being operated by a different entity than the app owner, the different entity would not be a third party due to the consumer's reasonable understanding of the nature of the direct interaction with that entity.

[11] As a result of the consistent application of the DAA Principles across channels, the principles should be considered in connection with the collection of data from computers and devices, such as navigation devices and connected television devices in addition to mobile devices.

Continued on page 3...

devices and systems. As a result, compliance with the DAA Principles in the mobile context may take a form different from compliance in the desktop computer environment, and implementation may vary based on the technological demands of other channels as well. The DAA anticipates providing further guidance on implementation practices.

Cross-App Data

Transparency

Under the Mobile Guidance, third parties should provide clear, meaningful, and prominent notice of their cross-app data collection and use practices. Such notice should be provided on the third parties' own websites or made accessible from any app from or through which they collect cross-app data.

Additionally, third parties should provide enhanced notice of their cross-app data collection and use practices by either using a notice in or around ads delivered using cross-app data (which can be satisfied through the use of the AdChoices icon) or in a number of ways that require the cooperation of the first party. If they do not provide enhanced notice in these ways, third parties should be listed individually on a mechanism or setting that meets DAA specifications and is linked from the first party's disclosure. Third parties who obtain consent[12] to their use and disclosure of cross-app data are not required to provide this enhanced notice.

Unless all third parties operating on the first party's app have provided enhanced notice or have obtained consent to their cross-app data collection and use practices, any first party who *affirmatively authorizes* a third party to collect and use cross-app data also should provide notice in a specified time and manner.

Consumer Control

Third parties should provide consumers with choice regarding their collection and use of cross-app data and should describe those choice mechanisms in the relevant notices described above. Additionally, first parties who affirmatively authorize third parties to collect and use cross-app data should link to an appropriate choice mechanism.

The Mobile Guidance also provides that entities should not collect and use cross-app data through their provision of a service or technology that collects cross-app data from all or substantially all apps on a device without obtaining consent and providing an ongoing, easy-to-use means for users to withdraw such consent.

Precise Location Data

Transparency

For precise location data, the Mobile Guidance imposes requirements similar to those in the DAA Principles, but allocates responsibility differently to account for first parties' greater ability to provide notice to consumers and obtain their consent in the mobile space.

First parties should provide notice of transfers of precise location data to third parties, as well as third parties' collection and use of such data from or through the first party's app and with the first party's affirmative authorization. This notice should be on the first party's website or accessible from or through the app from which precise location data is collected.

First parties also should provide enhanced notice regarding the collection and use of precise location data. The Mobile Guidance specifies permissible manners to provide such enhanced notice and notes that any method, or combination of methods, that provides equivalently clear, meaningful, and prominent enhanced notice is permissible.

Third parties should provide basic notice of their collection and use practices regarding precise location data on their own websites or made accessible from any app from or through which they collect precise location data.

Consumer Control

First parties should obtain consent (i) for their transfer of precise location data to third parties, (ii) for affirmatively authorized third parties to collect and use precise location data from or through the first party's app, and (iii) for their transfer of precise location data to non-affiliates. The first party also should provide an easy-to-use tool for users to withdraw such consent.

In addition, third parties should ensure that consent has been provided for their own precise location data practices, either directly or by obtaining reasonable assurances from the first party that it has obtained consent.[13]

Finally, the DAA notes in the Mobile Guidance that due to technical limitations of different devices and systems, it may not be feasible to comply with its guidance regarding precise location data on all devices in the same manner. The DAA may provide further guidance on implementation practices.

Personal Directory Data

The Mobile Guidance creates a new category of data, "personal directory data," which is "calendar, address book, phone/text log, or photo/video data created by a consumer that is stored on or accessed through a particular device."[14]

---

[12] The Mobile Guidance, consistent with the DAA Principles, defines "consent" as "an individual's action in response to a clear, meaningful, and prominent notice regarding the collection and use of data for a specific purpose."

[13] The Mobile Guidance lays out several illustrative actions that a third party may take to obtain reasonable assurances that a first party has obtained consent to its collection and use of precise location data. For example, a third party may obligate the first party contractually to obtain consent to the third party's data collection or use, or may verify that the first party publicly represents that it obtains consent to the transfer of precise location data to a third party.

[14] Personal directory data also includes unique values assigned or attributed to a device or a unique combination of characteristics associated with a device, where combined with data, meeting the definition of personal directory data. Personal directory data does not include data that is not associated with a specific individual or device, such as data that has been de-identified.

Continued on page 4...

The Mobile Guidance provides that third parties should not, without user authorization, intentionally access, obtain, and use personal directory data. Additionally, first parties should not affirmatively authorize any third party to do so.

Exceptions and Specific Restriction on Uses for Eligibility Purposes

The Mobile Guidance generally exempts first parties and third parties from their notice and choice obligations under the Mobile Guidance with respect to cross-app data, precise location data, and personal directory data that (i) is collected and used for specified purposes such as market research, product development, or operations and systems management, or (ii) has gone through, or within a reasonable period of time from collection goes through, an appropriate de-identification process. These exceptions are very similar to those contained in the MSD Principles. Also consistent with the MSD Principles, the Mobile Guidance specifies that, notwithstanding any of its other provisions, cross-app data, precise location data, and personal directory data should not be collected, used, or transferred for purposes of employment eligibility; credit eligibility; healthcare treatment eligibility; or insurance eligibility, underwriting, or pricing.

Other Mobile App Disclosure and Privacy Guidelines

The Mobile Guidance joins a number of other privacy-related considerations for app developers, ad networks, and other participants in the mobile app ecosystem, along with others potentially to come.

FTC Mobile Disclosures Report

As covered previously in *Eye on Privacy*,[15] the FTC issued a report in February 2013 encouraging all participants in the mobile ecosystem to work together to develop improved mobile privacy disclosures and industry best practices.[16] Notably, the FTC report recommends that app developers:

- publish appropriate privacy policies, and make them available through app stores/marketplaces;
- provide just-in-time disclosures and obtain affirmative express consent in order to collect information considered by the FTC to be sensitive;
- coordinate with ad networks, analytics companies, and other third-party service providers to obtain clear information about their privacy practices, in order to disclose them appropriately; and
- participate in self-regulatory programs, industry organizations, and trade associations to prepare uniform, short-form privacy disclosures.

