Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

EYE ON PRIVACY

MAY 2013

Welcome

In this month's issue of *Eye on Privacy*, we focus on new guidance and rules promulgated by privacy regulators in the United States and Europe. Specifically, we discuss recent revised guidance from the Federal Trade Commission on proper disclosure practices for online and mobile advertising, an extensive opinion from the Article 29 Working Party providing guidance on how to comply with the European Union's core data protection principle of "purpose limitation," and a recently issued rule from the Department of Health and Human Services that may have significant implications for cloud storage providers and other companies that may be storing protected health information. Finally, we also analyze the Supreme Court's recent decision in *Clapper v. Amnesty International USA* and its implications for companies defending against privacy class actions.

In addition to our bi-monthly issues of *Eye on Privacy*, we encourage you to review our WSGR Alerts for analysis of important privacy issues as they happen. Just last week, we issued an alert on the FTC's long-awaited overhaul of the Children's Online Privacy Protection Rule FAQs and the agency's decision not to postpone the July 1 effective date for the recent revisions to the COPPA Rule.

As always, we would love to hear your suggestions for future article topics—please feel free to send us a note at PrivacyAlerts@wsgr.com.

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

FTC Issues New Guidance for Disclosures in Online Advertising

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

Caitlin Courtney
Associate, Palo Alto
ccourtney@wsgr.com

Mobile and social media marketing are on the rise.[1] With that in mind, the Federal Trade Commission (FTC) issued new guidance for advertisers on how to make effective mobile and other online disclosures. Entitled ".com Disclosures: How to Make Effective Disclosures in Digital Advertising,"[2] the guidance provides an update to the FTC's 2000 publication on the same topic. The revised guidance is intended to address the expanding use of smart phones and social media marketing, where small screens and character limitations pose challenges for companies making advertising claims.[3] Although the guidance itself is not law, the FTC cautions that these disclosures are required by the laws it enforces.

The new guidance reiterates that the rules that apply in the consumer protection space as a whole, including the FTC Act's prohibition on "unfair or deceptive acts and practices," apply equally online and in the mobile marketplace.[4] Although the revised guidance includes specifics such as size, font, and locations of disclosures, it stresses that the ultimate test for whether a particular ad is deceptive, unfair, or violates an FTC law or rule is whether the information intended to be disclosed is

Continued on page 2...

[1] Total mobile and social media revenues increased 30.2 percent to $45.38 billion in 2011, and have risen at a compound annual growth rate of 28.7 percent since 2006. Mobile and social media revenues are expected to exceed $100 billion by 2015, the fastest any communications industry has surpassed this benchmark, outpacing subscription TV and the Internet by nearly 20 years. *See* "U.S. Mobile and Social Media Forecast 2012-2016," PQ Media, *available for purchase at* http://www.pqmedia.com/mobilesocialforecast-2012.html.

[2] FTC, ".com Disclosures: How to Make Effective Disclosures in Digital Advertising" (2013), *available at* http://www.ftc.gov/os/2013/03/130312dotcomdisclosures.pdf (".com Disclosures").

[3] *See id.* at i.

[4] *Id.*

In This Issue

actually conveyed to consumers. Importantly, the FTC warns that "if a particular platform does not provide an opportunity to make clear and conspicuous disclosures, then that platform should not be used to disseminate advertisements that require disclosures."[5]

FTC Advertising Law Basics Apply in the Online Space

As with the 2000 guidance, the new document emphasizes that the basic principles of FTC adverting law apply to advertisements in any form, including online ads. These core principles require that advertising must: (1) be truthful and not misleading; (2) be backed by evidence that supports the claims in the advertisement; and (3) not be unfair.[6] If an ad is likely to mislead a consumer, be unfair, or otherwise violate a FTC rule without certain qualifying information, then a disclosure must be used to qualify or limit that claim.[7] If practical, advertisers should incorporate this disclosure into the claim instead of having a separate disclosure that qualifies each claim.[8] The new guidance reiterates the long-held FTC principle that a disclosure can only qualify or limit a claim to avoid a misleading impression—it cannot cure a false claim.

