Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

EYE ON PRIVACY

SEPTEMBER 2012

Welcome

In this latest edition of *Eye on Privacy*, we continue to highlight some of the major privacy developments of the past two months, including the latest from the EU on cloud computing, LinkedIn's success in a class action suit, a federal magistrate decision that appears to expand the breadth of the Video Privacy Protection Act, an overview of the Federal Trade Commission's settlement with Facebook, the commission's proposed amendments to a rule governing the online collection of information from children, and efforts to protect privacy in the Asia-Pacific region.

In addition to *Eye on Privacy*, which we publish every other month, we currently are planning to launch a webinar series that will give us the opportunity to provide you with live and in-depth discussions of privacy issues. Please let us know if there are any specific topics that you're interested in and would like us to address. We may be reached at PrivacyAlerts@wsgr.com.

Lydia Parnes

Lydia Parnes
Partner, Wilson Sonsini Goodrich & Rosati

European Data Protection Law: New European Cloud Computing Guidelines

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

Anna Pateraki
Associate, Brussels
apateraki@wsgr.com

On July 1, 2012, the European data protection regulators (referred to collectively as the Article 29 Working Party or the Working Party) adopted an opinion providing guidelines for preparing cloud services agreements.[1] Opinions of the Working Party are not legally binding *per se*, but they are highly influential and indicate the attitude of the regulators in Europe, who have the authority to intervene in situations where personal data is processed (each of the 27 EU Member States has at least one data protection authority (DPA)). The opinion demonstrates the data protection risks associated with the use of cloud computing services in Europe.

The opinion is based on the common scenario in which cloud providers process data on behalf of corporate customers; it does not analyze situations where a cloud provider re-processes the cloud data for its own business

Continued on page 2...

[1] The opinion is available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

In This Issue

purposes. Although the Working Party acknowledges the financial benefit of using cloud services, especially for small enterprises, it also sees significant privacy risks (e.g., where the outsourcing chain involves multiple cloud providers and subcontractors). The Working Party believes that these risks are higher where non-EU cloud providers are engaged, and that therefore additional guarantees should be provided to ensure compliance with applicable European data protection law.

In that context, the Working Party calls on the relevant parties to enhance control over data processing and transparency in the cloud by using clear data protection and security language in their agreements. However, in order to be able to effectively rely on contractual arrangements, cloud customers should perform a risk assessment related to the cloud provider's data protection practices prior to engaging the provider, including identifying the locations of the servers where the data is processed and assessing the provider's terms and conditions from a data protection point of view. The Working Party also urges providers to produce proof of independent third-party audits and certifications.

Guidelines for Contractual Arrangements

The Working Party calls on the parties involved to clearly define their roles and allocate responsibilities in the relevant services agreements. Cloud customers are responsible for choosing a cloud provider that guarantees compliance with the applicable data protection legislation. Cloud providers also are directly responsible for data security.

Based on the opinion, customers should ensure that, at a minimum, the provider contractually agrees to do the following:

1. Provide adequate data protection guarantees and implement appropriate data security measures (as further specified below) in accordance with applicable law. It is particularly recommended that the contract includes a Service Level Agreement and specifies penalties in the event of non-compliance.
2. Return the data or securely destroy/erase it at the customer's request after the service has been concluded.
3. Notify the customer in the event of a data breach and disclosure of data to law enforcement.
4. Assist customers in responding to individuals' requests.
5. Be allowed to use a subcontractor only if the customer has consented in writing (e.g., in the initial customer-provider service agreement); contractually impose on the subcontractor the same data protection and security obligations; inform the customer of the identity of the subcontractor and of any changes in this regard, with the customer retaining its right to object to such changes or terminate the contract; and offer contractual recourse to the customer if the subcontractor breaches its contract.

Guidelines for Data Protection and Security

The Working Party further identifies a number of data protection guarantees that must be provided in the cloud customer-provider contractual relationship. These are as follows:

1. Transparency: The provider must inform the customer of all subcontractors, including the locations of all data centers, so that the customer can provide the same information to individuals.
2. Purpose specification and limitation: It must be ensured (e.g., through specific loggings and audits) that personal data is not processed by the cloud provider and its subcontractors for purposes beyond those agreed upon in the service agreement.
3. Data erasure: The agreements between customers and providers and between providers and subcontractors must include clear language on data retention and stipulate the means for secure erasure of data and log data (e.g., destruction of hard drivers, demagnetizing of backup tapes, overwriting of data, etc.).

In addition, the Working Party sets forth specific criteria for data security with which the cloud provider must comply, as outlined below:

1. Availability: Ensure timely and reliable access to the processed data and prevent accidental loss of data (caused, for example, by loss of network connectivity or hardware or infrastructure failures) by using effective backup mechanisms.
2. Integrity: Detect data alterations by using cryptographic authentication mechanisms and intrusion-detection/prevention systems.
3. Confidentiality: Encryption should be used in all cases where data is "in transit" and "at rest," and remote administration should take place via a secure communication channel. For hosting services, it is recommended that the cloud customer encrypts the data prior to sending it to the cloud, and not rely on the provider's encryption method.
4. Transparency: The data protection and security implications of installing software on the customer's systems (e.g., browser plug-ins) to provide a service should be made clear to the customer.
5. Isolation: Administrators and users must only be able to access specific information and not the entire cloud, while shared resources between several cloud customers must be managed properly.
6. Intervenability: The cloud provider should cooperate with the client in facilitating the exercise of the rights of individuals; the same obligation must be imposed on any subcontractor.

Continued on page 3...