The FTC's mobile privacy report also recommends that ad networks and other third parties (i) coordinate with app developers, so as to allow app developers to provide more accurate privacy disclosures, and (ii) work with platforms to develop, and then ensure effective implementation of, a Do Not Track system in the mobile context. To this end, in addition to various other recommendations for app trade associations and platform providers, the FTC mobile privacy report also recommends that app platform providers create and implement a Do Not Track mechanism consistent with the FTC's principles set forth in its consumer report on privacy.[17]

California Attorney General Best Practices for Mobile Privacy

Additionally, as also discussed previously in *Eye on Privacy*,[18] California Attorney General Kamala Harris released a report containing a set of privacy best practices for the mobile space in January 2013.[19] These best practices, which the report concedes in certain respects go beyond requirements of existing law, focus primarily on app developers who offer apps to California consumers. The report recommends that, among other things, they make an easily understood privacy policy available prior to app download and use enhanced measures outside of the privacy policy to alert users of, and give them control over, data practices that are not related to an app's basic functionality, or that involve sensitive information such as a user's precise location. The best practices also cover app platform providers, operating system developers, and mobile carriers, and provide specific guidance for each of them. Among other things, those best practices recommend that ad networks provide app developers with clear, comprehensive information on their privacy practices, and provide links to their privacy policies so that app developers may make them available to users before they download or activate their apps.

NTIA Mobile Application Transparency Multistakeholder Process

Finally, app publishers, ad networks, and others in the mobile ecosystem also should be aware of the multistakeholder

[15] FTC Releases Privacy Disclosure Guidelines for Mobile Ecosystem, WSGR *Eye on Privacy* (March 2013), available at http://www.wsgr.com/publications/PDFSearch/eye-on-privacy/Mar2013/#1.
[16] FTC Staff Report: Mobile Privacy Disclosures: Building Trust Through Transparency (February 2013), available at http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf. The report was issued by the FTC in view of its prior work in the mobile arena, together with panel discussions on, and written comments received in connection with, a March 2012 workshop focused on transparency in mobile apps.
[17] The FTC's report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012), is available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf. We summarize this report in our WSGR Alert available at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-FTC-final-privacy-report.htm. Since the issuance of the FTC's report, there has been significant industry effort at coming up with a uniform Do Not Track standard. As of the date of this publication, however, there is no industry-wide consensus on Do Not Track.
[18] California Attorney General Issues Privacy Practice Recommendations for Mobile Ecosystem, WSGR *Eye on Privacy* (March 2013), available at http://www.wsgr.com/publications/PDFSearch/eye-on-privacy/Mar2013/index.html#2_1.
[19] Attorney General Harris' report, Privacy on the Go: Recommendations for the Mobile Ecosystem (January 2013), is available at http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

Continued on page 5...

process convened by the National Telecommunications and Information Administration (NTIA) in June 2012,[20] whose participants continue to work toward developing a voluntary code of conduct to provide transparency in how companies providing apps and interactive services for mobile devices handle personal data.[21] This code of conduct, which would be adopted voluntarily by participating developers and publishers, has yet to be finalized, but generally seeks to settle on standard short-form notices that succinctly, and in a consistent format, set forth key information about data collected within apps and how that data is shared. The short form notices would be intended to help consumers compare and contrast data practices of apps, with the goal of enhancing consumer trust in app information practices.

Notably, the current draft NTIA code of conduct, which was frozen for user testing on July 25, 2013,[22] calls for transparency with respect to (i) the collection of certain types of sensitive data (such as biometrics, precise location information, user files, contact information on a mobile device, and web browser history or phone or text log), as well as (ii) any user-specific data shared with ad networks, carriers, consumer data resellers, data analytics providers, providers of operating systems, app platforms, other apps, and social networks, unless those third parties are bound by contract to limit the uses of any such consumer data solely to services rendered to, or on behalf of, that app and to abstain from sharing that consumer data with subsequent third parties. Notice requirements also do not apply with respect to data collected or shared without the app developer's affirmative authorization, so long as the app developer doesn't have actual knowledge of (or deliberately avoid obtaining actual knowledge of) such collection or sharing before it occurs. Finally, the code's notice requirements also do not apply with respect to the collection or sharing of any data that is not identified or that is otherwise promptly de-identified as long as reasonable steps are taken to prevent the data from being re-associated with a specific individual or device.

Implications

The Mobile Guidance likely will have significant ramifications for many participants in the mobile ecosystem. The FTC repeatedly has stated that the collection and use of information from mobile devices is one of its top agenda items because it believes consumers do not understand the collection that is occurring and how they can control it. The Mobile Guidance provides companies in the mobile space with much greater clarity regarding how to provide the transparency and consumer choice demanded by the FTC and privacy advocates. Members of the organizations that comprise the DAA, as well as other companies within the mobile industry, are encouraged to examine the Mobile Guidance in connection with a review of their own practices concerning the collection, use, and disclosure of cross-app data, precise location data, and personal directory data.

Additionally, the Mobile Guidance represents just one of several sets of guidelines issued recently regarding the collection and use of data by apps. Taken together, these various guidelines create a complex set of requirements and best practices for companies in the mobile ecosystem to consider.

---

[20] The NTIA's multistakeholder process on mobile app transparency was convened pursuant to the call for action in the Obama Administration's February 2012 report on consumer privacy, *Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (available at http://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf) (Administration Privacy Report), which, among other things, proposed a Consumer Privacy Bill of Rights and the establishment of multistakeholder processes to develop enforceable codes of conduct implementing that Consumer Privacy Bill of Rights. Our WSGR Alert regarding the Administration Privacy Report is available at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-consumer-privacy-bill-of-rights.htm.

[21] Information on the NTIA's process, including the most recent draft code of conduct, meeting agendas, and other documentation, is available at http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

[22] The current draft code of conduct is available at http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

Tip

Got health data? The effective date for the new HIPAA Privacy & Security Rule is TODAY!"

TCPA Update: Recent Decisions and Significant Upcoming Change to TCPA Rules

Tonia Klausner
Partner, New York
tklausner@wsgr.com

Michael Wolk
Associate, Palo Alto
mwolk@wsgr.com

Angel Díaz, San Francisco
Summer Associate

Congress enacted the Telephone Consumer Protection Act (TCPA)[1] on December 20, 1991, to address certain telephone and facsimile marketing practices that Congress found to be an invasion of consumer privacy. In general, and among other things, the TCPA prohibits unsolicited fax advertisements and automated or prerecorded calls (interpreted to include text messages) to cellular telephones or other devices for which the consumer would bear the cost of the call.[2] Congress vested the Federal Communications Commission (FCC) with authority to issue regulations implementing the TCPA. Pursuant to that authority, the FCC has issued a series of detailed and complex rules and regulations interpreting and implementing the statute's requirements.

