Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

EYE ON PRIVACY

JANUARY 2013

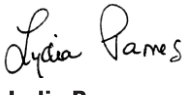
Welcome

In this month's issue of *Eye on Privacy,* we examine the Federal Trade Commission's final amendments to the Children's Online Privacy Protection Rule, review the increased privacy scrutiny facing mobile app developers, preview some of the key European and global privacy and data protection developments to expect this year, analyze the Federal Communications Commission's recent ruling regarding text message opt-out confirmations, and summarize the Department of Health and Human Services' recent guidance regarding the de-identification of protected health information.

Also, we have launched a webinar series to complement *Eye on Privacy* and provide you with another venue for in-depth discussions of privacy issues. Our next webinar will take place on January 18 and will cover the FTC's final COPPA Rule amendments and the significant implications for our clients and other interested parties.

In addition, please mark your calendar for February 5 at 11:00 a.m. Pacific/2:00 p.m. Eastern, when we will host a follow-up Q&A webinar featuring senior FTC attorneys Mamie Kresses and Phyllis Marcus, who have key responsibility for COPPA.

We're always open to hearing your suggestions for topics you'd like to see us cover in the future—please just send us a note at PrivacyAlerts@wsgr.com.



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

FTC Releases Final Amendments to Children's Online Privacy Protection Rule

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

Matthew Staples
Associate, Seattle
mstaples@wsgr.com

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

On December 19, 2012, the Federal Trade Commission (FTC) issued final amendments to the Children's Online Privacy Protection Rule (COPPA Rule), which implements the Children's Online Privacy Protection Act (COPPA).[1]

The COPPA Rule applies to operators of websites and online services[2] that collect information from children under 13 years of age.[3] The rule is triggered where either the website/service is *directed* to children or the operator has *actual knowledge* that the website/service is collecting "personal information" from children. The rule requires covered operators to, among other things, provide detailed notice to parents about the information being collected and its uses, and to obtain parents' verifiable consent prior to collecting, using, or disclosing personal information from children.

Continued on page 2...

[1] Federal Trade Commission, 16 C.F.R. Part 312: Children's Online Privacy Protection Rule: Final Rule Amendments and Statement of Basis and Purpose (Dec. 19, 2012), *available at* http://ftc.gov/os/2012/12/121219copparulefrn.pdf (Final Rule and SBP).

[2] The FTC has taken the position that the COPPA Rule applies to mobile apps.

[3] References to "children" in this article are to children under 13 years of age.

In This Issue

FTC Releases Final Amendments . . . *(continued from page 1)*

The FTC's final amendments to the rule, effective July 1, 2013, represent the culmination of the FTC's review of the rule that it commenced in 2010.[4] They follow the FTC's issuance of proposed amendments in September 2011 (the NPR)[5] and certain clarifications and additional proposed amendments published in August 2012 (the Supplemental NPR),[6] as well as multiple rounds of stakeholder comments. In its final amendments, the FTC retained many of its proposed updates to the rule without change, but it clarified a number of others.[7] In some cases, the FTC responded to comments by abandoning its proposed modifications.

This article briefly summarizes the FTC's final amendments to the rule that we believe will be of the greatest significance to our clients. We will hold a webinar on January 18, 2013, in which our attorneys will provide additional insight on the amendments and their implications for our clients and other interested parties.

Final Amendments

I. Strict liability for operators of child-directed websites and online services for third-party collection of personal information

By modifying the definition of "operator," an operator of a website or online service directed to children, or that has actual knowledge that particular users are children,[8] will be strictly liable for the third-party collection of personal information from its website or online service (e.g., ad networks or providers of software "plug-ins").[9]

Under these revisions, the first-party operator will be responsible for providing parents with notice and obtaining verifiable parental consent for the third-party collection of personal information.

II. Ad networks, providers of software plug-ins, and other third parties deemed "operators" if they have actual knowledge that they directly collect personal information from users of a child-directed website or online service

Replacing an earlier, more aggressive proposal,[10] the FTC provided that third-party operators of websites or online services (including, for example, ad networks, operators of software plug-ins, and social media services) will be covered "co-operators" if they have actual knowledge of collecting personal information from users of a website or online service that is directed to children.[11] In that case, the third-party operator will be responsible for complying with COPPA, including by providing notice to parents and obtaining verifiable parental consent prior to collecting such information.[12]

The FTC stated that "actual knowledge" most likely would be obtained when (i) a child-directed first-party operator directly communicates the child-directed nature of its content to the third-party operator, or (ii) a representative of the third-party operator recognizes the child-directed nature of the content on the first-party operator's website or online service, but that other facts might also suffice to establish actual knowledge on a case-by-case basis.[13]

III. Persistent identifiers that can be used to recognize a user over time and across different websites or online services are newly covered as "personal information," with exceptions to the requirement to obtain verifiable parental consent where they are collected only for the purpose of providing support for internal operations

The amended rule amends the definition of "personal information" to include "a persistent identifier that can be used to recognize a user over time and across different websites or online services."[14] Such persistent identifiers could include, but are not necessarily limited to, customer numbers held in cookies, IP addresses, and unique device identifiers.

The amended rule also includes, however, an exception to the requirement to obtain

---

[4] The FTC was not scheduled to review the COPPA Rule again until 2017, but, citing the rapid pace of technological change, including an explosion in children's use of mobile devices and the proliferation of online social networking and interactive gaming, the FTC initiated its review of the rule on an accelerated schedule.

[5] Federal Trade Commission, 16 C.F.R. Part 312: Children's Online Privacy Protection Rule: Proposed Rule; Request for Comment (Sept. 14, 2011), *available at* http://www.ftc.gov/os/2011/09/110915coppa.pdf.