European Data Protection Law . . . *(continued from page 2)*

7. Portability: The customer should check whether and how the provider guarantees sufficient data-migration procedures for transferring the data to another cloud provider.
8. Accountability: Providers should be able to demonstrate that they have taken appropriate steps to ensure that the applicable data protection requirements have been implemented (e.g., through documentation and policies, and data-breach monitoring and loggings).

Guidelines for Data Transfers

Under EU data protection law, personal data may not be transferred to countries outside the EU unless an "adequate level of data protection" is ensured in the country to which the data is being transferred. The Working Party has concerns about relying solely on the U.S.-EU Safe Harbor framework when EU cloud customers export personal data to a U.S. cloud provider. The Working Party thus advises cloud customers to conduct a thorough investigation regarding the implementation in practice of the Safe Harbor Principles by the cloud provider and, where necessary, to request that additional data protection guarantees be provided (e.g., conclusion of the EU Model Contracts, use of binding corporate rules (BCRs) for data processors, or third-party auditing and security certification). Finally, the Working Party views critically the processing of so-called "sensitive data" (i.e., data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, or data concerning health or sex life) in non-EU clouds, and requires that additional guarantees be deployed in such cases.

Court Rejects Privacy Claims Arising from LinkedIn's Alleged Sharing of Unique Identifiers and Browsing History with Advertisers and Other Third Parties

Tonia Klausner
Partner, New York
tklausner@wsgr.com

Sharon Lee
Associate, Palo Alto
shlee@wsgr.com

Plaintiffs' class action counsel once again have been thwarted in their efforts to pursue claims against websites based on the alleged sharing of unique identifiers and browsing histories without users' prior express consent, and allegedly in violation of the website's privacy policy. In *Low v. LinkedIn,* No. 11-CV-01468-LHK (N.D. Cal., July 12, 2012), the Northern District of California decisively granted the defendant's motion to dismiss such a claim with prejudice.

Background

The plaintiffs sued LinkedIn Corp. on behalf of a proposed class of LinkedIn users whose browsing histories as well as unique identifiers allegedly had been shared by LinkedIn with third-party advertisers, marketers, data brokers, and web-tracking companies. The plaintiffs alleged that LinkedIn's practice of transmitting the URL of the LinkedIn user profile being viewed (which includes the viewed user's LinkedIn ID) along with the cookie ID of the person viewing the LinkedIn profile made it possible for third parties to identify the plaintiffs and obtain their browsing histories. This practice, the plaintiffs claimed, violated various state and federal laws, as well as LinkedIn's privacy policy, which stated that LinkedIn did not share user information with third parties for marketing purposes. Based on these allegations, the plaintiffs asserted claims for alleged violations of the federal Stored Communications Act (18 U.S.C. § 2701 *et seq.*), the California constitutional right of privacy, and the California False Advertising Law (Cal. Bus. & Prof. Code § 17500), as well as claims for breach of contract and common-law invasion of privacy, conversion, and negligence. The plaintiffs alleged they were harmed because (i) they were embarrassed and humiliated by the disclosure of their personally identifiable browsing histories, and (ii) their browsing histories are valuable property and they should have been paid for their use. After dismissing the plaintiffs' original complaint for lack of standing but allowing the plaintiffs to file an amended complaint, Judge Lucy H. Koh found that the plaintiffs had standing to pursue their claims based on alleged violations of statutory and constitutional rights, but nonetheless dismissed the plaintiffs' amended complaint with prejudice for failure to state any viable claim against LinkedIn, putting an end to the litigation.

Stored Communications Act Claim

The Stored Communications Act (SCA) generally prohibits both an electronics communications service (ECS) and a remote computing service (RCS) from disclosing the contents of an electronic communication.[1] Despite the plaintiffs' class action lawyers' repeated reliance on the SCA in similar privacy actions, the court correctly recognized that the SCA is not a catch-all Internet privacy statute, and must be applied based on the

[1] *See* 18 U.S.C. § 2702(a)(1)-(2).

Continued on page 4...

context of the specific communication at issue. Based on the facts alleged in the amended complaint, the court found that LinkedIn acted as neither an ECS nor an RCS in connection with the conduct at issue—it was acting as neither an email provider nor a "virtual filing cabinet" when it disclosed the LinkedIn IDs of its users and the URLs of web pages they viewed.

Invasion of Privacy Claims

Both a claim under the California constitutional right of privacy and a common-law invasion of privacy claim require conduct that is an "egregious breach of social norms" or "highly offensive" to a reasonable person. Judge Koh recognized the high threshold required by these standards and found that it had not been met by the conduct alleged. The court further concluded that the plaintiffs' assertion that third parties could de-anonymize the data was not sufficient because it was not clear that anyone actually had done so or what information these third parties obtained.

False Advertising Law Claim

The court dismissed the plaintiffs' claim that LinkedIn violated California's False Advertising Law (FAL) because although one plaintiff had paid for a LinkedIn service and therefore met the FAL's monetary loss requirement,[2] neither plaintiff alleged that they relied on any false advertisements or representations made by LinkedIn in making any purchasing decision. The plaintiffs asserted that LinkedIn violated its privacy policy representations that it does "not sell, rent or otherwise provide [users'] personal identifiable information to any third parties for marketing purposes." Despite this purported material misrepresentation, the court dismissed the claim because the plaintiffs did not allege that they were aware of, saw, or read LinkedIn's privacy policy in deciding whether to purchase a service from LinkedIn.