Over the past decade, U.S. courts have been inundated with putative class actions asserting alleged violations of the TCPA. The statute contains a private right of action provision entitling a successful individual plaintiff to $500 per violation without regard to the defendant's state of mind, and up to $1,500 per "willful" violation. When filed as a putative class action on behalf of all recipients of a "fax blast" marketing campaign, or all recipients of an automated text message over a four-year period, the potential exposure for the defendants can be massive. These cases have become a popular area for plaintiffs' class action counsel, who stand to recover substantial attorneys' fees just for filing a recycled complaint based on a single fax or text message.

Recently, two courts have ruled in favor of defendants in putative TCPA class actions. In *Roberts v. PayPal*, a California district court held that the plaintiff's voluntary act of providing his cell phone number to PayPal constituted "prior express consent" under the TCPA to receive automated and prerecorded calls (and texts) from PayPal to that number, which defeated the individual plaintiff's claim.[3] In *Compressor Eng. Corp. v. Manufacturers Fin. Corp.*, an Illinois district court denied class certification based on the lack of an ascertainable class due to issues regarding who had standing to sue based on receipt of an unsolicited facsimile advertisement.[4] While the FCC's proposed upcoming changes to its TCPA rulemaking would limit the long-term value of the first decision to defendants faced with TCPA text class actions, the second decision may offer a longer-term basis to defeat TCPA unsolicited fax class actions.

Roberts and the Issue of "Prior Express Consent" for Calls to Cell Phones Under the TCPA

The TCPA prohibits the use of any "automatic telephone dialing system" to call any telephone number assigned to a cellular telephone service absent an emergency purpose or the "prior express consent of the called party."[5] Although the statute refers to "calls," the FCC has concluded that a "call" includes the transmission of a text message to a cellular telephone number.[6] Additionally, the statute defines "automatic dialing system" to mean any system that has the "capacity" to "store or produce numbers and dial those numbers at random, in sequential order, or from a database."[7] Thus, many putative TCPA class actions are based on text messages allegedly sent to users of a service using equipment with the capacity to function as an autodialer.

Roberts v. PayPal addressed such a claim and ruled in favor of the defendant. There, the court ruled on summary judgment that PayPal had obtained the plaintiff's "prior express consent" to send the plaintiff a text message using an autodialer when the plaintiff voluntarily submitted his cell phone number to PayPal. As a result, the text messages PayPal sent regarding PayPal's mobile services did not violate the TCPA.[8] The court looked to the FCC's guidance regarding the meaning of the phrase "prior express consent," which concluded that "persons who knowingly release their phone numbers have in effect given their invitations or permission to be called at the number which they have given, absent instructions to the contrary."[9] This decision cites and is consistent with *Pinkward v. Walmart*, where another district court found a consumer's act of voluntarily providing a cell phone number to Wal-Mart's pharmacy to constitute express consent under the TCPA to receive text messages from Wal-Mart, even though Wal-Mart did not explicitly

---

[1] 47 U.S.C. § 227.
[2] 47 U.S.C. § 227(b)(1)(C); *In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 18 F.C.C.R. 14014, 14115 (July 3, 2003). The TCPA also regulates automated and prerecorded calls to residential phone lines.
[3] No. C 12-0622 PJH, slip op. at 7 (N.D. Cal. May 30, 2013).
[4] No. 09-14444, slip op. at 15 (E.D. Mich. April 26, 2013).
[5] 47 U.S.C. § 227(b)(1)(A).
[6] *In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 18 FCC Rcd. 14014, 14115 (July 3, 2003). Numerous courts have adopted this interpretation. *See, e.g., Saterfield v. Simon & Schuster, Inc.*, 569 F.3d 946, 954 (9th Cir. 2009).
[7] *Id.* at 14092.
[8] *Roberts*, slip op. at 6.
[9] *See In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 7 F.C.C.R. 872, 8769 (Oct. 16, 1992).

Continued on page 7...

seek permission for the company to send text messages.[10,11]

The *Roberts* court distinguished its holding from the Ninth Circuit's decision in *Satterfield v. Simon & Schuster*, where the court rejected the argument that the plaintiffs had consented to receive the text messages at issue by voluntarily disclosing their cell phone numbers. In *Satterfield*, the plaintiffs voluntarily provided their cell phone numbers to a company called Nextones in order to receive a free ringtone, but then received a text message from a third party (Simon & Schuster) that had purchased a list of the Nextones subscribers to deliver them advertisements.[12] The *Satterfield* court held that the plaintiff's consent did not extend to an unrelated third party, as the plaintiffs were told they were only consenting to receiving communications from Nextones or its affiliates and brands.[13] In *Roberts,* in contrast, the text messages were from PayPal itself—the company to whom the plaintiff had voluntarily provided his cell phone number—not a third party.

The *Roberts* decision demonstrates a context-sensitive approach for determining whether "prior express consent" has been given to send text messages to a cell phone consistent with the FCC's current interpretation of that phrase. *Roberts* and the FCC's existing interpretation result in a common-sense outcome whereby a business may contact a consumer via a phone number voluntarily provided by the consumer directly to that business without violating the TCPA.

Unfortunately, and significantly, the FCC has issued new rulemaking effective October 16, 2013, that will eliminate its common-sense and business-friendly interpretation of "prior express consent" and replace it with an onerous prior ***express written*** consent requirement.[14] The FCC's upcoming changes may inhibit the future applicability of the *Roberts* and earlier *Pinkard* and *Satterfield* decisions, particularly with respect to calls and text messages to cellular telephone numbers made or sent after October 16, 2013. At minimum, the new requirements will provide plaintiffs' class action counsel with new grist for their TCPA mills.

Compressor and Standing to Sue for Violation of the Fax Advertising Provisions of the TCPA

Compressor addressed an action for alleged violation of the TCPA's prohibition on sending faxed advertisements without prior permission, and without an established business relationship with the recipient. The plaintiffs claimed receipt of such prohibited faxes and sought certification on behalf of a class of "all persons who were sent" the faxes at issue. The court denied the plaintiffs' motion for class certification due to the lack of an ascertainable class and because the claims are inherently individualized, as they only extend to unsolicited faxes.

Looking at the TCPA's legislative history, the *Compressor* court found that Congress sought to combat the uptake in "junk" faxes, which, among other things, shift the costs of printing advertisements from the sender to recipient.[15] The *Compressor* court held that the plaintiff's proposed class of persons who were sent fax advertisements was unnecessarily broad, as it could include everyone from the person to whom the fax was addressed to the person who happened to pick up the transmission, and failed to include a requirement that class members owned the fax machines that received the fax advertisements at issue. As defined, and particularly in light of the fact that the faxes were sent primarily to businesses, it was not clear that only persons with standing to pursue a claim would fall within the class.