The FTC also requires that disclosures be clear and conspicuous.[9] In determining whether a disclosure is clear and conspicuous, the FTC encourages advertisers to consider: (1) the proximity and placement of the disclosure; (2) the prominence of the disclosure, including the size, color, and graphics used to draw attention to the disclosure; (3) whether the disclosure is unavoidable; (4) the risk that other parts of the advertisement could distract a consumer from reading the disclosure; (5) whether the disclosure needs to be repeated multiple times or in multiple locations to effectively reach consumers; (6) whether the disclosure is at an adequate volume or appears for a sufficient duration; and (7) whether the language of the disclosure is understandable to the intended audience.[10]

Making Clear and Conspicuous Disclosures in Space-Constrained Online Ads

The FTC emphasizes that these traditional factors should be used to evaluate whether disclosures are likely to be clear and conspicuous in the context of online ads. With regard to the proximity and placement of disclosures, the FTC explains that the extent to which a consumer needs to scroll in order to view disclosures may affect whether the disclosures are clear and conspicuous, especially on a small screen.[11] If scrolling is necessary to view a disclosure, the FTC recommends that the disclosures be "unavoidable"—that is, consumers should be required to scroll through the disclosure before proceeding with a transaction.[12] The guide also encourages optimizing websites for mobile devices to eliminate the need for scrolling.

Another factor that the FTC will consider in determining if a disclosure is clear and conspicuous is the use of hyperlinks. The FTC cautions that while hyperlinks may be useful, particularly where the disclosure is lengthy or needs to be repeated, they may never be used if the disclosure is integral to or inseparable from the claim.[13] Rather, for inseparable claims, the disclosure must be placed on the same page and immediately next to the claim.[14] The guidance explains that for hyperlinks to be effective, they should be obvious; labeled to convey the importance, nature, and relevance of the information to which the hyperlink applies; indicate why a claim is qualified or linked to a disclosure; account for the technological differences and limitations of different platforms; be presented consistently in a hyperlink style throughout the ad; be prominently placed; and lead the user directly to the hyperlinked text.[15] The guidance cautions that hyperlinks are likely inadequate where they use a single word or phrase, or where they are labeled "disclaimer," "fine print," or "important information," because consumers are unlikely to understand the significance of the hyperlinked information.[16] Further, the guide encourages advertisers to use analytic tools that measure click-through rates and to not ignore data that suggests that hyperlinks are not followed.[17]

The FTC also singles out pop-ups as an issue that could negatively impact the effectiveness of required disclosures, because customers might not read the information or understand what claim the disclosure relates to, and pop-up-blocking software may block the pop-up.[18]

In addition, the new guidance clarifies that disclosures must be communicated *before* a customer makes the decision to purchase an item (e.g., before a customer adds an item to a shopping cart) rather than solely on the "order screen."[19] If a disclosure is unlikely to be read because a consumer is interested in completing the task at hand, such as signing up to receive a service, the guide recommends requiring the user to affirmatively acknowledge the disclosure by answering a question about the disclosure before an item is added to the shopping cart.[20] The FTC stresses that if a product will be sold at a physical store, companies must make the disclosure before the customer visits the store.[21]

The new guidance suggests that disclosures should be repeated if necessary. For example, if a customer can access a website in different ways, it may be necessary to include disclosures in multiple locations.[22] Likewise, if claims are repeated throughout an ad, it may be necessary to repeat the disclosure that relates to those claims.[23]

The release also addresses the space limitations imposed by different methods of advertising, such as space-constrained banner ads and tweets. The FTC reiterates that disclosures are required in each ad despite the limited space, and encourages companies to use creativity and abbreviations.[24] In determining whether the disclosure should be placed in the ad itself or on the landing page,

[5] *Id.* at iii.
[6] *Id.* at iv.
[7] *Id.* at 5-6.
[8] *Id.* at i.
[9] *Id.* at 6.
[10] *Id.* at 7.
[11] *Id.*
[12] *Id.* at 9.
[13] *Id.* at 10.
[14] *Id.*
[15] *Id.* at 11-13.
[16] *Id.* at 12.
[17] *Id.* at 13.
[18] *Id.* at 13-14.
[19] *Id.*
[20] *Id.* at 18-19.
[21] *Id.* at iii.
[22] *Id.* at 19.
[23] *Id.*
[24] *Id.* at 15 and 16.