Contract and Negligence Claims

The court dismissed the contract and negligence claims for failure to allege any "appreciable and actual damage" or "appreciable, nonspeculative, present injury." After noting the implausibility of the allegation, Judge Koh concluded that a breach of contract claim does not provide recovery for the alleged embarrassment and humiliation that the plaintiffs claimed to have suffered due to the disclosure of their LinkedIn IDs and browsing histories. The court also followed the numerous courts that have rejected the plaintiffs' theory that the unauthorized collection of personal information creates an economic loss. The court further noted that even if such a theory of loss was viable, the plaintiffs had not alleged that they had either attempted or been foreclosed from opportunities to capitalize on the value of their personal data.

Conversion and Unjust Enrichment Claims

The court dismissed the plaintiffs' conversion claim for several reasons. First, the court followed numerous others in holding that personal information does not constitute property. Second, the information allegedly disclosed was not the plaintiffs' personal information. Rather, the user ID numbers generated by LinkedIn were not property over which the plaintiffs established a legitimate claim to exclusivity and the LinkedIn profile pages viewed by users were not capable of exclusive possession or control by the plaintiffs. Finally, consistent with the court's conclusion of no damages in connection with the plaintiffs' contract and negligence claims, the court found no allegations to reflect that the plaintiffs had been denied any opportunity to capitalize on the value of the information disclosed. The court dismissed the plaintiffs' unjust enrichment claim because California does not recognize unjust enrichment as a stand-alone claim.

Implications

The *Low* decision is another positive outcome for websites and other technology companies facing a steady onslaught of putative privacy class actions based on the alleged disclosure of information about users. In this case, as in most, the plaintiffs were not harmed in any way by the disclosure, but sought to invoke statutes intended for entirely different purposes and take a kitchen-sink pleading approach to try to state any claim against the defendant. Judge Koh followed the trend of most courts in rejecting these claims at the pleading stage, thereby sparing LinkedIn the significant costs and burdens of discovery. Of course, LinkedIn still had to defend the action, engaging in two rounds of motion-to-dismiss briefing before finally ridding itself of the claims. Additionally, the FTC has shown a willingness to pursue enforcement actions against companies based on similar conduct where a privacy policy states that user information will not be shared. (See the Agreement Containing Consent Order between the FTC and Myspace LLC, FTC File No. 102 3058, in which Myspace must, among other requirements, establish a comprehensive privacy program and obtain biennial assessments of the program by an independent auditor for the next 20 years.[3]) As a result, companies are encouraged to engage in regular reviews of their privacy policies to ensure they are consistent with actual practices.

[2]The court rejected plaintiff Low's theory that he had lost money or property because of alleged loss of the value of personal information.
[3]Our *Eye on Privacy* article regarding the Myspace consent agreement is available at http://www.wsgr.com/publications/pdfsearch/Eye-On-Privacy/July2012/index.html#5.

Tip

Technology doesn't care about geographic boundaries, but the law does. When operating online, be wary of the legal consequences of collecting personal information outside the United States, especially from the EU.

New Decision Interpreting Video Privacy Protection Act

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

Wendy Devine
Associate, San Diego
wdevine@wsgr.com

A federal magistrate in the Northern District of California recently held that the Video Privacy Protection Act (VPPA) applies to video streamed on the Internet.[1] Congress passed the VPPA in 1988, banning the "wrongful disclosure" of video-rental and sales records and requiring the destruction of such records under certain circumstances. The legislation was passed as a reaction to United States Supreme Court nominee Robert Bork's video-rental history being leaked to the press during the Senate debate over his nomination.

In its decision, the court denied Hulu's motion to dismiss the class action brought against the company for alleged violation of the VPPA. Hulu argued that (1) it did not fall within the VPPA definition of a "video tape service provider" and thus is not required to comply; (2) the class action plaintiffs are not "consumers" as defined by the VPPA, and therefore the statute does not apply to records of their video viewing; and (3) Hulu's disclosure of viewing information to third parties is part of its ordinary course of business, and thus is permitted under the VPPA.[2] The court rejected Hulu's first two arguments and found that, with regard to the applicability of the ordinary-course-of-business exception, a question of fact existed to be decided at a later point in the litigation.

First, the court found that the VPPA definition of "video tape service provider," which includes entities engaged in "delivery of prerecorded video cassette tapes or similar audio visual materials," is not limited to brick-and-mortar vendors or tangible media, as Hulu contended. Rather, the court concluded that the VPPA broadly encompassed delivery of video through media unknown at the time the legislation was drafted—including the Internet. No other court had ever so held. Second, the court rejected Hulu's argument that the VPPA definition of "consumer" requires payment of money, finding that if Congress had intended such an interpretation it would have explicitly included it in the definition. Thus, the court found that the plaintiffs, who alleged violation of the VPPA arising from their viewing of free streaming video content on the Hulu website, properly stated a claim.

The last few years have seen the filing of a series of class action suits alleging violations of the VPPA. These include actions against Fandango, Blockbuster, Overstock.com, and Gamefly (all in connection with Facebook's ill-fated Beacon service), as well as suits against Redbox, Best Buy, Netflix, and, most recently, Hulu. It is not surprising that the VPPA is a magnet for class action litigation because plaintiffs can argue that violations are punishable by $2,500 in statutory damages per violation. While that argument is often criticized and can be seen as an abuse of the class action mechanism, it nonetheless is one that may be made. Thus, while it remains too early to tell exactly how the case will unfold, the magistrate's ruling may be significant because it is the first to hold that a service like Hulu's might be a "video tape service provider."

Implications

These cases suggest that there will continue to be increasing pressure relating to video privacy and regulation.[3] This uncertainty and the potential breadth of the federal video privacy protections have not gone unnoticed. Pending legislation would clarify the VPPA provisions on the disclosure of video viewing history (e.g., H.R. 2471). Businesses associated with access to and use of video content over the Internet (including IP TV, smart TV, and other new technologies) may want to carefully review the *Hulu* decision and earlier cases, as well as related federal statutes. As consumption of video through new media continues to increase in popularity and the class action plaintiffs' bar becomes increasingly active, online privacy in the video arena should continue to warrant attention.

