Volume 5, Issue 4, July 2014

SOCIALLY AWARE

THE SOCIAL MEDIA LAW UPDATE

THE BURTON AWARDS
2011 BEST LAW FIRM NEWSLETTER

IN THIS ISSUE

EDITORS

John F. Delaney
Gabriel E. Meister
Aaron P. Rubin

CONTRIBUTORS

Patrick Bernhardt
Delphine Charlot
Adam Fleisher
Reed Freeman
Libby Greismann
Susan McLean
Julie O'Neill
Karin Retzer
Miriam Wugmeister

FOLLOW US

Morrison & Foerster's Socially Aware Blog

@MoFoSocMedia

MORRISON FOERSTER

Welcome to a special privacy issue of *Socially Aware*, focusing on recent privacy law developments relating to social media and the Internet. In this issue, we analyze a controversial European ruling that strengthens the right to be forgotten; we examine a recent California Attorney General report regarding best practices for compliance with the updated California Online Privacy Protection Act; we summarize the FTC's recent settlement with Snapchat and its broader implications for mobile app developers; we report on a case filed by a French consumer association accusing three major social networking sites of using confusing and unlawful online privacy policies and terms of use; and we highlight the growing popularity of anonymous social apps and the security risks that they pose.

All this—plus a collection of thought-provoking statistics about online privacy . . .

EUROPEAN COURT OF JUSTICE STRENGTHENS THE RIGHT TO BE FORGOTTEN

By Karin Retzer, Miriam Wugmeister and Delphine Charlot

In a groundbreaking decision against Google, the European Court of Justice (ECJ)—the EU's highest court—has embraced the "right to be forgotten," creating significant implications for global companies.

On May 13, 2014, the ECJ issued a ruling that did not follow the rationale or the conclusions of its Advocate General, but instead sided with the Spanish data protection authority (DPA) and held that:

- Individuals have a right to request that Google not allow legitimately published website content to be searchable by name if the personal information contained in such content is inadequate, irrelevant or no longer relevant;
- Google's search function resulted in Google acting as a data controller within the meaning of the Data Protection Directive 95/46, despite the fact that Google did not control the data appearing on web pages of third-party publishers; and
- Spanish law applied because Google Inc. processed data that was closely related to Google Spain's selling of advertising space, even where Google Spain did not process any of the data (noting, despite earlier decisions to the contrary, that the services were targeted at the Spanish market and such broad application was required for the effectiveness of the Directive).

The ruling will have significant implications for search engines, social media operators and businesses with operations in Europe generally.

While the controversial "right to be forgotten" is strengthened, the decision may open the floodgates for people living in the 28 countries in the EU to demand that Google and other search engine operators remove links from search results. The problem is that the ECJ decision permits individuals to request removal of a broad range of data. The decision encompasses not only incorrect or unlawful data, but also data that is "inadequate, irrelevant, or no longer relevant," as well as data that is "excessive or not kept up to date" in relation to the purposes for which it was processed. It is left to the companies to decide when data falls into these categories.

While the controversial "right to be forgotten" is strengthened, the decision may open the floodgates for people living in the 28 countries in the EU to demand that Google and other search engine operators remove links from search results.

In that context, the ruling will likely create new costs for companies and possibly tens of thousands of individual complaints. What is more, companies operating search engines for users in the EU will have the difficult task of assessing each complaint they process and whether the rights of the individuals prevail over the rights of the public. Internet search engines with operations in the EU will have to handle requests from individuals who want the deletion of search results that link to pages containing their personal data.

That said, the scope of the ruling is limited to name searches. While search engines will have to deactivate the name search, the data can still be available in relation to other keyword searches. In an effort to maintain the freedom of expression (and more particularly, press freedom), the ECJ did not impose new requirements relating to the content of web pages. But the decision will still result in a great deal of legally published information being available only to a limited audience.

Below we set out the facts of the case and the most significant implications of the decision, and address its possible consequences on companies operating search engines.