Continued on page 3...

FTC Issues New Guidance . . . *(continued from page 2)*

the FTC advises advertisers to consider how important the information is to prevent deception, how much information needs to be disclosed, the burden of disclosing such information in the ad itself, how much information the consumer may absorb from the ad, and how effective the disclosure would be if it were made on the website.[25]

Finally, the FTC stresses that claims should be tailored to the media of the campaign. Audio claims should have audio disclosures that are presented in a sufficient volume and cadence to be understandable, and written claims should use written disclosures.[26] Disclosures in mixed media, such as video clips, should be presented for a duration that allows the customer to read them.[27]

Specific Guidance for Disclosures in Social Media, Such as Tweets and Blogs

Through sample mock advertisements, the FTC offers the following specific guidance for disclosures in social media, such as in blogs and space-constrained tweets:[28]

- The FTC's "Guides Concerning the Use of Endorsements and Testimonials in Advertising"—and particularly the requirement that endorsers must disclose any material connections to the products they endorse—apply equally to endorsements that bloggers and tweeters make in social media.[29]
- If you endorse a product through a tweet, it is not sufficient to include a non-descriptive hyperlink, such as a tiny URL, to additional disclosures. Even if the link in the message leads directly to sufficient disclosures, that would, in the FTC's view, still be insufficient because users may not click through to the linked website.[30]
- Including a required disclosure in a subsequent tweet would be problematic because unrelated messages may arrive in the interim and, by the time the disclosure arrives, consumers might no longer be reading these messages, or they may not realize that those disclosures pertain to the original message.[31]
- Even including a hashtag such as "#Spon" may not be sufficient to disclose that a person tweeting a product recommendation is a paid endorser because consumers may not understand that the hashtag means that the message was sponsored by an advertiser.[32] If a significant portion of the reasonable viewers would not understand this, then the ad would be deceptive. The FTC has previously advised that hashtags such as "#paid ad," "#paid," or "#ad" may be sufficient.[33]

A blog post disclosing in the last sentence that the blogger received the reviewed product for free may be insufficient where the blog post contains several hyperlinks in the text that could cause readers to click away before they get to the end of the text.[34]

Takeaways

As more advertising dollars are directed toward mobile and social media marketing, advertisers increasingly are challenged to make effective disclosures in limited spaces. The .com Disclosures can serve as a roadmap for how to incorporate such disclosures into mobile and social marketing. Advertisers would be well advised to familiarize themselves with the guidance because, although it is not law, the FTC may bring enforcement actions against companies that decline to follow it.

---

[25] *Id.* at 15.
[26] *Id.* at 20.
[27] *Id.*
[28] *Id.* at A-17 – A-20.
[29] FTC, "Guides Concerning the Use of Endorsements and Testimonials in Advertising" (16 C.F.R. Part 255), 73 Fed. Reg. 72374 (Nov. 28, 2008).
[30] *See* .com Disclosures at A-17.
[31] *See id.* at A-19.
[32] *See id.* at A-20.
[33] "The FTC's Revised Endorsement Guides: What People are Asking," *available at:* http://business.ftc.gov/documents/bus71-ftcs-revised-endorsement-guideswhat-people-are-asking.
[34] *See* .com Disclosures at A-25.

European Regulators Opine on "Purpose Limitation" Principle – What Constitutes "Compatible Use" in the Context of Big Data?

Cédric Burton
Associate, Brussels
cburton@wsgr.com

Anna Pateraki
Associate, Brussels
apateraki@wsgr.com

On April 2, 2013, the European data protection regulators (the "Article 29 Working Party" or the "WP29") issued a 70-page opinion providing guidance on how to comply with the core EU data protection principle of "purpose limitation."[1] This opinion gives a good indication of how EU regulators would apply their national data protection law to specific processing activities such as email marketing, behavioral advertising, profiling, and tracking of user behavior and big data. It is relevant for companies of all sizes, including non-EU-based companies, offering online services to users in the EU, since the EU regulators tend to take a broad approach regarding the applicability of EU data

Continued on page 4...