The magistrate's ruling may be significant because it is the first to hold that a service like Hulu's might be a "video tape service provider"

[1] *In re Hulu Privacy Litigation*, 2012 WL 3282960 (N.D. Cal., Aug. 10, 2012).
[2] 18 U.S.C. 2710(a)(4). ("'video tape service provider' means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.") 18 U.S.C. 2710(a)(1). ("'consumer' means any renter, purchaser, or subscriber of goods or services from a video tape service provider.")
[3] Cable television is currently regulated. 47 U.S.C. § 551.

FTC Settles with Facebook and Will Review Its Practice of Allowing Companies to Settle Charges of Wrongdoing While Denying the Violations Occurred

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

Dan Kane
Associate, Washington, D.C.
dkane@wsgr.com

On August 10, 2012, the Federal Trade Commission (FTC) announced that it had reached a final settlement with Facebook, Inc., over claims that Facebook deceived consumers by (1) misrepresenting its privacy policies and (2) making public certain user-generated information that users previously had designated as private. Under the settlement, Facebook agreed to not make any private user information public without the users' explicit consent and also agreed to submit to third-party audits for the next 20 years.

The commission's vote was 3-1-1, with Commissioner Maureen K. Ohlhausen abstaining and Commissioner J. Thomas Rosch dissenting. In his dissent, Commissioner Rosch questioned the FTC's statutory authority to accept a consent decree with an express denial of liability. Subsequently, the FTC announced that it will review its Rules of Practice in light of Commissioner Rosch's comments.

Background

Facebook operates www.facebook.com, a social networking website that enables site users to create online profiles and communicate with others. A user's online profile can include information such as the user's name, a profile picture, interest groups they have joined, a "friends" list of others on the site to whom the user is connected, photo albums and videos, and messages and comments posted by them or by other users. According to the FTC, Facebook had more than 750 million users as of August 2011.[1]

To run its network, Facebook assigns each member a user identification number (User ID), a persistent, unique number that enables retrieval of certain stored profile information.[2] According to the FTC's complaint, Facebook collected and stored profile information about its users, including: (1) registration information such as name, gender, email address, and birthday; (2) optional information such as profile picture, hometown location, interests, relationships, and education and work; and (3) other information based on a user's activities over time, such as a friends list, "liked" pages, photos and videos, and messages.

Further, Facebook operates the Facebook platform, a set of tools and programming interfaces that enables third parties to develop, run, and operate software applications, such as games, that users can interact with online ("third-party apps"). Facebook designed its platform such that third-party apps could gain access to user profile information when a user specifically authorized such access and if a user's "friend" authorized that third-party app to gain access to his or her user profile information. However, in practice, if a user authorized a third-party app to provide reminders about friends' birthdays, that application could access, among other things, the birthdays of the user's friends, even if these friends never authorized the application.[3]

FTC's Claims

In November 2011, in its eight-count complaint, the FTC alleged that Facebook's privacy practices were unfair and deceptive, and thus in violation of the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq.* Specifically, the FTC argued that Facebook's stated privacy policies did not match its actual privacy practices and that the company made significant retroactive changes to its privacy practices without obtaining users' consent.

Below is a detailed enumeration of the FTC's claims:

1. The FTC charged that Facebook promised that users could restrict their information to a limited audience by using certain privacy settings. However, when users went to Facebook's central privacy page and selected who could see their profiles and personal information, that choice did not apply to third-party applications.

2. The December 2009 changes to the privacy policy were marketed as giving users "more control," but instead certain information designated as private was made public under the new policy.

3. When Facebook overrode users' existing privacy choices in December 2009, the company materially changed the privacy of users' information and retroactively applied changes to information that it previously collected. The FTC alleged that doing so without users' informed consent was an unfair practice in violation of the FTC Act.

4. For a significant period of time after Facebook started featuring third-party apps on its site, it deceived users about how much of their information was shared with the apps they used. According to the complaint, third-party apps could access all user information, not only the information necessary to run the app.

5. Between September 2008 and May 2010, Facebook shared the User IDs of

[1] Analysis of Proposed Consent Order to Aid Public Comment In the Matter of Facebook, Inc., File No. 0923184, November 29, 2011, http://www.ftc.gov/os/caselist/0923184/111129facebookanal.pdf.
[2] Complaint In the Matter of Facebook, Inc., File No. 0923184, November 29, 2011, http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf.
[3] *Id.*

Continued on page 7...

members who clicked on site advertisements even though it told users it would not share their personal information with advertisers.

6. The FTC challenged the function of Facebook's Verified Apps program. While Facebook claimed that apps in the program were subject to a "detailed review process . . . to help users identify applications they can trust," the FTC found that Facebook took no additional steps to verify either the security of a Verified App's website or the security the app provided for the information it collected beyond what it did for any other app.

7. The FTC charged Facebook with making deceptive claims about its photo and video deletion policy. Each of the photos and videos a user uploads onto Facebook has a content URL—a URL for its location on Facebook's servers. While Facebook allegedly told users they could deactivate or delete their accounts and no one would be able to gain access to those users' photos and videos after that point, Facebook still provided access to photos and videos to anyone who accessed them via the content URL.

8. Finally, the FTC challenged Facebook's statements about its compliance with the U.S.-EU Safe Harbor Framework, a mechanism by which U.S. companies may transfer data from the European Union to the United States consistent with European law.