The court went on to conclude that even if the plaintiffs modified their class definitions to include those with statutory standing, or limited it to recipients of "unsolicited" faxes, class certification would still be inappropriate because standing would remain dependent on an individualized determination.

The *Compressor* decision is likely to prove useful to defendants in TCPA unsolicited fax advertisement cases, particularly where the faxes at issue were sent to doctors' offices or other businesses where more than one person may utilize a fax machine and fax numbers change over time.

---

[10] 2012 WL 5511039 (N.D. Ala. Nov. 9, 2012).
[11] A district court in Florida has rejected the FCC's interpretation and concluded that the voluntary provision of a cell phone to a business does not amount to "express" consent to receive text messages from that business. *Mais v. Gulf Coast Collection Bureau*, No. 11-61936, 2013 WL 1899616 at *9 (S.D. Fla. May 8, 2013).
[12] 569 F.3d at 949.
[13] *Id.* at 955.
[14] *In re Rules and Regulations Implementing The Telephone Consumer Protection Act of 1991*, Report and Order, 27 F.C.C.R. 1830, 1831 (Feb. 15, 2012).
[15] *Compressor* at 16.

Employee Social Media Accounts Protected Under New Laws

Laura Merritt
Partner, Austin
lmerritt@wsgr.com

Emily Schlesinger
Associate, Seattle
eschlesinger@wsgr.com

Rebecca Stuart
Associate, Palo Alto
rstuart@wsgr.com

On April 30, 2013, Washington's state legislature passed SB 5211, which prohibits employers from requesting social media log-in information from applicants and employees. The bill, which was signed into law by Washington's governor on May 21, 2013, and went into effect on July 28, 2013, makes Washington the sixth state to pass a social media privacy law, after Maryland, Illinois, California[1] Michigan, and Utah.

Similar to new state laws across the country governing employer social media policies, Washington's SB 5211 prohibits employers from requesting, requiring, or coercing an employee or applicant to disclose his or her social media password, log into a social media site in the employer's presence, or change his or her privacy settings. The law also prohibits an employer from compelling or coercing an employee or applicant to add the employer to a social networking site as a "friend." As with similar state laws, Washington employers cannot take adverse action against an employee for refusing to take any of the actions prohibited by the law. Notably, however, there are exceptions allowing an employer to seek social media credentials for either use in investigations or job-related social media accounts.

In the absence of a federal statute addressing employer requests for social media credentials, states are continuing to pass social media privacy laws. As of July 2013, laws prohibiting employers from requiring or requesting social media credentials are pending or have been passed in the following 30 states: Arizona, Arkansas, California, Colorado, Connecticut, Georgia, Hawaii, Illinois, Iowa, Kansas, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Dakota, Oregon, Rhode Island, Texas, Utah, Vermont, and Washington.

As the law in this area evolves, employers should remain vigilant regarding restrictions placed on them by state law, and exercise caution in requesting social media credentials from employees or applicants. Moreover, employers must keep in mind that even in states without a social media law in place, they might invariably access information while viewing an applicant or employee's social media site that could open them up to later liability, such as information on the individual's race, sex, religious affiliation, or a similar protected category.

[1] "New California Law Gives Employees and Job Applicants Greater Social Media Use Protections," WSGR Alert, October 11, 2012.

FCC Actions Clarify That Mobile Data Security Rules Apply to Data on Devices

Gerard Stegmaier
Of Counsel, Washington, D.C.
gstegmaier@wsgr.com

Wendell Bartnick
Associate, Washington, D.C.
wbartnick@wsgr.com

Telecommunications carriers must take precautions to protect call and location data stored on customers' devices, according to the Federal Communications Commission (FCC).[1] As discussed in a prior WSGR *Eye on Privacy* article,[2] the FCC reacted to the carriers' use of Carrier IQ to collect customers' call information, despite its data security vulnerabilities. The FCC sought public comment on whether this type of data collection should fall within the agency's authority under the Communications Act of 1934, as amended. After reviewing public comments, the FCC issued a Declaratory Ruling concluding that carriers must provide safeguards for certain types of data that carriers cause to be stored on their customers' devices directly or through their agents. This security requirement applies to data transferred to carriers' systems as well as data stored on the consumers' devices.

This ruling affects any service providers collecting call and location data from devices on behalf of telecommunications carriers. Following the ruling, many carriers, as well as those providing services to them, are expected to review how they collect, use, and share information. These service

[1] *In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, FCC 13-89 (June 27, 2013) (hereinafter *Declaratory Ruling*).
[2] The article is available at http://www.wsgr.com/publications/PDFSearch/eye-on-privacy/July2012/index.html#6.

Continued on page 9...

providers also can expect increased diligence from carriers and additional contractual requirements before forming business relationships.

This Declaratory Ruling does not directly apply to apps and service providers collecting call and location data from devices at the direction of *consumers*. However, past experience suggests that agencies commonly are influenced by complementary actions of their fellow agencies. Therefore, the Federal Trade Commission (FTC), which has taken an active role in privacy and data security enforcement, may look at applying similar requirements to the entities it regulates. Moreover, while the apps and service providers are not directly at risk for any violations of the Communications Act, the FTC may investigate any apps or service providers involved in any matters raised by the FCC against a carrier.

Customer Proprietary Network Information (CPNI).

The FCC reviewed how Section 222 of the Communications Act applied to customer proprietary network information collected and stored on mobile devices. CPNI includes customer-specific personal information related to an individual's use of a telecommunications service, including dialed phone numbers; frequency, time, and duration of calls; device technical configuration; and the location where calls are dialed or received. To be CPNI, the data must be available to the carrier solely by virtue of the carrier-customer relationship. Specifically, the FCC analyzed whether the above-listed information collected through pre-installed applications or forced updates and stored on the device constituted CPNI. If the data stored on consumers' devices is CPNI, then Section 222's privacy protections apply. Section 222 establishes several requirements for telecommunications carriers, including the duty to "protect the confidentiality" of CPNI.

FCC Removes Industry Uncertainty.

The FCC noted that the wireless industry was uncertain about its obligations under Section 222 to protect CPNI collected by mobile devices. Through this Declaratory Ruling, the FCC intended to remove the uncertainty. The agency stated that the security obligations apply to CPNI collected at the carrier's direction when the carrier or its agent has access to, or control over, such information. This includes access, or control over, information while it is stored on the device. The FCC came to this conclusion after finding that telecommunications carriers were in a position to protect the privacy and security of information collected in such a manner.

Carriers Must Implement "Reasonable" Security Measures.