[6] Federal Trade Commission, 16 C.F.R. Part 312: Children's Online Privacy Protection Rule: Supplemental Notice of Proposed Rulemaking; Request for Comment (Aug. 6, 2012), *available at* http://www.ftc.gov/os/2012/08/120801copparule.pdf.

[7] We discussed the most significant amendments proposed in the NPR (at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/pdfsearch/wsgralert-childrens-online-privacy-protection.htm) and the Supplemental NPR (at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-COPPA-additional-revisions.htm) in WSGR Alerts.

[8] The FTC's discussion of this matter in the Final Rule and SBP is framed in terms of child-directed content providers integrating plug-ins or other online services into their sites. The FTC clarified, however, that the same strict liability standard would apply to a general audience content provider that allows a third-party service to collect personal information from a specific user when the provider has actual knowledge that the user is a child. *See* Final Rule and SBP at *20 n. 59.

[9] Final Rule and SBP at *15-24. The FTC clarified that personal information will be deemed to be collected on behalf of an operator where it benefits by allowing another person to collect personal information *directly from* users of such operator's website or online service. This limits the scope of the provision to operators that design or control the child-directed content, and would exclude platforms that merely provide access to a third party's child-directed websites or online services. Final Rule and SBP at *24.

[10] The FTC initially had proposed holding responsible as a co-operator any website or online service that "knows or has reason to know" that it is collecting personal information through a host website or online service that is directed to children. Supplemental NPR, 77 Fed. Reg. at 46,645.

[11] Final Rule and SBP at *24-27.

[12] The FTC included an exception to this requirement in the narrow circumstance in which an operator collects a persistent identifier, and no other personal information, from a user who affirmatively interacts with the operator and whose previous registration with that operator indicates that such user is not a child. Such exception applies only where the user affirmatively interacts with the operator's online service (e.g., by clicking on a plug-in), and does not apply if the online service otherwise passively collects personal information from the user while he or she is on another site or service. *See* Final Rule and SBP, at *92.

[13] Final Rule and SBP at *27.

[14] Final Rule and SBP at *31-39.

Continued on page 3...

verifiable parental consent in situations in which an operator collects a persistent identifier for the sole purpose of providing support for its internal operations.[15] The new definition of "support for internal operations of [a] website or online service" includes those activities necessary to (i) maintain or analyze the functioning of the website or online service; (ii) perform network communications; (iii) authenticate users of, or personalize the content on, the website or online service; (iv) serve contextual advertising on the website or online service or cap the frequency of advertising; (v) protect the security or integrity of the user, website, or online service; (vi) ensure legal or regulatory compliance; or (vii) fulfill a request of a child as permitted by two exceptions to COPPA's verifiable parental consent requirements.[16]

The FTC clarified specifically that "support for internal operations" does not include the collection of persistent identifiers used to track children over time and across sites or services, or to amass a profile on an individual child user based on the collection of identifiers over time and across different websites in order to make decisions or draw insights about the child.[17]

The rule also provides for a new method for industry members to request that the FTC formally approve new activities to be added to the "support for internal operations of the website or online service" definition.[18]

IV. Additional types of personal information

In addition, the amended rule includes other new types of data as "personal information" that cannot be collected from a child without parental notice and consent. These include (i) photographs, videos, and audio files that contain a child's image or voice;[19] (ii) screen or user names that function as "online contact information" (i.e., where they are substantially similar to an email address and permit direct contact with a person online);[20] and (iii) geolocation information sufficient to identify street name and name of a city or town.[21]

V. Revisions to definition of "website or online service directed to children"

Under the COPPA Rule, whether a website or online service, or a portion thereof, is directed to children is a totality of the circumstances test in which the FTC considers various factors such as the website's or online service's subject matter, visual or audio content, age of models, language or other characteristics, advertising, evidence regarding audience composition and intended audience, and whether a site uses animated characters and/or child-oriented activities and incentives.[22]

The amendments to the rule add musical content, the presence of child celebrities, and celebrities who appeal to children to the factors that it will consider.[23]

The final amendments also permit a website or service that is directed to children, but that does not target children as its primary audience, to use an age screen to identify users under 13, and obtain verifiable parental consent only for data collection from those users.[24]

VI. Streamlined notices to parents

The final amendments simplify the notices that must be provided on the operator's website and online service, as well as the direct notice to the parent.

For online notices, the final amendments eliminate the COPPA Rule's current lengthy recitation of an operator's information collection, use, and disclosure practices in favor of a simple statement of (i) what information the operator collects from children, including whether the website or online service enables a child to make personal information publicly available; (ii) how the operator uses such information; and (iii) the operator's disclosure practices for such information.[25]

As for direct notices, the final amendments provide for "just in time" notices that are intended to be more useful to parents. The final amendments specify, in each instance in which direct notice is required, the precise information that operators must convey to parents regarding the items of personal information the operator already has obtained from the child; the purpose of the notification; any action that the parent must or may take; and what use, if any, the operator will make of the personal information collected. They also specify that each direct notice must contain a link to the operator's online notice of information practices.[26]

VII. Additional methods for obtaining verifiable parental consent

The COPPA Rule specifies that to obtain verifiable parental consent, operators must do so by "mak[ing] reasonable efforts to obtain verifiable parental consent, taking into consideration available technology," and that "[a]ny method to obtain verifiable parental consent must be reasonably calculated in light of available technology to

[15] Final Rule and SBP at *37.

[16] Final Rule and SBP at *37-38.

[17] Final Rule and SBP at *39.

[18] Final Rule and SBP at *38.

[19] Final Rule and SBP at *40-43.

[20] Final Rule and SBP at *28-30. The FTC clarified that this definition does not reach, among other things, single log-in identifiers that permit children to transition between devices or access related properties across multiple platforms.

[21] Final Rule and SBP at *43-46.