Settlement Terms

Under the settlement originally proposed in November 2011[4] and approved on August 10, 2012, Facebook is required to give consumers clear and prominent notice and obtain their express approval prior to sharing any information outside of their privacy settings. To ensure that all levels of the company comply with this standard, Facebook must maintain a comprehensive internal privacy program focused on protecting consumers' information.

In addition, the proposed settlement bars Facebook from making any further deceptive privacy claims, requires that the company obtain consumers' approval before it changes the way it shares their data, and requires that it obtain periodic assessments of its privacy practices by independent, third-party auditors for the next 20 years. Failure to comply with these terms may result in a penalty of $16,000 for every violation.[5]

Specifically, under the proposed settlement, Facebook is:

- barred from making misrepresentations about the privacy or security of consumers' personal information;
- required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences;
- required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;
- required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers' information; and
- required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected.

The proposed order also contains standard record-keeping provisions to allow the FTC to monitor compliance with its order.

Commissioner Rosch's Dissent

Commissioner Rosch dissented on two fundamental aspects of the settlement agreement. The first focuses on substantive concerns over the scope of the settlement. The second addresses a procedural question regarding the FTC's jurisdiction to reach a settlement of this nature.

In Commissioner Rosch's opinion, though an application may technically be independent of Facebook, the way it interacts with the larger framework makes it an integral aspect of the social network. As such, consumers will be deceived if applications do not provide users with clear and obvious notice of their disclosure protocols. Commissioner Rosch does not believe that the settlement adequately protects consumers from future violations due to the lax privacy standards of certain applications found within the Facebook ecosystem.

In response, the majority argued that the settlement's breadth allays Commissioner Rosch's concerns. Under the settlement's framework, the majority believe that Facebook is required to accept liability for any privacy violations committed by applications within the Facebook ecosystem.[6]

Commissioner Rosch also questioned whether the FTC is statutorily empowered to accept a consent decree where a respondent expressly denies liability.

> [In t]he Agreement Containing Consent Order, respondent Facebook "expressly denies the allegations set forth in the complaint, except for the jurisdictional facts." Our Federal Trade Commission Rules of Practice do not provide for such a denial. . . . [A]s I read Section 5, Commissioners are authorized to accept a consent agreement only if there is reason to believe that a respondent is engaging in an unfair or deceptive act or practice

[4]FTC Press Release, "Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises," November 29, 2011, http://www.ftc.gov/opa/2011/11/privacysettlement.shtm.
[5]Statement of the Commission In the Matter of Facebook, Inc., File No. 092 3184, Docket No. C-4365, August 10, 2012, http://www.ftc.gov/os/caselist/0923184/120810facebookstmtcomm.pdf.
[6]*Id.*

Continued on page 8...

FTC Settles with Facebook . . . *(continued from page 7)*

> and that acceptance of the consent agreement is in the interest of the public. . . . I should add that I am also in favor of reconsidering Rule 2.32's authorization of the inclusion of language in a consent agreement that it "is for settlement purposes only and does not constitute an admission by any party that the law has been violated as alleged in the complaint."

The majority here strongly disagreed with Commissioner Rosch's premise that Facebook's denial of liability negated the FTC's authority to enter the settlement. They noted that a respondent's denial does not hinder the commission's ability to find a reasonable basis to finalize a settlement or to enforce the order that follows. The majority noted that an extensive investigation and detailed staff recommendation has given the commission a strong—not just a reasonable—basis to issue its complaint, which cannot be diminished by the denial of liability on the part of Facebook. Moreover, express denials of liability are consistent with the commission's current Rules of Practice.

Despite their disagreement with Commissioner Rosch's position in this matter, the majority noted that express denials will be strongly disfavored in the future. In addition, the majority noted that the commission will consider whether Commissioner Rosch's suggestion that consent order language should include a statement that the respondent "neither admits nor denies" will be more effective in ensuring that there are no misimpressions about the commission's process. Accordingly, the FTC will consider whether a modification to the FTC's Rules of Practice is warranted in the coming months.[7]

Implications

Facebook's settlement with the FTC underscores the agency's growing interest in protecting the privacy of consumers in the social media space. This settlement, particularly in light of the FTC's consent agreement with Myspace earlier this year,[8] indicates that the FTC regards proper privacy disclosures in social media as essential moving forward. Indeed, Chairman Leibowitz's words shortly after filing the complaint indicate as much: "Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users. . . . Facebook's innovation does not have to come at the expense of consumer privacy."[9]

Additionally, it will be interesting to see how the FTC responds to Commissioner Rosch's dissent. While the majority previewed that express denials of liability will be strongly disfavored in future settlements, the FTC is not the only federal agency that allows a company to deny liability in a settlement. In July, the Justice Department reached a $2 billion settlement with GlaxoSmithKline over allegations that the company defrauded the government with pharmaceutical sales. Despite the payment, GlaxoSmithKline expressly denied that it had engaged in any wrongful conduct.[10] To the extent that accepting a formal position on a certain type of settlement would put the FTC at a disadvantage compared to other agencies, it may not want to commit to not accepting a settlement where liability is expressly denied.

[7] *Id.*
[8] Our *Eye on Privacy* article regarding the Myspace consent agreement is available at http://www.wsgr.com/publications/PDFSearch/eye-on-privacy/July2012/index.html#5.
[9] FTC Press Release, "Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises," November 29, 2011, http://www.ftc.gov/opa/2011/11/privacysettlement.shtm.
[10] Edward Wyatt, "Letting Companies Settle While Denying Guilt Reconsidered by FTC," *New York Times*, August 10, 2012, http://www.nytimes.com/2012/08/11/business/facebook-settlement-on-privacy-is-finalized-by-ftc.html.