The FCC emphasized that the ruling does not ban the collection and use of CPNI; instead, the agency clarified that CPNI must be protected and used only as permitted by law. The FCC stated that it expects carriers to take "reasonable measures" to secure customer information, and such measures may vary based on the sensitivity of the information. For example, the FCC previously has stated that a carrier must encrypt its CPNI databases if it would provide significant additional protection at a reasonable cost given the technology a carrier already has implemented.[3] However, in its Declaratory Ruling, the FCC did not require any particular type of safeguard and allows carriers to choose their own methods of protecting CPNI.

Data Not Yet Transmitted to Telecommunications Carrier Still Must Be Protected.

The FCC stated that the fact that CPNI located on the device has not yet been transmitted to the carrier does not remove the duty that carriers have to protect the data collected at its direction. According to the FCC, a telecommunications carrier need not receive CPNI to have security obligations; it is enough that they caused the data to be stored on the customers' mobile devices.

Declaratory Rule Does Not Apply to Third-Party Apps.

Third-party apps installed by customers also may raise privacy concerns. However, the FCC's ruling makes clear that Section 222 does not cover customer-installed third-party apps and their data collection. Information stored on a mobile device that is not accessible by the carrier as part of providing the telecommunications service is not CPNI.

No Effect on Data Use for Network Maintenance and Improvement.

The FCC's ruling does not limit data collection. In general, the existing CPNI rules focus on usage limitations and obtaining appropriate consent after notice. The FCC reiterated that telecommunications carriers can collect CPNI without consent to improve and maintain their networks. The Declaratory Ruling clarifies, however, that such information should be secured.

No Effect on Aggregate Information.

Section 222 does not impose a duty to protect all data collected or stored on a device by a telecommunications carrier or its agents. Aggregate customer information (i.e., information "from which individual customer identities and characteristics have been removed") is not subject to confidentiality obligations under Section 222, which are intended to protect "individually identifiable" CPNI.[4]

FCC Does Not Support Self-Regulatory Codes of Conduct.

Unlike the FTC's support for self-regulatory codes of conduct, the FCC has taken the position that self-regulatory initiatives are not a substitute for the agency fulfilling its

[3] *Report and Order and Further Notice of Proposed Rulemaking*, 22 FCC Rcd 6927, 6959 ¶ 64 (2007).
[4] *Declaratory Ruling*, FCC 13-89, at 12-13.

Continued on page 10...

FCC Actions Clarify . . . *(continued from page 9)*

statutory role. Congress specifically has imposed statutory duties upon carriers with respect to CPNI through the Communications Act. Therefore, the FCC may not deem compliance with self-regulatory standards as compliance with obligations under Section 222.

Enforcement.

The FCC warned that it would hold carriers accountable for compliance with these statutory and regulatory obligations. Carriers' inadvertent disclosures of CPNI—even CPNI that resides solely on customers' mobile devices—may violate Section 222, depending on the facts and circumstances of the case. For example, carriers may be liable for unauthorized access and disclosure by third-party apps to the CPNI collected and stored by the telecommunications carrier or its agents on the device.

Implications.

Telecommunications carriers likely face increased pressure to provide reasonable safeguards of the data they and their agents store on customers' mobile devices. As a result, carriers likely will take an active role to ensure that any third-party apps installed at the direction of a carrier collect and store information on mobile devices using security measures that meet the FCC's requirements. Businesses working with carriers in these areas can continue to expect stringent indemnity requirements and representations regarding compliance, privacy, and data security in their agreements with carriers. Importantly, third-party apps that are installed by customers do not fall under the authority of the FCC. However, these third-party apps likely fall under the jurisdiction of the FTC, which also expects apps to have reasonable data security.

Whether the two agencies' requirements and approaches will parallel one another remains to be seen. Neither the FCC nor the FTC has undertaken rulemaking or other authoritative measures to define the parameters of "reasonable" security for mobile applications. It seems likely that some level of uncertainty will persist as telecommunications carriers and apps and service providers seek through trial and error to satisfy requirements and avoid investigations and penalties. Following this latest ruling, companies may benefit from renewed review and evaluation of their privacy and data protection practices.

Policing Privacy: Undercover FTC Staff "Test-Shop" Data Brokers to Identify FCRA Violators

Valentina Rucker
Associate, Washington, D.C.
vrucker@wsgr.com

Ted Serra,
Summer Associate,
Washington, D.C.

In early May, Theodore Moss, the CEO of online background-check provider Crimcheck.com, received a letter from the Federal Trade Commission (FTC) notifying him that "recent test-shopping contacts" had indicated that his company was possibly selling consumer information unlawfully.[1] Crimcheck.com provides background-check services to businesses conducting employment screenings for potential job candidates.[2] Such companies, often referred to as "data brokers," collect and compile information on individual consumers, drawing from public sources such as court databases and consumer credit records to piece together profiles of individuals' financial, retail, recreational, and criminal behaviors.[3] But it is precisely that assembling of detailed information on individuals—even information compiled from public sources—that can trigger provisions of the Fair Credit Reporting Act, prompting the FTC to take a closer look at how these companies collect and use consumer information.

The Fair Credit Reporting Act

Under the Fair Credit Reporting Act (FCRA), consumer information used for employment, insurance, or credit purposes is subject to certain safeguards.[4] Enacted in 1970, the FCRA was designed "to ensure fair and accurate credit reporting, promote efficiency in the banking system, and protect consumer privacy."[5] Section 1681a(f) defines a "consumer reporting agency" (CRA) as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . ."[6] The

[1] Letter from Maneesha Mithal, Associate Director, Federal Trade Commission, to Theodore Moss, CEO, Crimcheck.com (May 3, 2013), *available at* http://www.ftc.gov/os/2013/05/130507databrokerscrimcheck.pdf.
[2] Crimcheck.com, http://www.crimcheck.com (last visited June 19, 2013).
[3] Natasha Singer, "Congress to Examine Data Sellers," *The New York Times*, July 24, 2012, *available at* http://www.nytimes.com/2012/07/25/technology/congress-opens-inquiry-into-data-brokers.html; Craig Timberg, "FTC Warns Data Brokers on Privacy Rules," *The Washington Post*, May 7, 2013, *available at* http://articles.washingtonpost.com/2013-05-07/business/39090758_1_data-brokers-personal-data-data-reports. Those profiles can then be sold to third parties for a variety of purposes. *Id.* According to one estimate, U.S. companies spend over $2 billion annually on such personal data from third-party providers. Danny Yadron, "FTC Says Brokers Bid Private Data," *The Wall Street Journal*, May 7, 2013, *available at* http://online.wsj.com/article/SB10001424127887323687604578469392421956334.html.
[4] *See* 15 U.S.C. § 1681 *et seq.*
[5] *Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 52 (2007).
[6] 15 U.S.C. § 1681a(f).