[22] *See* NPR, 76 Fed. Reg. at 59,814; 16 CFR § 312.2.

[23] Final Rule and SBP at *52.

[24] Final Rule and SBP at *56-60.

[25] Final Rule and SBP at *52-53.

[26] Final Rule and SBP at *54-56.

Continued on page 4...

ensure that the person providing consent is the child's parent."[27]

The rule sets forth a non-exclusive list of methods that meet this standard, such as requiring a parent to use a credit card in connection with a transaction, or providing consent forms to be signed by the parent and returned by postal mail or facsimile. In its final amendments, the FTC added several new methods to this non-exhaustive list, including electronic scans of signed parental consent forms; videoconferencing; use of electronic or online payment systems (with appropriate direct notice to the parent), including notification of each discrete monetary transaction to the primary account holder; and use of government-issued identification (such as a driver's license or a segment of the parent's Social Security number), checked against a database, provided that the parent's ID is deleted promptly after verification is complete.[28]

Additionally, while the FTC declined to add digital or electronic signatures to its non-exhaustive list of parental consent mechanisms, it noted that its amended COPPA Rule would not prohibit an operator's acceptance of a digitally signed consent form where the signature provides other indicia of reliability that the signor is an adult, such as an icon, certificate, or seal of authenticity that accompanies the certificate.[29]

The FTC's amendments also add two new means of obtaining FTC approval for other proposed methods of obtaining verifiable parental consent. First, applicants will be able to present the FTC with a detailed description of the proposed consent mechanism, along with an analysis of how the mechanism meets applicable requirements. The FTC would publish the application for public comment and rule on the request within 120 days.[30] Second, the amendments provide that operators participating in an FTC-approved COPPA safe harbor program may use any parental consent mechanism that the safe harbor program deems to meet the rule's parental consent standards.[31]

Further, despite having proposed in the NPR to eliminate the "email-plus" consent mechanism, the FTC retained it in its final amendments.[32] The email-plus consent method permits operators collecting personal information only for their internal use to obtain verifiable parental consent via email, provided that the email is coupled with an additional step (such as a follow-up telephone call or letter, or a delayed follow-up email message).[33]

VIII. Strengthening of confidentiality and security requirements

The COPPA Rule presently obligates operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.[34] The amended COPPA Rule requires operators to take reasonable measures to release children's personal information only to service providers and third parties that are capable of maintaining the confidentiality, security, and integrity of such information, and that provide assurances that they will maintain the information in such a manner.[35]

The amended COPPA Rule also adds new data-retention and deletion provisions under which operators must (i) retain children's personal information for only as long as is reasonably necessary to fulfill the purpose for which the information was collected; and (ii) take reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.[36]

IX. Increased oversight of safe harbor programs

COPPA contains a "safe harbor" for participants in FTC-approved COPPA self-regulatory programs.[37] The COPPA Rule provides that operators complying fully with an approved safe harbor program will be deemed to be in compliance with COPPA for purposes of enforcement, and participation in an approved program may afford companies some protection against FTC enforcement.[38]

The amendments to the rule strengthen its safe harbor provisions by: (i) requiring safe harbor program applicants to submit comprehensive information about their capability to run an effective safe harbor program; (ii) establishing more rigorous baseline oversight by FTC-approved safe harbor programs of their members (including annual comprehensive reviews of members' information practices); and (iii) requiring FTC-approved safe harbor programs to submit periodic reports to the FTC.[39]

---

[27] 16 CFR § 312.5(b)(1).

[28] The FTC also eliminated the use of a digital certificate using public key technology, and email accompanied by a PIN or password obtained through another FTC-approved verification method, from the COPPA Rule's non-exhaustive list of methods by which verifiable parental consent may be obtained. *See* 16 CFR § 312.5(b)(1); Final Rule and SBP at *160-61.

[29] Final Rule and SBP at *70-71.

[30] Final Rule and SBP at *81-85.

[31] Final Rule and SBP at *85-86.

[32] Final Rule and SBP at *76-81.

[33] 16 CFR § 312.5(b)(2).

[34] 16 CFR § 312.8.

[35] Final Rule and SBP at *95-96.

[36] Final Rule and SBP at *96-99.

[37] 15 U.S.C. § 6503.

[38] The COPPA Rule provides that when considering whether to initiate an investigation or to bring an enforcement action for violations of the COPPA, and in considering appropriate remedies, the FTC will take into account whether an operator has been subject to an approved safe harbor program and has taken remedial action pursuant to such program's guidelines. *See* 16 CFR § 312.10(b)(4).

[39] Final Rule and SBP at *99-103.

Continued on page 5...

FTC Releases Final Amendments . . . *(continued from page 4)*

Implications of the Final Amendments

The FTC has enforced the COPPA Rule aggressively since its enactment in 2000. Numerous companies have paid multimillion-dollar penalties as a result of non-compliance. The FTC's changes to the COPPA Rule are significant and reflect the FTC's continued focus on consumer privacy, particularly with regard to children. Companies that collect personal information from children will need to evaluate and, where appropriate, revise their practices to conform to the modifications to the COPPA Rule. Further, the revised rule will now impose compliance obligations on many operators of websites and online services that were previously unaffected by the rule.

As mentioned in the introduction to this article, we will be offering a webinar on January 18, 2013, in which we will provide additional information on the FTC's updates to the COPPA Rule. If you would like to receive an invitation to this webinar, please contact us at PrivacyAlerts@wsgr.com.