FTC Proposes Additional Revisions to Children's Online Privacy Protection Rule

Tonia Klausner
Partner, New York
tklausner@wsgr.com

Matthew Staples
Associate, Seattle
mstaples@wsgr.com

On August 1, 2012, the Federal Trade Commission (FTC) issued a supplemental notice of proposed rulemaking (Supplemental NPR)[1] in which it proposed additional modifications to the Children's Online Privacy Protection Rule (COPPA Rule), which implements the Children's Online Privacy Protection Act (COPPA).

COPPA generally requires that all operators of commercial websites or online services that are directed to or knowingly collect personal information from children under 13 years of age disclose their information-collection practices and obtain verifiable parental consent before collecting personal information from children. The proposed modifications augment the FTC's notice of

[1] The Supplemental NPR is available at http://www.ftc.gov/os/2012/08/120801copparule.pdf.

Continued on page 9...

proposed rulemaking issued on September 15, 2011,[2] and address certain comments received by the FTC to date regarding the original NPR, as well as the FTC's experience in administering and enforcing the COPPA Rule. As explained below, the proposed modifications would further expand the scope of entities that the FTC deems to be covered by COPPA, but they also would ease consent requirements somewhat with respect to covered websites and online services that appeal to mixed-age audiences.

Companies that may be affected by the proposed amendments have until September 24, 2012, to submit comments to the FTC.

Proposed Amendments

The FTC's proposed amendments would modify four key definitions in the COPPA Rule: "operator," "website or online service directed to children," "support for internal operations," and "personal information."

Modifications to "Operator" and "Website or Online Service Directed to Children" to Address Third-Party Collection of Personal Information

In the Supplemental NPR, the FTC noted that public comments and its law enforcement experience highlighted the need for the FTC to allocate and clarify responsibilities under COPPA when independent entities or third parties such as advertising networks, social media services, or other providers of downloadable software kits (referred to in the Supplemental NPR as "plug-ins") collect information from users through child-directed websites and online services. A child-directed site or online service would determine the child-directed nature of the content, but third-party advertising networks and providers of plug-ins collect information that would be considered personal information under the COPPA Rule.

The FTC noted changes in technology that have made it easy and commonplace for child-directed sites and services to integrate social networking and other personal-information-collection features into the content offered to their users without maintaining ownership, control, or access to the personal information that is collected. Given these advancements in technology, the FTC proposes changes to the definitions of "operator" and "website or online service directed to children" that would hold ***both*** (i) the child-directed website or online service and (ii) the information-collecting website or online service responsible as covered "co-operators" under the COPPA Rule.

First, the modified COPPA Rule would redefine the term "operator." COPPA applies to child-directed websites and online services that directly collect or maintain information about users, "or on whose behalf such information is collected or maintained."[3] The modified COPPA Rule would make clear that operators of websites that do not themselves collect personal information that triggers the notice and consent requirements of COPPA still would be subject to those requirements if third parties such as advertising networks or downloadable plug-ins collect such information. In the FTC's view, such third parties are collecting the information "on behalf of" the child-directed website or online service. Specifically, the FTC proposes revising its definition of "operator" to add a proviso stating:

> Personal information is *collected or maintained on behalf of* an operator where it is collected in the interest of, as a representative of, or for the benefit of, the operator.[4]

The FTC reasoned that a child-directed site or service is in the position to provide the required notice and obtain the required parental consent, and can control which plug-ins, software downloads, or advertising networks it integrates into its site or service.

Second, the modified COPPA Rule would make clear that any third-party operator that collects personal information through child-directed websites and services also is subject to COPPA's requirements if it knows or has reason to know that it is collecting such information through a child-directed website or online service. The FTC would effectuate this by including in the definition of "website or online service directed to children" any operator that "knows or has reason to know" it is collecting personal information through any website or online service otherwise covered by COPPA.[5] In proposing this modification, the FTC expressed a desire to cover advertising networks, plug-ins, and other third-party websites and online services that collect personal information through child-directed properties.

The FTC clarified that in using the phrase "reason to know" as part of this proposed modification, it is not imposing a duty on third-party operators to monitor or investigate whether their services are incorporated into child-directed properties; these entities, however, would not be free to ignore credible information brought to their attention indicating that such is the case. Critically, while the examples given by the FTC center around advertising networks and plug-ins, the operator of any third-party website or online service that collects personal information through another website or online service would be subject to this "knows or has reason to know" standard.

The FTC stated its belief that the proposed modification to "website or online service directed to children," along with its proposed modifications to the definition of "operator," would hold a child-directed property to be a "co-operator" equally responsible under the COPPA Rule for personal information collected by a plug-in, advertising network, or other third-party website or online service, which would help ensure that operators in both positions cooperate to fulfill their obligations under COPPA to notify parents and obtain parental consent.[6]

---

[2]The original NPR is available at http://www.ftc.gov/os/2011/09/110915coppa.pdf. Our WSGR Alert covering the original NPR is available at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/pdfsearch/wsgralert-childrens-online-privacy-protection.htm.
[3]*See* 15 U.S.C. 6501(2).
[4]Supplemental NPR, 77 FR at 46644.
[5]Supplemental NPR, 77 FR at 46645.
[6]*Id.*

Continued on page 10...