Continued on page 11...

term "consumer report" is further defined to include virtually any information used for extension of personal credit, insurance, or employment purposes.[7] Read together, these two provisions indicate that an entity that collects consumer information later used for credit, insurance, or employment determinations is a CRA for purposes of the FCRA.

Qualifying as a CRA is consequential because it triggers a number of consumer protection measures. Among other steps, CRAs must do the following:

- Use reasonable measures to ensure that information contained in their reports is as accurate and up-to-date as possible[8]
- Ensure that the information will only be used for a permissible purpose under the statute[9] (Section 1681b lists the exclusive set of permissible purposes)
- Obtain certification that consumer reports for employment purposes will be used in compliance with equal opportunity laws and that the potential employee authorized the report and has an opportunity to challenge any contents that result in adverse action[10]
- Ensure that consumer reports for credit evaluations be used only for *firm* offers of credit[11]
- Inform data buyers of their own FCRA obligations[12]

Clearly, an entity's designation as a "consumer reporting agency" under the FCRA carries some substantial obligations.

FTC Enforcement Efforts

In recent years, the FTC has renewed its efforts to enforce the FCRA to protect consumer privacy. In December 2012, the FTC launched a study of the "data broker" industry, ordering nine different companies to disclose information concerning their collection and use of consumer data.[13] Those orders followed on the heels of several earlier settlements with data brokers, with one, Teletrack, settling for $1.8 million after the FTC alleged that it unlawfully sold consumer report information without a permissible purpose.[14] Another case, in which the FTC alleged that data broker Spokeo unlawfully marketed its consumer information to companies for use in hiring or recruiting, settled for $800,000.[15]

In May, the FTC conducted a sting operation to identify companies that provide or were willing to provide consumer information to buyers without complying with FCRA safeguards. FTC staffers targeted 45 data brokers, posing as company representatives or individuals seeking to purchase consumer information for use in screening consumer creditworthiness, insurance eligibility, or employment suitability.[16] While a company may promote its products exclusively for marketing purposes, in the FTC's view, "[e]ven if a company is not compiling and sharing data for the specific purpose of making employment, credit, or insurance eligibility decisions, if the company has reason to believe the data will be used for such purposes, it would still be covered by the FCRA."[17] According to the FTC, employees at ten companies were unaware of the necessary FCRA safeguards when selling consumer information for such purposes.[18] Among the ten, six—Crimcheck.com, 4Nannies, Case Breakers, People Search Now, USA People Search, and U.S. Information Search—seemed willing to sell data for employment determination purposes; two—Brokers Data and US Data Corporation—seemed willing to sell data for insurance decisions; and two—ConsumerBase and ResponseMakers—seemed willing to sell pre-screened lists for credit offers.[19] The FTC subsequently sent these ten companies warning letters, recommending that the companies review their products, internal policies and procedures, and employee training programs for compliance with the FCRA.[20]

The FTC noted that it was warning the recipients but that the letters were not formal complaints since it had not "evaluated" the companies' practices for FCRA compliance.[21]

---

[7] 15 U.S.C. § 1681a(d).
[8] *See* 15 U.S.C. § 1681e(b).
[9] *See* 15 U.S.C. § 1681e(a).
[10] *See* 15 U.S.C. §§ 1681b(a), 1681b(b).
[11] Letter from Maneesha Mithal, Associate Director, Federal Trade Commission, to Eric Rothchild, ResponseMakers (May 6, 2013), *available at* http://www.ftc.gov/os/2013/05/130507databrokersresponsemakers.pdf.
[12] *See* 15 U.S.C. § 1681e(d).
[13] Press Release, Federal Trade Commission, "FTC to Study Data Broker Industry's Collection and Use of Consumer Data" (Dec. 18, 2012), *available at* http://www.ftc.gov/opa/2012/12/databrokers.shtm.
[14] Press Release, Federal Trade Commission, "Consumer Reporting Agency to Pay $1.8 Million for Fair Credit Reporting Act Violations" (June 27, 2011), *available at* www.ftc.gov/opa/2011/06/teletrack.shtm.
[15] Press Release, Federal Trade Commission, "Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA" (June 12, 2012), *available at* http://www.ftc.gov/opa/2012/06/spokeo.shtm.
[16] Press Release, Federal Trade Commission, "FTC Warns Data Broker Operations of Possible Privacy Violations" (May 7, 2013), *available at* http://www.ftc.gov/opa/2013/05/databroker.shtm.
[17] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change" (Mar. 2012). For example, when FTC staffers contacted US Data Corp. and expressed an intention to purchase data for insurance eligibility purposes, such a stated intention constituted sufficient notice to render the data covered by the FCRA even if US Data only promoted its products for use in marketing. *See* Letter from Maneesha Mithal, Associate Director, Federal Trade Commission, to Jeff Herdzina, US Data Corporation (May 2, 2013), *available at* http://www.ftc.gov/os/2013/05/130507databrokersusdata.pdf.
[18] Yadron, *supra* note 3.
[19] Mithal, *supra* note 11; Lesley Fair, "FTC Staff Goes Shopping for Info – with Interesting Results," FTC Business Center Blog (May 7, 2013), http://business.ftc.gov/blog/2013/05/ftc-staff-goes-shopping-info-%E2%80%94-interesting-results.
[20] Mithal, *supra* note 1.
[21] *See, e.g.*, Mithal , *supra* note 11; Fair, *supra* note 19.

Continued on page 12...

However, the FTC specifically pointed to the *Teletrack* settlement as an example of the penalties it could seek, as well as to another recent settlement in which a data broker was enjoined from certain practices and required to adopt FCRA compliance procedures for a period of 20 years.[22]

A Global Push

Internationally, the FTC's efforts were complemented by similar actions by other member nations in the Global Privacy Enforcement Network (GPEN).[23] According to its mission statement, GPEN aims to "connect[] privacy enforcement authorities from around the world to promote and support cooperation in cross-border enforcement of laws protecting privacy."[24] For 2013, GPEN member states are focusing on privacy practice transparency.[25] Other member countries, including Canada, the UK, Australia, Germany, and Hong Kong, participated in their own compliance efforts in early May.[26] In Canada, for instance, authorities conducted a "sweep" of numerous popular websites to check for privacy policies and contact information.[27]