[1] Article 29 Working Party Opinion 03/2013 on purpose limitation, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

protection law.[2] This article addresses certain aspects of the opinion.[3]

The Principle of "Purpose Limitation"

"Purpose limitation" means that personal data can only be collected for specific, pre-defined purposes ("purpose specification") and not be used for purposes that are incompatible with the purposes for which the data was originally collected ("compatible use").[4] The WP29 elaborates further on these two elements:

(1) Purpose specification: Personal data must be collected for *specific, explicit, and legitimate* purposes. This means that the purposes of the data collection must be: defined prior to the collection (i.e., companies should be able to predict the data uses); clearly communicated in an intelligible and transparent form; and be legitimate under one of the legal grounds listed in the EU Data Protection Directive.[5] In the online context, the WP29 recommends using layered notices[6] so that users can determine the level of information they would like to obtain. In addition, vague and generic language should be avoided (e.g., data is used "for marketing").

(2) Compatibility test: A compatibility test is necessary to ensure that personal data is not further processed for purposes that are incompatible with the purposes for which the data was originally collected. A simple change of privacy policy would not be sufficient to legitimize a new, incompatible data-processing purpose. In order to assess whether a purpose is compatible or not, companies should conduct a "compatibility test" that takes into account the following criteria:

a. the relationship between the purposes of the processing at the time of data collection and the purposes of further processing;

b. the context of the data processing (e.g., purchase, service subscription) and the reasonable expectations of the individuals regarding further use of data (e.g., email marketing in the context of existing customer relationships);

c. the sensitivity of the data and the impact on individuals' privacy; and

d. the use of mitigating measures, such as adequate security and confidentiality measures ensuring fair processing and limiting the impact on individuals' privacy.

However, a new purpose is not necessarily incompatible. For example, further use of data for historical, statistical, or scientific purposes is generally compatible and would not raise major issues, provided that adequate security is in place (e.g., data minimization, anonymization, privacy-enhancing techniques).

Compatibility Test and Big Data

The WP29 defines "big data" as reuse of "gigantic digital datasets" held by corporations that are extensively analyzed using computer algorithms (i.e., data analytics). It acknowledges the benefits associated with the use of big data for research and innovation, especially in the fields of marketing, mobile communications, smart grid, traffic management, fraud detection, and healthcare. However, the WP29 stresses that big data entails certain privacy risks (e.g., tracking and profiling based on a combination of data from different sources, limited transparency, inaccurate analytics results, highly intrusive personalized advertising, poor data security, and increased risk of government surveillance). Therefore, it recommends conducting a compatibility test when big data is used for the following:

(1) Predicting general trends (emphasis on security): According to the WP29, companies should apply adequate security and confidentiality measures (e.g., anonymization, pseudonymization, aggregation) when they use big data to predict general trends, especially if it involves the sharing of data with third parties. In particular, the WP29 advocates for the "functional separation" of processing activities, meaning, for example, that data used for statistical or other research purposes should not be used for other purposes directly related to individuals.

(2) Analyzing preferences, behaviors, and attitudes to target users (emphasis on opt-in consent): Big data can also be used to analyze or predict preferences, behavior, and attitudes of customers with a view to create personalized discounts or provide special offers and targeted advertisements. In such cases, the WP29 requires *free, specific, informed, and unambiguous opt-in consent* to legitimize the reuse of customer data, in particular when conducting the following activities: tracking and profiling for direct marketing, behavioral advertising, data-brokering, location-based advertising, or tracking-based digital market research. In those circumstances, the WP29 recommends that companies disclose to their customers the decisional criteria and sources of data used for the targeting; implement strong security safeguards; and provide individuals with access to their data in a portable and user-friendly format to allow them to correct or update their profiles.

---

[2] Regarding the applicability of EU data protection law to non-EU-based companies, *see for example* "EU Regulators Issue Opinion on Mobile Apps," March 2013.