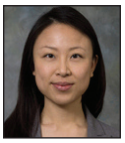
Mobile Apps Face Heightened Privacy Enforcement - Policies and Practices Scrutinized

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

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

Matthew Staples
Associate, Seattle
mstaples@wsgr.com

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



Sharon Lee
Associate, Palo Alto
shlee@wsgr.com

Mobile app developers faced new scrutiny at state and federal levels this past December, with app makers removing apps and taking action to respond. On December 6, 2012, California Attorney General Kamala Harris filed suit against Delta Air Lines after its failure to include a privacy policy within its mobile app.[1] A few days later, the Federal Trade Commission (FTC) issued a report titled "Mobile Apps for Kids: Disclosures Still Not Making the Grade," which concluded that industry has made little or no progress in improving privacy disclosures in children's mobile apps since the FTC issued its last report on this topic in February 2012.[2] The report also signaled that the FTC has launched multiple non-public investigations of children's app developers regarding their privacy disclosures and practices. These developments parallel the growth of mobile devices generally and make clear the importance of addressing privacy considerations in the mobile space.

State Privacy Enforcement Action Against Delta Air Lines

In the Delta complaint, Attorney General Harris alleged that Delta's "Fly Delta" app violated the California Online Privacy Protection Act (CalOPPA)[3] and California's Unfair Competition Law.[4] The complaint alleged that Delta did not make a privacy policy available to consumers within the "Fly Delta" app and, furthermore, that Delta's website privacy policy neither mentioned the "Fly Delta" app nor disclosed several types of personally identifiable information that it collected, including the user's geolocation, photographs, full name, telephone number, and email address.

CalOPPA requires operators of commercial websites to "conspicuously" post on their websites, and operators of online services to make reasonably accessible, a privacy policy that informs consumers residing in California about the categories of personal information collected by the operators and the categories of third parties with which the data is shared. California's Unfair Competition Law prohibits individuals and entities from committing unlawful, unfair, or fraudulent business acts and practices.

Attorney General Harris has taken the position that CalOPPA applies to mobile apps, and that a privacy policy for a mobile app is not

[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] The December 2012 FTC report is titled "Mobile Apps for Kids: Disclosures Still Not Making the Grade" and is available at http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf. The February 2012 FTC report is titled "Mobile Apps for Kids: Current Privacy Disclosures are Disappointing" and is available at http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

[3] California Online Privacy Protection Act (CalOPPA), Cal. Bus. & Prof. Code §§ 22575-22579.

[4] Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et seq.*

Continued on page 6...

Mobile Apps Face Heightened . . . *(continued from page 5)*

reasonably accessible to consumers under that statute if it is not available to consumers within the app itself.[5] Attorney General Harris has asserted that violations of CalOPPA may result in penalties of up to $2,500 per app download.[6]

Federal Privacy Investigations of Children's Apps

The FTC's survey of children's apps for its December 2012 FTC staff report examined the substance of privacy disclosures, moving beyond its prior report, which focused more on the presence of disclosures. This new qualitative emphasis likely brings greater challenges for early-stage companies with limited resources.

The FTC expressed concern that a majority of surveyed apps shared children's information (including device IDs) with third parties, or included interactive features such as advertising, the ability to make in-app purchases, or links to social media services, without disclosing these practices to parents. With respect to information sharing, FTC staff found that 59 percent of surveyed apps transmitted some information from a user's mobile device back to the developer or to a third party. Of those apps, all transmitted a device ID to the app developer or, more typically, to a third party.

Both 2012 FTC staff reports examined the number of children's apps with privacy disclosures and found that most surveyed apps failed to provide *any* information about the data collected through the app. The February 2012 report stated that only 16 percent of surveyed apps provided parents with a link to a privacy disclosure before app download. The December 2012 report stated that this percentage had increased only slightly, from 16 percent to 20 percent.

The most recent report urged players in the app ecosystem (i.e., app stores, app developers, and third parties that interact with apps) to develop accurate privacy disclosures for children's apps, including disclosing the presence of interactive features. The report also expressed the view that companies should make privacy disclosures available prior to the download of an app. The technical feasibility of this practice was advanced in 2012 when Attorney General Harris and the operators of leading mobile app platforms—Amazon, Apple, Google, The Hewlett-Packard Company, Microsoft, Research in Motion, and Facebook—entered into an agreement pursuant to which these operators agreed to provide means in their app marketplaces for developers to make available privacy policies for all apps prior to download.[7]

In addition, the FTC urged the mobile app industry to develop "best practices" to protect privacy, including the three key principles from the FTC's March 2012 final consumer privacy report:[8] (1) adopting a "privacy-by-design" approach to minimize risks to personal information, (2) providing consumers with simpler and more streamlined choices about relevant data practices, and (3) providing consumers with greater transparency about how data is collected, used, and shared.

Significantly, the report stated that enforcement actions will be "vitally important" to ensuring that the privacy of consumers and their children is protected. To that end, the FTC initiated a number of investigations of children's app developers to "address the gaps between company practices and disclosures" and determine whether these entities in the mobile app marketplace have violated the Children's Online Privacy Protection Act (COPPA)[9] or engaged in unfair or deceptive trade practices in violation of the FTC Act.[10] COPPA applies to operators of websites and online services that are directed to children or from which the operator collects or maintains personal information from users that it has actual knowledge are under 13 years of age. COPPA requires such operators to, among other things, provide detailed notice to parents and obtain verifiable consent prior to collecting, using, or disclosing personal information from children under the age of 13. The FTC has taken the position that COPPA applies to mobile apps.

In light of regulators' increased privacy enforcement against players in the mobile app marketplace, mobile app developers can expect to face continued close scrutiny of their practices. Given this enforcement focus, understanding how an app collects, uses, and discloses information is increasingly important. Formulating disclosures that accurately reflect data practices in a manner that is simple, easy to understand, and accurate poses significant challenges generally, but especially in mobile.

---

[5] An open question is whether CalOPPA is preempted by the Airline Deregulation Act. 49 U.S.C. §§ 40101 *et seq.*

[6] CalOPPA provides that a commercial website or online service operator is in violation of CalOPPA if the operator fails to post its privacy policy within 30 days after being notified of noncompliance. When Attorney General Harris filed suit against Delta, more than 30 days had passed since she had served a warning letter to Delta.