FACTS OF THE CASE

In 2010, a Spanish national lodged a complaint before the Spanish DPA against the publisher of a daily newspaper with a wide audience in Spain, *La Vanguardia*, and against Google Spain and Google Inc. for their refusal to remove web links to the newspaper. The web pages contained the claimant's personal details in an announcement concerning an auction of real estate connected with a procedure prompted by Social Security debts.

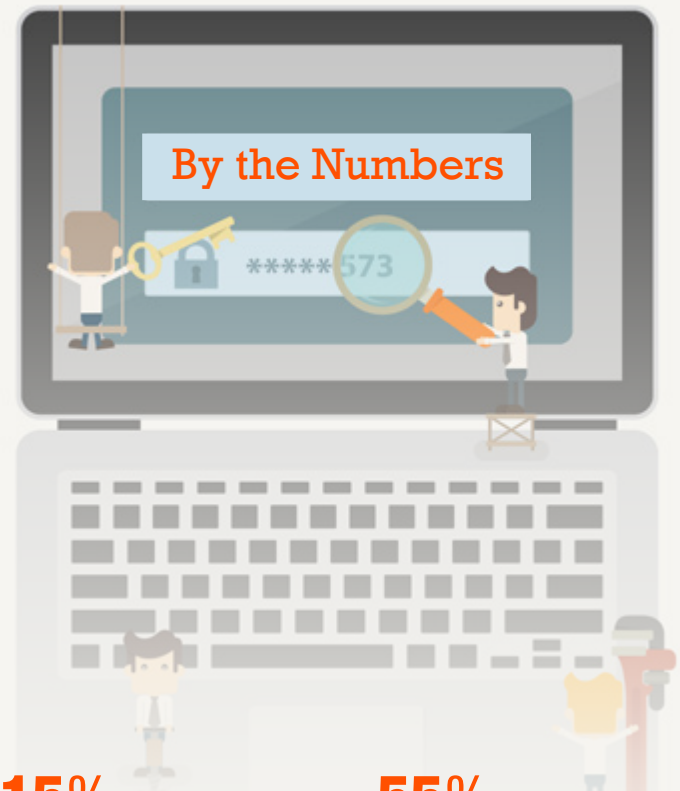
The Spanish DPA did not require the newspaper to take down the pages, but ordered Google Spain and Google Inc. to remove the data from their search results and to render future access to them impossible. Google appealed to the Spanish National High Court, seeking an annulment of the DPA decision.

QUESTIONS REFERRED TO THE COURT

The Spanish National High Court referred the following questions to the ECJ for a preliminary ruling:

- Is Google a data controller with respect to its search engine activity?
- Does the Directive apply even though Google Spain does not carry out any activity related to the search engine?

ONLINE PRIVACY



15% of U.S. adults have taken no steps to protect their privacy online.[1]

25% of millennials are willing to share personal information in return for more relevant ads (versus 19% of people 35 and over).[2]

25% of Facebook users don't bother with any kind of privacy control.[3]

45% of U.S. adults feel that they have little or no control over the collection of their personal information while using the Internet.[1]

55% of Internet users have taken steps to avoid observation by specific people or organizations or by the government.[4]

59% of Internet users do not believe it possible to be completely anonymous online.[4]

68% of Internet users believe current laws are insufficient to protect people's privacy online.[4]

86% of Internet users have taken steps online to remove their digital footprints.[4]

SOURCES

1. http://ipsos-na.com/news-polls/pressrelease.aspx?id=5972
2. http://annenberg.usc.edu/News%20and%20Events/News/130422CDF_Millennials.aspx
3. http://www.go-globe.com/blog/social-media-facts/
4. http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/

- Can individuals require the erasure of their personal data by Google in a search engine, regardless of whether third-party content is legitimate?

The ECJ is the highest court that decides on the interpretation and application of EU law. Decisions of the ECJ are legally binding on the courts in all EU countries that apply EU law. When a case is referred for a preliminary ruling, the answers of the ECJ must be applied by national courts, which then issue their own ruling on the specific facts of a case. There is no appeal following a preliminary ruling.