FTC Proposes Additional Revisions . . . *(continued from page 9)*

Modifications to "Website or Online Service Directed to Children" to Address Websites and Online Services Directed to Children and Families

The FTC also proposes to modify the COPPA Rule's definition of "website or online service directed to children" to treat websites differently depending on the extent to which they are directed to children. Currently, all websites and online services directed to children are subject to COPPA's requirements, even if only a portion of the site or service is so directed, and even if the site or service attracts a substantial number of persons over the age of 13 as users. Under the proposed revisions, websites and online services that knowingly target or have content likely to draw children under 13 as their primary audience still must treat all users as children (that is, provide notice to parents and obtain consent before collecting personal information from any user).[7] Websites and online services with child-oriented content appealing to a mixed audience, where children under 13 are likely to be an overrepresented group, would not be deemed directed to children if they use an age screen prior to collecting personal information from any users. When users identify themselves as under 13 in the age screen, the site or service would be deemed to have actual knowledge that such users are under 13. As a result, it would need to obtain appropriate parental consent before collecting any personal information from them, and also comply with all other aspects of the COPPA Rule.[8] Parental consent would not be required from users who identify themselves as 13 or older.

Definition of "Personal Information"

The FTC also seeks to clarify two aspects of the definition of "personal information," the collection of which subjects the operator to COPPA's requirements: screen or user names and persistent identifiers.

I. Screen or User Names

In the original NPR, the FTC had proposed to define as personal information "a screen or user name where such screen or user name is used for functions other than or in addition to support for the internal operations of the website or online service." This was intended to address scenarios in which a screen or user name could be used by a child as a single credential to access multiple online properties, thereby permitting him or her to be directly contacted online regardless of whether the screen or user name contained an email address.

Citing comments promoting the benefits of using screen names as alternatives to email addresses and other personal information, including the benefits of using single sign-in identifiers across sites and services, the FTC proposes to modify the definition of "personal information" to include screen names or user names only where they function in the same manner as "online contact information" (i.e., they permit direct contact with a person online).[9]

II. Persistent Identifiers and Support for Internal Operations

In the original NPR, the FTC proposed changes to the definition of "personal information" to include, among other things, persistent identifiers "used for functions other than or in addition to support for the internal operations of the website or online service." The FTC also proposed to include in the definition of personal information "identifiers that link the activities of a child across different websites or online services."[10]

In response to various concerns of commenters, the FTC proposes modifications to the definition of "personal information" to (i) address concerns about the confusion caused by having two different portions of the "personal information" definition dealing with persistent identifiers and (ii) provide more specificity to the types of activities that would be considered "support for internal operations."

First, with respect to persistent identifiers, the FTC proposes that they be included as "personal information" where they "can be used to recognize a user over time, or across different websites or online services."[11] These would include, but would not be limited to, customer numbers held in cookies, IP addresses, processor or device serial numbers, and unique device identifiers. Critically, unlike the FTC's original modified definition, persistent identifiers would have to be able to recognize a user over time or across different websites or online services in order to be considered "personal information."

Second, the FTC proposes adding a definition for the "support for internal operations" exclusion to include "those activities necessary to: (a) maintain or analyze the functioning of the website or online service; (b) perform network

---

[7]The proposed revised definition of "website or online service directed to children" in the Supplemental NPR is a commercial website or online service, or portion thereof, that:

(a) knowingly targets children under age 13 as its primary audience; or
(b) based on the overall content of the website or online service, is likely to attract children under age 13 as its primary audience; or
(c) based on the overall content of the website or online service, is likely to attract an audience that includes a disproportionately large percentage of children under age 13 as compared to the percentage of such children in the general population; *provided however that* such website or online service shall not be deemed to be directed to children if it: (i) does not collect personal information from any visitor prior to collecting age information; and (ii) prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first obtaining verifiable parental consent.

Supplemental NPR, 77 FR at 46646.
[8]*Id.*
[9]Supplemental NPR, 77 FR at 46647. In the original NPR, the FTC had proposed amending "online contact information" to include "an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over Internet protocol (VOIP) identifier, or a video chat user identifier." NPR, 76 FR at 59810.
[10]NPR, 76 FR at 59812.
[11]Supplemental NPR, 77 FR at 46647.

Continued on page 11...

FTC Proposes Additional Revisions . . . *(continued from page 10)*

communications; (c) authenticate users of, or personalize the content on, the website or online service; (d) serve contextual advertising on the website or online service; (e) protect the security or integrity of the user, website, or online service; or (f) fulfill a request of a child as permitted by [limited circumstances under the COPPA Rule]; so long as the information collected for the activities listed in (a)-(f) is not used or disclosed to contact a specific individual or for any other purpose."[12] The FTC emphasized that to fall within the "support for internal operations" exclusion, the information may not be used or disclosed to contact a specific individual, including through the use of behaviorally targeted advertising, or for any other purpose not elucidated in the proposed "support for internal operations" definition.[13]

Implications of Proposed Amendments

The FTC's proposed amendments reflect its continued expansion of the scope of the COPPA Rule, while at the same time recognizing some of the compliance challenges faced by covered operators, as well as the need for more clarity regarding the FTC's expectations under the original proposed modifications to the COPPA Rule.

The amendments requiring operators of websites and online services directed to children to know whether advertising networks, the operators of integrated social media services or other plug-ins, or other integrated third-party services collect personal information would impose new burdens on the operators of those child-directed sites and services. Similarly, the operators of websites and online services that collect personal information through third-party websites and online services would need to assess what they know about the websites and online services into which they are integrated in order to determine whether they may have notice and consent requirements.

Otherwise, the changes generally appear helpful to operators of websites and other online services. The amendments to permit websites and online services with child-directed content to age-screen may allow those website and service operators to engage in greater collection and use of personal information from their users who are 13 years of age or older. The clarifications regarding "screen and user names" address concerns that many website and online service operators had after seeing those data elements identified as "personal information" in the original NPR. Similarly, the modifications to the definition of "support for internal operations" add some much-needed clarification.