[3] The opinion also suggests improvements of "purpose limitation" in the context of the draft EU Data Protection Regulation and analyzes issues related to "open data" (i.e., accessibility of information processed by public bodies).

[4] *See* Art. 6(1)(b) of the EU Data Protection Directive 95/46/EC.

[5] Legal grounds for data processing are, e.g., consent, performance of a contract, or a company's overriding interest.

[6] A layered notice consists of multiple layers with different levels of detail, ranging from high-level information that is easy for customers to understand to more detailed information that includes all the requirements for processing.

Continued on page 5...

European Regulators Opine on "Purpose Limitation" . . . *(continued from page 4)*

Examples of Incompatible Further Use of Data

- Marketing: Opaque racial profiling of customers to provide greater personalized discounts in a specific region (e.g., Asian customers); use of data analytics on a loyalty card to identify when a woman is pregnant and to send targeted marketing offers without providing prior specific information.
- Social media: Oversimplification of the different purposes (e.g., email, social networking, photo and video uploads) without any granularity; modifying the privacy policy with the intention to start using photos already uploaded on the platform for the promotion of the website and subjecting such changes to an "I accept" button without allowing individuals to continue using the website.

Recommendations and Conclusions

Below are a few key takeaways from the WP29's opinion:

- Assess new purposes in light of a compatibility test
- Use granular layered notices
- Break down general purposes into "sub-purposes"
- Avoid generic descriptions such as "marketing," "IT-security," and "further research"
- Avoid using general terms and conditions to justify new data processing to which individuals have not consented

The opinion is probably one of the most important opinions analyzing compliance with EU data protection law, since the purpose limitation principle is one of the core principles of EU data protection. It analyzes a large number of examples with a view to help companies interpreting this principle in light of innovative business trends such as the (re)use of personal data in the context of big data.

Cloud Storage Providers Storing Protected Health Information May Be Obligated to Comply with HIPAA Regulations

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

Wendy Devine
Associate, San Diego
wdevine@wsgr.com

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

A recently issued government rule may unknowingly create significant liability and legal risk for many technology enterprises. The expanded definition of "business associates" and related interpretations by the Department of Health and Human Services (HHS) suggest that many companies should revisit how they provide services and ask whether they are providing their services to health care providers, health plans, or health care clearing houses (collectively, "covered entities"). HHS seeks to implement the mandates of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) by modifying its regulatory scheme (the "HIPAA Rules") that implements the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[1] Two of the most important changes involve "business associates," defined as entities that perform functions or activities on behalf of covered entities or other business associates that involve the use or disclosure of protected health information (PHI). Among many other changes, the omnibus rule:

1. expanded the definition of "business associate" and
2. placed the obligation of HIPAA compliance directly on business associates.

Companies Storing PHI May Be Business Associates

Under the new rule, any entity "that provides data transmission services with respect to protected health information to a covered entity and that requires routine access to such protected health information" is a "business associate."[2] HHS considers entities to be business associates when they persistently store PHI; however, entities that act as mere conduits for the transmission of PHI, possessing the PHI for only a brief period of time to facilitate a data transfer, are likely not business associates. Addressing the question of where to draw the line between a business associate and a conduit, in the guidance accompanying the omnibus rule, HHS states that the determination is "based on the nature of the services provided and the extent to which the entity needs access to protected health information to perform the service for the covered entity." In essence, entities that deal with PHI in a transient manner are not business associates, but all other entities are business associates to the extent that they deal with PHI for covered entities or business associates. Many entities historically took the position that because they neither accessed nor maintained PHI in any knowing way, they were not business associates. Instead, they maintained that

[1] Changes also were made according to the Genetic Information Nondiscrimination Act.
[2] For additional detail, please see our prior WSGR Alert at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert_HIPAA.htm.

Continued on page 6...

their activities were incidental to the provision of their services and they should not be treated as business associates under the statute.