In this specific case, the case will go back to the Spanish National High Court, which will have to decide on the specific facts while taking into account the principles highlighted by the ECJ.

OPINION OF THE ADVOCATE GENERAL

On June 25, 2013, the Advocate General at the ECJ, Niilo Jääskinen, issued an Opinion recommending that Google should not be required to remove links to legitimate third-party content based on data protection principles. In his Opinion, Jääskinen emphasized the importance of freedom of speech and the preservation of historic newspaper reports.

The Advocate General agreed that sales offices in EU countries suffice to trigger the application of that country's data protection law. In his view, the processing of personal data takes place within the context of an "'establishment" if that establishment is linked to a service selling targeted advertising in the Member State, even if the technical data processing operations are situated in third countries.

However, the Advocate General stated that Google cannot be considered the data controller of data available on third-party websites as it does not control the content of these sites. Also, he made it clear that in his opinion, there was no such thing as a general "right to be forgotten" under the current Data Protection Directive.

The ECJ ultimately took a very different view. It is unusual that the ECJ disagreed with the opinion of an Advocate General as it did here.

GOOGLE IS A DATA CONTROLLER

In its decision, the ECJ explained that Google's search engine activity consists of retrieving, recording and organizing personal data which it stores on its servers and, as the case may be, discloses to its users in the form of lists of results. In the ECJ's view, this indexing activity is a processing of personal data, regardless of the fact that the search engine does not distinguish between personal data and other types of data.

The ECJ further regarded Google as a data controller in relation to the processing of the data by the search engine. According to the ECJ, Google determines the purposes and means of data processing and its activity is "liable to significantly affect" individuals' fundamental rights to privacy. The ECJ highlighted that the definition of a data controller in the Directive is broad.

This conclusion is surprising as it means that Google is the data controller of search results even though it cannot control the web pages from which the data are pulled. In fact, third-party publishers are the data controllers when it comes to the content of the web pages. This fact however, was not relevant to the ECJ and the finding may have broader implications regarding the definition of a data controller in other contexts.

APPLICATION OF EU DATA PROTECTION LAW WHERE PROCESSING RELATES TO ACTIVITIES OF LOCAL SALES AGENTS

The ECJ held that the Google's search engine is subject to EU data protection laws even if Google Spain does not carry out any activity directly linked to the indexing or storing data.

In fact, the ECJ said that a broad interpretation of the territorial scope of EU laws was required to ensure the effectiveness of Art. 4.1(a) of the Directive, which states that local EU data protection law applies where "the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable."

The ECJ determined Google Spain constitutes a stable establishment of Google Inc. within the meaning of the Directive, and Google Inc.'s processing is closely related to Google Spain's activity because it is intended to promote and sell advertising space in Spain in order to make the service offered by the engine more profitable. In doing so, the Court considered whether Spanish users were targeted for marketing and for advertising, a consideration provided in the draft EU Regulation and discussed in literature, but not currently provided in the Directive. Thus, this finding is new and quite unexpected.

The ECJ ruling follows the same line as its General Advocate and a common position in the Member States with respect to the meaning of an "establishment." It defined "establishment" not just in terms of control over personal data, but also in the economic function of the EU subsidiaries of the foreign companies. The interpretation of "establishment" has been continuously broadened by the EU DPAs. This may, in the end, be the finding that has the broadest implications for companies. Essentially, if an EU subsidiary is intertwined with the goals and purposes of a foreign parent company and if the service is aimed at the local EU Member State market, EU law may be found to apply to the non-EU entity.

RECOGNITION OF THE MUCH-DEBATED "RIGHT TO BE FORGOTTEN"

According to the ECJ opinion, a website operator should remove links to web pages that are published by third parties each time the inclusion of the link is or has become incompatible with the Directive. Opposing the Advocate General's reasoning, the ECJ stated that a link is incompatible with the Directive not only when the data are false or unlawful (which is the current position in many Member States), but also when the data are inadequate, irrelevant or no longer relevant, or where the data are excessive or not kept up to date in relation to the purposes for which they were processed. This is a significant expansion of the definition of the correction rights as currently implemented and interpreted in many Member States.