[7] *See* https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy and https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-expansion-california%E2%80%99s-consumer.

[8] The FTC's March 2012 final privacy report is titled "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers" and is available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[9] Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-6506.

[10] FTC Act, 15 U.S.C. §§ 41-58.

Tip

Preparing template privacy and data security provisions can help speed negotiations and close transactions faster and more easily.

Global and European Data Protection Law: What Will the Hot Issues Be in 2013?

Christopher Kuner
Senior Of Counsel, Brussels
ckuner@wsgr.com

Cédric Burton
Associate, Brussels
cburton@wsgr.com

Anna Pateraki
Associate, Brussels
apateraki@wsgr.com

This past year was one of the busiest ever for data protection globally, and 2013 is promising to be even busier. In Europe, a number of milestone events occurred last year, including the introduction of a proposal for a new data protection regulation (the Draft Regulation) and key discussions around online data collection and emerging technologies such as cloud computing and mobile devices.

We have launched the WSGR EU Data Protection Regulation Observatory site (available at www.wsgr.com/eudataregulation/) to follow developments around the EU data protection reform and help companies better understand EU data protection and privacy issues that may have a significant impact on their business. The reform will likely go on for several years and we will continue tracking the developments; please visit our site regularly for timely updates and materials.

We begin this exciting new year for privacy and data protection with an outline of some of the key European and global developments to expect in 2013.

1. Review of the EU Data Protection Legal Framework

In 2013, the EU data protection reform will continue and accelerate. The debates will intensify as the draft goes through the legislative process. First, the EU Parliament LIBE committee will issue its report on the draft regulation to the Parliament together with a proposal for amendments. Debates in the Parliament are expected to begin in January 2013. In parallel, the Council of the European Union will continue its work via the DAPIX working group, among others. Discussions are expected to be vigorous; however, their outcome is unclear.

Following these discussions, the EU Commission will most likely adapt its proposal to take into account the various amendments and to try to reach a political agreement between the three institutions. The EU Commission is pushing hard on the draft regulation and is eager to have it adopted as soon as possible. The objective of the EU Commission is to reach a political agreement on the review of the data protection reform during the Irish presidency or in the second half of 2013 at the latest, which means that this year will be full of activity in Brussels.

2. Busy Year for European Regulators

The coming year also will be very busy for the data protection regulators both at a national and at a European level. The EU regulators, via the Article 29 Working Party, are expected to issue opinions on a number of key topics such as mobile applications, the EU purpose limitation principle (how data can be used in a way that is compatible with the purpose of its collection), and new developments regarding Binding Corporate Rules (BCRs) for data processors. It is also expected that national regulators will issue new or update existing guidance on the EU cookie rules. Further, there is a trend of better coordination among regulators, which is likely to lead to increased enforcement action at a local and European level.

3. Adoption of New Privacy Legislation Globally

It is anticipated that more and more non-EU countries will adopt data protection legislation in 2013. This will confirm the trends seen in 2012, when data protection legislation was enacted in a significant number of countries such as Angola, Colombia, Costa Rica, Gabon, Peru, Philippines, South Korea, St. Lucia, and Trinidad and Tobago. In addition, the existing legal framework was revised in Australia, Hong Kong, New Zealand, Russia, Taiwan, and Ukraine in 2012.

We may see a number of additional countries enacting new legislation or modifying their existing legal framework in 2013. Next on the list are Barbados, Malaysia, Singapore, and South Africa, where privacy legislation has been adopted but is not yet fully in force, and countries where data privacy bills are currently in consultations such as Brazil, Georgia, and Kenya. Further, other countries, such as El Salvador, have announced that discussions to pass comprehensive data protection legislation will be initiated in 2013.

4. Adequacy Trends and Global Interoperability

The European Commission held in 2012 that Uruguay and New Zealand provide an "adequate level of data protection," allowing the free transfer of European data to those countries. Next on the list is Monaco, which has already received a positive opinion from the Article 29 Working Party but still awaits the European Commission's official adequacy recognition. Further, other countries seem to be exploring the possibility of filing adequacy requests this year. In addition, substantive developments are expected in 2013 in the work of the Asia-Pacific Economic Cooperation (APEC) in Asia, especially with respect to potential interoperability between the EU's BCR scheme and APEC's Cross Border Privacy Rules (CBPR) system.

5. Council of Europe – Modernization of Convention 108

Political discussions will occur at the Council of Europe (not to be confused with the Council of the European Union) regarding the modernization of Convention 108. As previously reported on the WSGR EU Data Protection Regulation Observatory, the data

Continued on page 8...

Global and European Data Protection Law . . . *(continued from page 7)*

protection working group of the Council of Europe finalized its proposed changes to Convention 108 on November 30, 2012. Although the Council of Europe is not an EU institution, Convention 108 underlies the EU framework for data protection, and its amendment can provide insight into the ongoing EU reform, particularly since the working group largely consists of national governments and data protection authorities from the EU and other countries. The text will now be taken up at a political level and discussions will occur in 2013.

Overall Prediction

The coming year likely will bring a large number of new developments on the privacy and data protection scene. The legal framework is changing in Europe and globally: regulators are becoming more active in enforcing privacy, and developments are expected in relation to innovative technologies such as cloud computing, big data, and the "Internet of Things." With all this in mind, 2013 looks to be very promising and exciting. Happy New Year!