Storage Providers May Be Business Associates Even Without Tangible Access or Use of PHI

The newly released rule may give cause for alarm among many technology companies that provide services to health-related businesses. Many such businesses historically have given little thought to whether or not their customers were covered entities under HIPAA. Or, because they did not have access to any PHI, they believed the HIPAA rules did not apply. Under the omnibus rule, however, whether an entity actually accesses the PHI is irrelevant to HHS's determination of whether an entity is a business associate. Per HHS, "An entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information." Further, HHS specifically calls out data storage companies and explains that they are in fact business associates, regardless of whether they ever actually access the PHI that they store.

The significance of "maintaining" data for many companies cannot be understated. The application of HIPAA regulations to entities that store data should strongly encourage many entities to consider re-evaluating their policies and compliance strategies and review their client bases to evaluate risk exposure and liability under the HIPAA Rule.

Storage Providers May Be Business Associates Even Without a Direct Relationship with a Covered Entity

HITECH also contains, and the HIPAA omnibus rule reflects, a mandate that subcontractors of business associates be directly required to comply with all regulations applicable to business associates. HHS explained that this requirement reflects an effort to "avoid having privacy and security protections for protected health information lapse merely because a function is performed by an entity that is a subcontractor rather than an entity with a direct relationship with a covered entity."

This regulation shift directly affects data storage providers to the extent that they store PHI downstream from a covered entity. Cloud providers that simply transmit PHI likely are not business associates, but once a cloud provider stores the PHI in anything other than a transient manner, according to HHS, it may assume the role of a business associate, even if (1) it never accesses the PHI, and (2) it did not receive the PHI directly from a covered entity. Even cloud providers that store PHI far down the chain of service providers from the covered entity may have HIPAA compliance obligations. Given that many providers often lack any specific knowledge or awareness of the type and nature of client data they may maintain, and often do so specifically for privacy and security reasons, the new rule could easily catch many off guard.

Compliance Risks for Data Storage Providers: Direct Liability and Civil and Criminal Penalties

Prior to HITECH, covered entities were directly responsible for compliance with HIPAA regulations, while business associates were contractually obligated to meet regulation requirements via their business associate agreements with covered entities. While covered entities could face government enforcement actions, the risk to business associates was historically limited to private lawsuits from their customers and indemnity obligations in most cases.

The omnibus rule makes business associates directly responsible for compliance with applicable HIPAA regulations. From a practical standpoint, for entities formerly contractually obligated to comply, this change may have no effect. However, for entities such as cloud storage providers and subcontractors that may have no—or incomplete—preexisting compliance obligations, the impact is significant. Moreover, a considerable amount of the compliance risks are now shifted from the shoulders of the covered entity to the entities that it works with—and every entity downstream from the covered entity. As HHS stated in the omnibus rule guidance, "we believe that making subcontractors directly liable for violations of the applicable provisions of the HIPAA Rules will help to alleviate concern on the part of covered entities that protected health information is not adequately protected when provided to subcontractors."

Direct responsibility for, and liability for lack of, HIPAA compliance is especially significant in light of the considerable monetary and criminal penalty provisions mandated by HITECH. Failure to comply can result in sizable fines and even imprisonment.[3] For example, the minimum fine is $100 per violation, with a calendar-year cap of $25,000 for identical violations, and the maximum fine can be as high as $50,000 per violation, with a $1.5 million calendar-year cap for identical violations. As another example, any person, including an employee of a covered entity or business associate, that commits certain acts knowingly may be fined up to $250,000 and/or imprisoned for up to 10 years.

Notably, while business associates now have direct compliance responsibility, they also retain contractual responsibility and risk. The omnibus rule kept the preexisting requirement that covered entities and business associates execute specific business associate agreements. So, business associates must still provide contractual assurances that they will comply with HIPAA regulations. Further, contractual obligations and risk flow down the relationship chain, as subcontractors also must execute such agreements with business associates. As HHS stated in the omnibus rule guidance, "covered entities must ensure that they obtain satisfactory assurances required by the Rules from their business associates, and business associates must do the same with regard to subcontractors, and so on, no matter how far 'down the chain' the information flows."