Continuing Efforts

The FTC's sting operation, coupled with the actions of its international peers, is further evidence that regulatory authorities are keeping their eyes on privacy. As for the recipients of the FTC's warning letters, there have been some mixed reactions, both to the commission's interpretation of the FCRA and to its test-shopping operation. Even while the FTC has taken the position that CRAs, as defined by Section 1681a(f), encompass more than traditional credit bureaus,[28] a few of the companies dispute whether they acted unlawfully or are CRAs to begin with. Mr. Moss, for his part, acknowledged that Crimcheck.com is a CRA, though he insisted that his company was in compliance with the FCRA.[29] In contrast, Eric Kaminsky, CEO of US Data Corporation, disputed the FTC's characterization of his business as a CRA, while at the same time praising the commission's efforts to "catch people who are bad guys."[30]

Even if the recipients agree that the FTC is right to go after the "bad guys," the enforcement efforts are instead most likely to impact the unaware. Indeed, one goal of the FTC is to raise awareness about consumer privacy issues and to encourage businesses that unknowingly or unintentionally may be in violation of the FCRA to revisit their practices.[31] Whether or not consumer information is sourced from public records or gathered only for marketing or sales purposes, it still may be subject to the FCRA's many safeguards, depending on the information buyer's purpose or intentions. Companies would be well advised to ensure their FCRA compliance, to avoid ending up on the FTC's warning-letter mailing list.

---

[22] Mithal, *supra* note 1 (citing *In the Matter of Filiquarian Publishing, LLC*, FTC File No. 112 3195 (May 1, 2013)).
[23] Fair, *supra* note 19 (adding that GPEN "[n]etwork members are taking steps this [same] week to encourage companies to meet their obligations about the privacy of consumers' personal information").
[24] "Action Plan for the Global Privacy Enforcement Network (GPEN)," Global Privacy Enforcement Network, https://privacyenforcement.net/public/activities (last amended Jan. 22, 2013).
[25] Press Release, Office of the Privacy Commissioner of Canada, "Global Privacy Enforcement Network Internet Privacy Sweep: Questions and Answers" (May 6, 2013), *available at* http://www.priv.gc.ca/media/nr-c/2013/nr-c_130506_qa_e.asp.
[26] *Id.*
[27] *Id.*
[28] Federal Trade Commission, *supra* note 17, at 68 ("The Commission has monitored data brokers since the 1990s, hosting workshops, drafting reports, and testifying before Congress about the privacy implications of data brokers' practices.") (citing "Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the Senate Committee on Banking, Housing, & Urban Affairs," 109th Congress 7-8 (Mar. 10, 2005) (statement of FTC Chairwoman Deborah Platt Majoras), *available at* http://www.ftc.gov/os/testimony/050310idtheft.pdf ("Although the most common example of a 'consumer report' is a credit report and the most common CRA is a credit bureau, the scope of the FCRA is much broader. . . . CRAs other than credit bureaus provide many different types of consumer reports. . . . Data brokers are subject to the requirements of the FCRA only to the extent they are providing 'consumer reports.'")).
[29] "Crimcheck.com Complies with the Federal Fair Credit Reporting Act (FCRA)," PRWeb, May 8, 2013, http://www.prweb.com/releases/2013/5/prweb10713337.htm ("CEO, Ted Moss of Crimcheck.com stated that his company is in fact a CRA and has always complied with and will continue to comply with the FCRA. 'Our firm has rigorous procedures which ensure maximum possible accuracy when conducting employment screening, all of our clients are put through a comprehensive due diligence process before they can order employment screening reports and they are thoroughly explained their obligations as well as the applicants[']s rights under the FCRA.' Moss furthered that, 'To surmise that a call to a receptionist is evidence of wrong doing is like assuming the receptionist at your doctor's office is qualified to give medical advice, the people who answer our phones do not set up new accounts and we do not sell data in the sense that the FTC implies. If the FTC expects to protect consumers they [*sic*] should at least get the facts straight.'").
[30] Katie Kaye, "FTC Sting Operation Results in Warnings to 10 Data Brokers," *Ad Age*, May 7, 2013, http://adage.com/article/privacy-and-regulation/ftc-data-shopping-sting-results-warnings-10-data-brokers/241335.
[31] Timberg, *supra* note 3 (quoting attorney for FTC's Bureau of Competition that the warning letters hopefully would raise awareness of privacy issues and FCRA compliance).

Delta Wins Dismissal of California AG Mobile App Privacy Action

Tonia Klausner
Partner, New York
tklausner@wsgr.com

Emily Schlesinger
Associate, Seattle
eschlesinger@wsgr.com

At a May 9, 2013, hearing, the California Superior Court dismissed the lawsuit that California Attorney General Kamala Harris filed against Delta Airlines in December 2012.[1] As reported in the January 2013 issue of *Eye on Privacy*,[2] the state's lawsuit alleged that the company's "Fly Delta" mobile application (app) violated the California Online Privacy Protection Act (CalOPPA) by failing to provide required privacy disclosures.[3] The AG sought enforcement of CalOPPA through California's Unfair Competition Law (California UCL).[4] According to the AG, Delta violated CalOPPA by "fail[ing] to conspicuously post a privacy policy in its Fly Delta app" despite the AG's earlier written notice of non-compliance, and because the Fly Delta app failed to comply with the privacy policy posted on Delta's website.[5] The court dismissed the action based on its conclusion that the state law claim was preempted by the Federal Airline Deregulation Act of 1978 (ADA).[6]

While this specific holding would not apply to most companies offering consumer apps, the action demonstrates the California AG's intent to vigorously enforce CalOPPA in the context of such apps based on her position that mobile apps collecting personally identifiable information (PII) are "online services" under CalOPPA.

Background on CalOPPA

Enacted in 2004, CalOPPA was the first state law in the country to require owners of commercial websites or online services to post a distinctive and easily accessible link to a privacy policy.[7] The law requires operators of commercial websites or online services that collect PII through the Internet from California consumers who visit the site or use the service to "conspicuously" post a privacy policy on their site that informs consumers about the categories of PII collected on the site, as well as the categories of third parties with whom that PII is shared. The law also requires operators of online services to make such a policy reasonably accessible to users.