FCC Declares Opt-Out Confirmation Text Messages Allowable under the TCPA, Makes No Sweeping Changes to Its Interpretation of the Statute

Tonia Klausner
Partner, New York
tklausner@wsgr.com

Jason Mollick
Associate, New York
jmollick@wsgr.com

In a decision[1] welcomed by consumer protection and marketing organizations alike, the Federal Communications Commission (FCC) recently ruled that final, one-time text messages confirming opt-out requests do not violate the Telephone Consumer Protection Act (TCPA).[2] Such messages may even include information on how a recipient may opt back in, so long as no effort is made to encourage the recipient to do so. The FCC made clear that opt-out confirmation texts amount to good consumer policy and are widely used and expected by both businesses and consumers. Although the ruling's impact is confined to its specific context, the FCC did show a willingness to accept new technologies and industry standards that serve the public interest and the overall purposes of the TCPA, even if such practices do not fall squarely within the statute's text.

The TCPA and Text Messages

In 1991, long before text messaging became a widespread method of communication, Congress passed the TCPA to address the increasing number of telemarketing calls and faxed advertisements considered to be an invasion of consumer privacy and risk to public safety. The TCPA prohibits, among other things, the use of "automated telephone equipment . . . to make any call (other than a call made for emergency purposes or made with the prior express consent of the called party) . . .to any telephone number assigned to a . . . cellular telephone service . . . or any service for which the called party is charged for the call."[3] Any person or entity receiving such non-emergency automated calls without prior express consent may bring a private right of action to recover statutory damages of $500 per violation, or up to $1,500 per call for a willful or knowing violation.[4]

The availability of significant statutory damages has led plaintiffs' class action lawyers to regularly file putative class actions on behalf of all persons who allegedly received a "call" governed by the TCPA without the requisite express consent. The statute applies only to calls and therefore it does not clearly cover text messaging services such as short message service (SMS) messages. However, both the Ninth Circuit and the FCC have concluded that a text message is a "call" within the meaning of the statute.[5] Recent years therefore have seen a large number of putative TCPA class actions filed against companies engaged in text messaging services and marketing campaigns, and/or the providers that manage those services and campaigns. Many of these suits have addressed the common practice of sending a text confirming receipt of an opt-out request—a practice required by the Mobile Marketing Association's (MMA's) U.S. Consumer Best Practices.[6] According to

---

[1] *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, SoundBite Communications, Inc. Petition for Expedited Declaratory Ruling*, Declaratory Ruling, CG Docket No. 02-278, FCC File No. 12-143, ¶ 2 (Nov. 29, 2012) ("SoundBite Declaratory Ruling"), *available at* http://www.fcc.gov/document/declaratory-ruling-re-soundbite-tcpa-petition.

[2] Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227.

[3] *Id.* § 227(b)(1)(A)(iii).

[4] *Id.* § 227(b)(3).

[5] *Satterfield v. Simon & Shuster*, 569 F.3d 946, 951-52 (9th Cir. 2009); *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 18 FCC Rcd. 14014, 14115, ¶ 165 (2003).

[6] Mobile Marketing Association, U.S. Consumer Best Practices (Version 6) § 1.6-4 (Apr. 1, 2011), *available at* http://www.mmaglobal.com/bestpractices.pdf ("When STOP, or any of the opt-out keywords above, is sent to a program, the program must respond with an MT message, whether or not the subscriber is subscribed to the program.").

Continued on page 9...

plaintiffs' class action lawyers, this practice, although required by the MMA and often contractually required of service providers managing texting services and marketing campaigns, violates the TCPA because the sender no longer has express consent to send texts to that number. Given the lack of guidance in either the statute or its regulations regarding when opt-out requests become effective, many defendants have chosen to settle these actions rather than risk possible eight-figure or greater liability. In one such case arising out of opt-out confirmations sent to an estimated 67,500 persons, Barclays Group agreed to settle the matter for a payment of up to $8,262,500, including up to $1,580,000 in attorneys' fees.[7]

SoundBite's Petition

On February 16, 2012, SoundBite, a communications platform that sends text messages to wireless subscribers on behalf of a number of companies, filed a petition with the FCC seeking a declaratory ruling that sending a final, one-time text message confirming a consumer's opt-out request is not a violation of the TCPA.[8] SoundBite put forth three arguments in support of its petition: (1) it does not use an "automatic telephone dialing system" as that term is defined in the TCPA;[9] (2) even if the confirmation texts are sent by such a system, the FCC nonetheless should recognize a "grace period" to effectuate opt-out requests similar to those in the case of telemarketing voice calls;[10] and (3) opt-out confirmations are consistent with good consumer policy, are widely used in the industry (and often contractually required), and promote the public interests implicated by the TCPA.[11]

The FCC's Declaratory Ruling

The FCC granted SoundBite's request and held that "one-time texts confirming a request that no further text messages be sent does not violate the TCPA or the Commission's rules" so long as the confirmation texts (1) "merely confirm the consumer's opt-out request," (2) "do not include any marketing or promotional information," and (3) "are the only additional message sent to the consumer after receipt of the opt-out request."[12]

The FCC reached this conclusion based not on any of the arguments made by SoundBite, but rather on its own determination that "a consumer's prior express consent to receive text messages from an entity can be reasonably construed to include consent to receive a final, one-time text message confirming that such consent is being revoked at the request of that consumer." Opt-out confirmations of the type used by SoundBite are widespread practices in the texting industry that are "considered part of the opt-out process" and are "expected or desired" by consumers at the time they provide consent to receive messages in the first place.[13] According to the FCC, no consumer has ever complained about receiving confirmation texts, although some consumers have in fact complained about *not* receiving such confirmations.[14] Moreover, confirmation texts are good consumer policy and further the TCPA's goal of promoting public safety by ensuring that the consumer is aware of the opt-out request, in case such request was made by a third party without authorization (e.g., to prevent the consumer from receiving bank fraud alerts). Thus, the receipt of a final, one-time confirmatory text is deemed inherent in the "prior express consent" given to the sender by the recipient.[15]

In order to qualify under the FCC's ruling, the confirmation text should be sent within five minutes of receiving the opt-out request. "If it takes longer, however, the sender will have to make a showing that such delay was reasonable, and the longer this delay, the more difficult it will be to demonstrate that such messages fall within the original prior consent."[16] Moreover, the inclusion of "contact information or instructions as to how a consumer can opt back in fall reasonably within consumer consent," whereas texts that encourage consumers to opt back in do not.[17] The FCC's ruling is limited to the specific type of communications at issue in the matter, and no sweeping change was made to its interpretation of key terms in the TCPA.