Conclusion

In view of these significant changes to HIPAA regulations and HHS's explicit contemplation of data storage providers as business associates, entities that provide such services

[3] For additional detail, please see our prior WSGR Alerts at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert_HIPAA.htm and http://www.wsgr.com/publications/PDFSearch/BNA0511.pdf.

Continued on page 7...

Cloud Storage Providers Storing Protected . . . *(continued from page 6)*

should consider a review of their policies and procedures for privacy and data security. In doing so, evaluation of customer profiles and relationships and performance of risk assessments regarding potential storage of PHI may make sense. A challenge under the new regulations is the risk that data storage providers may unknowingly receive PHI from clients, and thereby may become subject to penalties and enforcement actions. As a consequence, some businesses may seek to bring their security measures into compliance without knowing for certain whether the rules apply or they may evaluate ways to expressly exclude entities possessing PHI from their services in efforts to avoid unnecessary liability.

Clapper v. Amnesty International USA: The U.S. Supreme Court Strengthens Defendants' Shield Against Privacy Class Actions

Tonia Klausner
Partner, New York
tklausner@wsgr.com

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

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

Rachel Landy
Associate, New York
rlandy@wsgr.com

One of the most common and effective defenses raised by privacy class action defendants has been lack of standing. Federal courts have jurisdiction over cases only when the plaintiff has standing to sue. Therefore, courts will dismiss a case when the plaintiff does not meet the requirements for standing. For standing to exist, the plaintiffs' injury must be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[1] In other words, the plaintiff must have suffered some actual harm, or face an imminent risk of suffering a concrete injury. Frequently, class action plaintiffs have been unable to establish standing based on alleged injuries from the unauthorized exposure of personal information. The recent U.S. Supreme Court case of *Clapper v. Amnesty International USA*[2] may have strengthened the standing shield for defendants even more.

Plaintiffs Are Asserting Creative Injuries in Privacy Class Actions

In an effort to establish standing, plaintiffs often assert creative and sometimes theoretical injuries that allegedly resulted from an entity's exposure of information about them. For example, plaintiffs have alleged harm based on the loss of control over or value of the disclosed personal information, fear that data will be used against their interests, embarrassment of the disclosure, the cost of identity-theft protection, and the replacement cost of mobile devices purportedly involved in the data compromise. Federal courts have largely rejected these supposed injuries and dismissed claims asserted following a data-breach incident for lack of standing. However, some courts have allowed the cases to proceed.[3]

Clapper v. Amnesty International USA: Standing Arguments

The U.S. Supreme Court recently analyzed the standing requirement in *Clapper* and may have made the requirement more stringent in practice. In *Clapper*, the plaintiffs argued that a section of the Foreign Intelligence Surveillance Act (FISA) is unconstitutional, because it allows for the government's surveillance of sensitive and privileged conversations between the plaintiffs and individuals located outside the United States. In a 5-4 decision, the Supreme Court declined to reach the constitutional issue because it concluded that the plaintiffs lacked standing. In so holding, the Court rejected the two theories of standing asserted by the plaintiffs:

1. there was "an objectively reasonable likelihood" that their communications would be intercepted pursuant to FISA in the future; and
2. the risk of future surveillance under FISA was so great that the plaintiffs incurred costs to protect against such future surveillance of their international communications.

Speculative Injury Does Not Confer Standing

In considering whether the plaintiffs had standing to challenge the constitutionality of FISA, the Court first rejected the "objectively reasonable likelihood" of future injury standard proposed by the plaintiffs, which had been applied by the Second Circuit. The Court clarified that to find standing based on a threat of future harm, the "threatened injury

---

[1] *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. ___, 130 S.Ct. 2743, 2752 (2010).
[2] *Clapper v. Amnesty Int'l USA*, 568 U.S. _____, 133 S. Ct. 1138 (2013).
[3] *E.g., Krottner v. Starbucks*, 628 F.3d 1139 (9th Cir. 2010) (holding that "generalized anxiety and stress" and increased risk of future identity theft resulting from a laptop theft containing sensitive information conferred standing); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007) (holding that the plaintiffs had standing due to the threat of future harm or an increased threat of future harm after the defendant's website was hacked, even without evidence of any data misuse or "completed direct financial loss"); *Ruiz v. Gap, Inc.*, 622 F.Supp.2d 908 (N.D. Cal. 2009) (holding that the plaintiffs' increased risk of identity theft following the theft of a laptop containing sensitive information conferred standing); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F.Supp.2d 273 (S.D.N.Y. 2008) (relying on *Pisciotta* to hold similarly in the case of a stolen laptop).