The statute specifically defines PII as "individually identifiable information about an individual consumer," including: "(1) a first and last name; (2) a home or other physical address, including street name and name of a city or town; (3) an e-mail address; (4) a telephone number; (5) a social security number; (6) any other identifier that permits the physical or online contacting of a specific individual; [and] (7) information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in [the statute]."[8] The privacy policy itself must contain the following information:

- A list of the categories of PII the operator collects;
- A list of the categories of third parties with whom the operator shares that PII;
- A description of the process by which the consumer can review and request changes to the PII the operator collects from him or her;
- A description of the process through which consumers are notified that the operator has materially changed its privacy policy; and
- The privacy policy's effective date.[9]

Further, under CalOPPA, a "conspicuous" post means any of the following:

- The privacy policy appears on the website's homepage;
- The privacy policy is directly linked to the website's homepage through an icon containing the word "privacy" and it appears in a color different from the background color of the homepage itself; or
- The privacy policy is linked to the website's homepage through a hypertext link containing the word "privacy," in all capital letters either equal to or greater than the size of the surrounding text, in a color that differs from the background color of the homepage.[10]

The California AG's Enforcement of CalOPPA in the Context of Mobile Apps

Around October 26, 2012, the California AG sent letters to approximately 100 allegedly non-compliant companies, including Delta, notifying them of her view that CalOPPA applies not just to websites, but also to mobile apps.[11] The letter stated that

---

[1] *State of California v. Delta Air Lines, Inc.*, Case No. CGC-12-526741 (Cal. Sup. Ct., complaint filed Dec. 6, 2012), *available at* http://oag.ca.gov/system/files/attachments/press_releases/Delta%20Complaint_0.pdf?
[2] Wilson Sonsini Goodrich & Rosati, "Eye on Privacy," (Jan. 2013), *available at* http://www.wsgr.com/publications/pdfsearch/eye-on-privacy/mar2013/eye-on-privacy_03-13.pdf.
[3] California Online Privacy Protection Act (CalOPPA), Cal. Bus. & Prof. Code §§ 22575-22579, *available at* http://oag.ca.gov/privacy/COPPA.
[4] California Unfair Competition Law (California UCL), Cal. Bus. & Prof. Code §§ 17200 *et seq.*, *available at* http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=17001-18000&file=17200-17210. The California UCL prohibits individuals and entities from committing unlawful, unfair, or fraudulent business acts and practices, and government officials bringing suit for violations of CalOPPA may seek civil penalties and equitable relief under the UCL. Cal. Bus. & Prof. Code §§ 17203, 17206-07. Private plaintiffs may also assert claims for violations of CalOPPA under the UCL. *Id.* § 17204.
[5] *See* complaint, *supra* note 1 at ¶30.
[6] Airline Deregulation Act (ADA), Pub. L. 95-504, 49 U.S.C. § 1371, *et seq.*
[7] *See supra* note 3.
[8] Cal. Bus. & Prof. Code § 22577(a).
[9] *Id.* § 22575(b).
[10] *Id.* § 22577(b).
[11] A sample of the letter is available here.

Continued on page 14...

companies with apps used by California residents would have 30 days to respond with their specific plans and timelines to comply with CalOPPA, or an explanation of why the mobile app in question was not covered by CalOPPA, or else they would face an enforcement action. Non-compliance could result in fines amounting to $2,500 per individual download.[12] Delta acknowledged receipt of the letter on October 30, 2012, and stated that it would "provide the requested information," but for whatever reason, did not do so within the 30-day window.[13]

Attorney General Harris made good on her promise by suing Delta over its Fly Delta app on December 6, 2012. The complaint alleged that Delta did not make a privacy policy available to consumers within the Fly Delta app.[14] The complaint also asserted that Delta's website privacy policy neither mentioned the Fly Delta app nor disclosed the types of PII collected, which included the user's geolocation, photographs, full name, telephone number, and email address.[15]

Dismissal of the Delta Litigation

In a motion filed on February 11, 2013, Delta asked the court to dismiss the California AG's lawsuit at the pleading stage. Delta primarily argued that the preemption provision of the ADA precluded enforcement of CalOPPA against Delta. Alternatively, the company asserted that CalOPPA did not apply to the Fly Delta app because a mobile app is not an "online service" as defined by the statute. Delta explained that "online service" is a technical term that is not satisfied by the fact that an app sends or receives information over the Internet. Delta also claimed that the Delta privacy policy was already reasonably accessible to consumers through its homepage, which satisfied the statutory requirements.[16]

Adopting Delta's primary argument, Judge Marla J. Miller agreed that the AG's claim was preempted because the ADA evinces Congress' intent that any regulatory burdens on air carriers would be imposed only through the Department of Transportation. In an oral ruling,[17] the judge focused on the ADA's provision stating "that a state court may not enact or enforce a law, regulation or other provision having the force and effect of law related to a price, route, or service of an air carrier."[18] She noted that although the Fly Delta app could be used by non-Delta customers, and collect information irrelevant to airline services, it also could be used by airline customers in connection with such services. Thus, in offering the Fly Delta app, Delta acts as a "provider" of airline-related "services" under the ADA,[19] and the AG's claim "deriv[ed] from the enactment or enforcement of state law" and "relate[d]" specifically to airline "services."[20]

Implications for Mobile App Operators

Unfortunately, because the court based its dismissal of the Delta action on federal preemption and did not address the substantive requirements or scope of CalOPPA, the decision provides no guidance or solace to companies in the mobile app space that do not have any possibility of making similar federal preemption arguments. Nonetheless, the fact that the California AG proceeded with a lawsuit against a well-funded defendant based on her position that CalOPPA extends to mobile apps demonstrates that her office will vigorously enforce CalOPPA against companies with mobile apps that collect PII from California residents.

Until a court thoroughly evaluates CalOPPA's scope, operators of mobile apps that collect PII from California consumers can reduce their risk by complying with the law's requirements. This means, among other things, ensuring that the company's privacy policy is accessible from within its mobile application and ensuring that the policy accurately describes any PII collection, use, sharing, and disposal practices.

---

[12] The press release announcing the letters explained that the action followed Attorney General Harris's agreement with seven leading mobile and social app platforms—Amazon, Apple, Facebook, Google, Hewlett-Packard, Microsoft, and Research in Motion—to "improve privacy protections for millions of users around the globe who use apps on their smartphones, tablets, and other electronic devices." *See* "Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law" (Oct. 30, 2012), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance. These seven platforms "agreed to privacy principles designed to bring the industry in line with" CalOPPA under the AG's interpretation that it applies to mobile apps. *Id.* According to Harris, the parties' agreement also allowed consumers the opportunity to review an app's privacy policy before downloading the app rather than after, and "offer[ed] consumers a consistent location for an app's privacy policy on the application-download screen in the platform store." *Id.*

[13] The letter to Delta was attached to the complaint. *See* complaint, *supra* note 1.

[14] *See id.*

[15] *Id.*

[16] A copy of Delta's opening brief is available here. Delta's reply brief is available here.

[17] A transcript of the ruling is available here ("*Delta* Transcript").

[18] *Delta* Transcript at 21.

[19] *See* Karen Gullo, "Delta Wins Dismissal of California Mobile" (May 9, 2013), *available at* http://www.businessweek.com/news/2013-05-09/delta-wins-dismissal-of-california-mobile-app-privacy-suit-1.

[20] *Id.* at 22.

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