Implications

The FCC's declaratory ruling comes as immediate relief to companies that previously were forced to choose between violating the MMA Consumer Best Practices and facing class action lawsuits seeking millions in statutory damages under the TCPA. Companies should feel confident in their ability to send confirmation text messages so long as they (1) merely confirm the opt-out request, (2) do not include any marketing or promotional information to encourage opt in

---

[7] *See Gutierrez v. Barclays Group*, No. 10-cv-1012-DMS-BGS (S.D. Cal. Oct. 11, 2011), Settlement Agreement and Release, *available at* www.cptgroup.com/gutierrezclasssettlement/SettlementAgreementandRelease.pdf.

[8] SoundBite Declaratory Ruling, ¶ 3.

[9] 47 U.S.C. § 227(a)(1) ("The term 'automatic telephone dialing system' means equipment which has the capacity—(A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers.").

[10] The FCC allows telemarketers up to 30 days after an opt-out request to remove the subscriber's phone number from their systems. SoundBite Declaratory Ruling, ¶ 4 n.16.

[11] *Id.* ¶¶ 4-5.

[12] *Id.* ¶ 7 and n.31.

[13] *Id.* ¶ 8.

[14] *Id.* ¶¶ 9-10.

[15] 47 U.S.C. § 227(b)(1)(A).

[16] SoundBite Declaratory Ruling, ¶ 11.

[17] *Id.* ¶ 12.

Continued on page 10...

FCC Declares Opt-Out Confirmation Text Messages . . . *(continued from page 9)*

(but may include information or instructions on how a consumer can opt back in), (3) are the only additional message sent to the consumer after receipt of the opt-out request, and (4) are sent within five minutes of receiving the request. Of course, companies must remain cognizant of the "prior express consent" requirement of the TCPA and should consider whether the technology they utilize to send text messages to consumers constitutes an "automatic telephone dialing system" as that term has been broadly interpreted by the courts and the FCC. The FCC's SoundBite ruling suggests that while the FCC is unlikely to make any changes to its prior expansive interpretations of the TCPA's provisions, it is willing to take a flexible approach when interpreting the express consent requirement when faced with new technologies and industry practices that are good consumer policy.

Agency Issues Guidance on De-Identification of Health Information: Process Guidance May Have Far-Reaching Influence

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

Wendy Devine
Associate, San Diego
wdevine@wsgr.com

Federal regulators from the United States Department of Health and Human Services (HHS) recently issued guidance relating to standards for de-identification of protected health information (PHI). The 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act required that the agency provide guidance identifying acceptable methods for de-identifying protected health information to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Many organizations that encounter health information in their businesses increasingly look to HIPAA's rules and regulations as a source for information on emerging and better practices, regardless of whether those businesses are required to follow the rules.

The anonymization and de-identification of data represents an emerging area of interest for businesses, consumers, and regulators as information management, especially for health data, continues to be an important risk area for enterprises. HIPAA regulations generally govern the use and disclosure of PHI. If PHI is de-identified, i.e., modified such that it does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual, many federal restrictions on use and disclosure do not apply; however, state law or other regulations still may apply to such use and disclosure.[1] Class action litigation growing out of allegedly "anonymous" data also has begun to emerge. The recent HHS guidance is intended to clarify and define exactly what de-identification methods meet the HIPAA de-identification standard. Because de-identification, and the suggestion that data is "anonymous," increasingly has been depended upon to help alleviate concerns about data usage, regulations and guidance relating to de-identification are of interest to many enterprises.

In March 2010, the HHS Office of Civil Rights (OCR) hosted a workshop focused on topics related to de-identification methods and policy. The agency reached out to the public, especially stakeholders with practical, technical, and policy experience in de-identification. De-identification and how to accomplish it are increasingly hot topics as technology is making analysis of aggregated data easier and more valuable and, simultaneously, as the penalties for the improper use and disclosure of PHI have grown to include severe civil penalties and the possibility of criminal sanctions.[2]

The resulting HHS guidance details two methods for accomplishing HIPAA-compliant de-identification of PHI: (1) the expert determination method and (2) the safe harbor method.[3]

Expert Determination De-Identification Method

The expert determination method requires that "[a] person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" apply those methods and determine that any risk that the information could be used (alone or with

---

[1] § 164.514 (a) ("Standard: de-identification of protected health information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.")

[2] For more information, please see our WSGR Alert titled "Health Privacy Changes Create Increased Risks and Obligations for Holders of Health Data," which is available at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert_HIPAA.htm.

[3] § 164.514(b)(1)-(2).

Continued on page 11...

other information) to identify the person to which the information relates is "very small." Further, that person must document the methods and results of his or her analysis.

The guidance also discusses whether expert determinations of risk expire, stating that while no specific requirement for an expiration date exists in the HIPAA regulations, some experts may choose to provide time-limited analyses. HHS notes that such an "expiration" does not indicate that de-identified information that already has been disclosed is at risk, but rather that any future disclosures may require a fresh expert determination of risk. Further, the guidance addresses the question of who qualifies as an "expert" such that they may perform the analysis. The agency concluded that no specific degree or certificate is required. Rather, expertise can be reflected in various educational backgrounds and related experience. HHS does note that, with respect to enforcement, a given expert would be evaluated based on his or her education and experience in PHI de-identification methods. As a practical matter, it seems likely that specialized consultants will emerge and that experts who have "done it before" could be perceived as more credible than others. Over time, at least for now, it seems likely that the process for selecting and retaining these experts might be similar to those used in hiring and retaining testifying experts in litigation settings. Ultimately, an organization whose de-identification processes are reviewed or challenged likely will seek to rely on the guidance and opinion of their retained experts.