Continued on page 8...

must be *certainly impending* to constitute injury in fact." Allegations of possible future injury are inadequate. The Court found that the plaintiffs failed to show any "certainly impending" harm because a series of events involving independent actors would have to occur before the government could intercept any of the plaintiffs' international communications under FISA.

The Court acknowledged in a footnote that at times, it has found standing based on the existence of a "substantial risk" of future injury that reasonably prompts a plaintiff to incur costs to avoid or mitigate that harm. Even under the "substantial risk" test, however, the plaintiffs in *Clapper* did not have standing due to the attenuated chain of inferences necessary before any possible future injury. As the Court explained, "We decline to abandon our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors."[4]

Self-Imposed Costs Do Not Confer Standing Where the Future Harm Is Not Certainly Impending

The Court also rejected the plaintiffs' theory that the costs of their preventative actions constitute present economic injury that confers standing. The *Clapper* plaintiffs asserted that they took costly measures to protect the confidentiality of communications and prevent government surveillance. These measures, the plaintiffs argued, constituted an injury that met standing requirements.

The Supreme Court rejected the argument and stated that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[5] Otherwise, the Court concluded, an enterprising plaintiff would be able to secure a lower standard for standing by simply making expenditures "based on a nonparanoid fear" of speculative future harm.

Implications

The Supreme Court's holding in *Clapper* that speculative future injuries and present economic expenditures based on such speculative harm are insufficient to confer standing will likely provide a valuable strengthened shield for privacy-related class action defendants.[6]

The alleged harm from data breaches typically involves a future harm with several links in a chain of inferences involving independent actors. For example, in cases where a hacker has accessed encrypted credit card numbers on a company's servers, the company could argue that a long series of events would need to occur before an actual and concrete injury was "certainly impending." Such plaintiffs would need to show:

- the hacker actually acquired the data;
- the hacker successfully decrypted the data;
- the hacker was targeting that specific type of data (e.g., the data related to the plaintiff was not obtained ancillary to an effort to obtain intellectual property, classified information, or some other payload);
- the plaintiffs' credit card account was not closed by the credit card company; and
- any fraudulent purchases on the credit card would not be reimbursed by the credit card company.

Moreover, *Clapper* supports the conclusion that federal courts have generally reached, which is that the cost of identity-theft protection taken preemptively by the plaintiffs does not constitute an injury that confers standing. Plaintiffs commonly assert that they have subscribed to identity-theft protection services after learning that information about them has been compromised and claim that the cost of such service is the injury. If the chain of events that would have to occur before the plaintiff would suffer harm is too attenuated, the plaintiff's self-imposed costs are insufficient to establish standing under *Clapper*. The Supreme Court made clear that plaintiffs cannot obtain standing by purchasing protections based on fears of speculative future harm, which may describe preemptively subscribing to identity-theft services based on a fear of identity theft.

In summary, *Clapper* will likely provide defendants with a stronger shield in privacy class action litigation. Defendants may prompt dismissal of a case by arguing that the alleged injury to the plaintiffs relies on a series of speculative events involving independent actors that is insufficient to support standing. In cases where plaintiffs allege that the costs of identity-theft protection services or other precautionary measures are the injury conferring standing, defendants can respond that plaintiffs may not self-impose costs in response to speculative future harm to obtain standing.

---

[4] *Id.* at 1150.
[5] *Id.* at 1151.
[6] Sony has made this argument in its privacy class action litigation. The motion is pending before the court at the time of this writing. *In re: Sony Gaming Networks and Customer Data Security Breach Litigation,* No. 11-md-2258 AJB (MDD) (S.D. Cal.).

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