Operators of commercial websites and online services, particularly child-directed websites or online services that contain integrated third-party services that may collect personal information, as well as websites or online services that collect personal information through integration with third-party services or that collect persistent identifiers in connection with behavioral advertising, may wish to review their existing practices and consider submitting comments.

More generally, all companies that interact with children on the Internet should be aware of COPPA, the COPPA Rule, and the FTC's enforcement in this area. Since its enactment in 2000, the COPPA Rule has been aggressively enforced by the FTC. Numerous companies have paid multimillion-dollar settlements or penalties due to non-compliance. The FTC's proposed revisions to the COPPA Rule in the original NPR, and now in the Supplemental NPR, reflect the commission's continued focus on consumer privacy, particularly with respect to children.

[12] Supplemental NPR, 77 FR at 46648.
[13] *Id.*

Voluntary Privacy Framework for Asia-Pacific Economic Region Takes Next Steps with U.S. Participation

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

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

The Federal Trade Commission (FTC) continues to support voluntary efforts to protect privacy. On July 25, 2012, the Asia-Pacific Economic Cooperation (APEC) approved the United States' participation in the APEC Cross-Border Privacy Rules (CBPR) system. The CBPR system is a process by which an organization can be certified by an independent agent as adhering to a set of baseline privacy program requirements consistent with the APEC Privacy Framework. It is believed that the CBPR system will promote greater confidence in international transfers of personal data within APEC member countries.

APEC's Privacy Framework

APEC is a cooperative group of countries working to facilitate economic growth, cooperation, trade, and investment in the

Continued on page 12...

Asia-Pacific region.[1] To help avoid barriers to personal information flows, the APEC member countries adopted common information privacy standards through the APEC Privacy Framework, which was finalized in 2005 and includes the following principles:

- preventing harm
- notice
- limiting collection to the purposes stated in the notice
- uses of personal information
- choice
- integrity of personal information
- security safeguards
- access and correction
- accountability

Cross-Border Privacy Rules

The APEC Privacy Framework does not have legal status as a treaty or other law, and many detractors have argued that it lacks effectiveness because it has no meaningful enforcement requirements. In September 2007, APEC sought to address this alleged lack of enforcement by developing the APEC CBPR system to facilitate personal data flows across the APEC region. Importantly, participation in the APEC CBPR system does not replace a participating organization's domestic legal obligations. Where domestic legal requirements exceed what is expected in the APEC CBPR system, the full extent of such domestic law and regulation will continue to apply.

Participation in the APEC CBPR System

To participate in the APEC CBPR system, an organization must develop internal business policies and procedures controlling cross-border data transfers. An APEC-recognized accountability agent must assess and confirm that the policies and procedures comply with the minimum requirements of the APEC Privacy Framework. If the policies and procedures are deemed compliant, an organization is certified as complying with the APEC CBPR system. An organization that participates in the APEC CBPR system must publicly declare that it will comply with the system's program requirements, and must make these requirements publicly accessible.

FTC's Involvement

On July 25, 2012, the U.S. was confirmed as the first country that met the conditions set forth in the APEC CBPR Charter for participation in the new CBPR system. The United States nominated the FTC as the CBPR system enforcement authority in the U.S. Participating organizations that adhere to the CBPR principles will be subject to the FTC's jurisdiction to investigate and prosecute unfair and deceptive trade practices.

Generally, under Section 5 of the FTC Act, the FTC can enforce the public representations made by organizations. Section 5 prohibits unfair or deceptive acts or practices in or affecting commerce and gives the FTC broad authority to take action against such acts and practices. Accordingly, if an organization fails to comply with any of the CBPR system program requirements, its public representation of compliance may constitute an unfair or deceptive act or practice subject to enforcement of Section 5 of the FTC Act.

According to the United States' Notice of Intention to Participate in the CBPR System,[2] the U.S. government took the position that the following practices may violate Section 5 of the FTC Act, 15 U.S.C. § 45:

- failing to comply with a representation relating to any of the CBPR system program requirements;
- failing to comply with the CBPR system program requirements when displaying a seal, trustmark, or other symbol on the organization's website or on any other of its own publicly available documentation that indicates that it participates in the CBPR system; or
- failing to comply with the CBPR system program requirements after causing the organization's name to appear on a list of organizations that are certified for participation in the CBPR system.

Implications

Organizations contemplating widespread data transfers and processing of personal data within the APEC member countries may benefit by participating in the CBPR system. An organization can become certified with the APEC CBPR system to increase trust with third parties and consumers with which it does business. However, it may be too early to identify the practical and long-term benefits of the system for individual participating organizations, because the system does not displace local legal requirements. Further, unlike the EU, geographic restrictions on personal data transfers have not yet taken hold. While the benefits of voluntary certification are unclear, the potential legal consequences of noncompliance for participating organizations are now in place. Once an organization in the U.S. represents that it complies with the CBPR system program requirements, the FTC has the jurisdiction to assess penalties for non-compliance under Section 5 of the FTC Act. The APEC CBPR system is the latest in a series of steps being undertaken globally to facilitate international data transfers in a responsible and accountable manner that respects privacy considerations.

---

[1] Member countries include Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; The Republic of the Philippines; The Russian Federation; Singapore; Chinese Taipei; Thailand; United States of America; and Viet Nam.

[2] The U.S.'s Notice of Intention to Participate in the CBPR System is available at http://web.ita.doc.gov/ITI/itiHome.nsf/($All)/367984E24FD1012485257A48004493C5/$FILE/United%20States%20Notice%20of%20Intent%20to%20Participate%20in%20the%20CBPR%20System.pdf.