Similarly, under the expert determination method, identification of what constitutes a "very small risk" and the methodology for assessing that risk acceptably is dependent on the particular circumstances and data set. Instead of requiring the use of a particular method and a particular risk cut-off, the expert is required to use reasonable methods and document how those methods and the results of the analysis justify the determination of a "very small" risk. Such methods may include an assessment of whether particular data is unique or linkable to a particular person in a particular population. Accordingly, the guidance for this method favors the creation of process-focused controls and accountability through experts in evaluating the suitability of any de-identification protocols.

Principles that may be used as a starting point for evaluating risk under the guidance include replicability, data-source availability, and distinguishability. To illustrate these concepts, the guidance provides a workflow that depicts a series of steps: (1) the expert evaluates whether the PHI can be linked to an individual by an intended recipient; (2) the expert provides guidance to the covered entity or business associate on what methods can be used to deal with any identified risk; (3) the expert applies those methods as authorized by the covered entity or business associate; and (4) the expert repeats step (1) with respect to the new data set, assessing whether any risk still remains, and if so, whether that risk is "very small."

Safe Harbor De-Identification Method

A second acceptable method for de-identification is the safe harbor method. This method provides a greater level of specificity and requires removal of 18 particular types of data from the PHI for acceptable de-identification, including among them names, contact details, Social Security numbers, and similar unique identifiers.[4] Notably, the list includes IP addresses. Once the required information is removed, if the covered entity or business associate does not have actual knowledge that the remaining information can be used (alone or with other information) to identify the subject of the PHI, it may be considered de-identified.

The guidance clarifies that ZIP codes may be included in a de-identified data set where, per Census data, combining all ZIP codes with the same first three digits results in a geographic unit that contains greater than 20,000 people. Alternatively, ZIP codes may be included in a de-identified data set where the initial three digits of the ZIP code are changed to 000.

Further, the guidance states that all of the identifiers listed in footnote No. 4 must be removed. For example, a data set that includes the last four digits of a Social Security number or a person's initials (in lieu

[4] § 164.514(b)(2)(i) ("A covered entity may determine that health information is not individually identifiable health information only if: . . . [t]he following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

1. Names;
2. All geographic subdivisions smaller than a state (e.g., street address, city, etc.);
3. All date information that relates to the individual (e.g., birth date, death date, etc.), however note that year does not need to be removed except with respect to data that indicates an age over 89 years. Such data elements may be aggregated into an age 90+ category;
4. Telephone numbers;
5. Fax numbers;
6. Email addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate and license numbers;
12. Vehicle identifiers;
13. Device identifiers;
14 URLs;
15. IP addresses;
16. Biometric identifiers (includes finger prints and voice prints);
17. Full-face photographs/images; and
18. Any other unique identifier including numbers, characteristics, and codes.")

Continued on page 12...

of the full name) is not de-identified. Similarly, removal of date information requires removal of all such information, including test and treatment dates.

The guidance also provides illustrative examples of what types of information fall within the 18th category catch-all "any other unique identifier." Specific examples include clinical trial numbers, a patient-unique bar code embedded into an electronic medical record, or the occupation of the patient if it distinguished and allowed for identification of the individual.

Finally, the guidance discusses what constitutes actual knowledge that a data set may be used to identify an individual, concluding that it requires the covered entity or business associate to be "aware that the information is not actually de-identified information." Examples of such circumstances include (1) a data set that includes a patient occupation that may be used in combination with other data (e.g., state of residence and age) to identify that individual; (2) disclosing the data set to a person who has a close relationship with the patient and thus would be reasonably expected to be able to identify the patient from the limited data set; and (3) disclosing information regarding rare clinical events that may have been widely reported and discussed (e.g., an unusually large multiple birth) such that the recipient would reasonably be expected to be able to identify the patient based on the clinical event. What constitutes "actual knowledge" regarding data matters is becoming increasingly important in multiple sectors as the collection, use, and disclosure of information expands dramatically. The ability of an organization to meaningfully understand its data practices continues to be increasingly complex, challenging, and, for many organizations, expensive. But the financial and legal consequences of failing to have such an understanding have seemed to continue to grow in parallel.

Implications

While the guidance on de-identification retains the subjective nature of the de-identification standard in that it does not provide hard rules for methods or evaluation of risk, it does address some common scenarios and provide useful illustrative examples. Furthermore, the lack of hard-line rules underscores the fact-specific nature of the de-identification process and the need to perform a full evaluation for each data set and disclosure.

Given the continued growth and development of privacy-related litigation, especially headline-grabbing cases relating to allegedly anonymous information, de-identification of data will continue to be an emerging and significant area of interest for enterprises. Because of HHS' efforts in this area, enterprises can expect that advisers and others' experience with de-identification of health information will spill over into de-identification of other areas of data. In particular, the de-identification standard in HIPAA focuses on whether or not the information is PHI. So, as long as the information is not PHI, the use of the information remains unrestricted by HIPAA regulations. Enterprises that are focused on the collection, use, and analysis of data in new and innovative ways may want to pay close attention to HIPAA developments. The past decade has shown that regulators (and plaintiffs' class action lawyers) have leveraged heavily their experience in particular industry sectors in connection with broader privacy regulation.

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 New York Palo Alto San Diego San Francisco Seattle Shanghai Washington, DC