The ECJ did make an exception for individuals who are public figures or where the public interest in the information would outweigh the privacy rights of the individuals.

In the specific case at hand, the ECJ found that the web pages contained true information that had been lawfully published, but they stated, "having regard to the sensitivity of the information contained on the web page, and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that that information should no longer be linked to his name." Thus, the ECJ found that even where the data are lawfully published and the underlying website will not be altered, the individual still has the right to request that the "aggregator" of such information remove the data. The ECJ, however, did not impose a specific requirement as to how much time must pass for a request to be considered valid, leaving that question to search engine operators, data protection authorities and national courts to answer on a case-by-case basis.

As a result, although the information was legitimately published, and may remain available off-line and on the Internet, the information should no longer be searchable via the name of the individual. That said, it would still be permissible for the search engine platform to allow the information to be searchable by date, location or any other keyword.

A NEW SOURCE OF CONTENTIONS BEFORE THE DPAS

The ECJ justified the new constraint it imposes on technology companies by the "seriousness of the interference in the private life of the individuals" that may be caused by a name search. In fact, any Internet user, when he or she searches an individual's name, may obtain a structured overview of the information relating to that individual, the ECJ said. This information potentially concerns a vast number of aspects of an individual's private life which, without the search engine, could not have been interconnected.

What this likely means in practice is that an individual may make a request to a company to have the links based on name be removed. If the company does not agree, then the individual will have the right to go to the Data Protection Authority or the local courts to try to force the company to remove the links. This will thus create quite a bit of additional work for the DPAs and the courts.

A DIFFICULT BALANCE TO STRIKE BETWEEN THE INTERESTS OF THE INDIVIDUALS AND THOSE OF THE INTERNET COMMUNITY

The ECJ ruling creates a new requirement that search engine operators and other aggregators of information must seek a fair balance between the interests of the individuals and those of the public. The ECJ stated that the following factors need to be taken into account by the search engine provider in deciding whether to make information available via name search: the balance will depend on (i) the nature of the information, (ii) the sensitivity of the information for the individual's private life and (iii) the interests of the general public in having that information. Such interest may vary according to the role played by each individual in public life. Again, it is for the companies to assess in which case such role may justify the indexing of the data. This will likely be a costly and uncomfortable position for many companies.

PRESS FREEDOM AND FREE SPEECH PRESERVED BUT POTENTIALLY LIMITED

The ECJ affirmed that publishers of websites are still allowed to publish contested personal data for journalistic purposes. These rights do not, however, extend to search engines. Therefore, while an individual may require the erasure of his or her data by a search engine's operator, the content of the web page would be left unchanged.

However, the decision is likely to affect the activity of journalists and, more generally, freedom of expression. The removal of contested links will lower the number of times a web page is visited, thus adversely affecting freedom of expression. The ECJ did not uphold the Advocate General's opinion that the erasure of legitimate and legal information would amount to a form of "censorship" by a private party.

CURRENT STATE OF PLAY AT EU LEVEL

The introduction of a right to be forgotten has been proposed by the EU commission in the proposed General Data Protection Regulation. In a first reading of March 2014, the Parliament adopted a new article 6, which set out that any data that is inaccurate, incomplete or no longer up to date should not be disclosed. The proposed Regulation also sets out that the right to erase incorrect data extends to third parties. However, the Parliament did not retain the Rapporteur's proposition for a reference to clear time limits.

For the proposed Regulation to become law, the Council must agree on a common position with the Parliament. It is not certain that these developments will be upheld by the Council, which has stated that it wants to remove administrative burdens from companies. While Parliament has expressed the need to adopt a reform by the end of the year, the Council has not yet formed official positions or started official negotiations to reach a common position. In view of the coming European elections and the appointment of a new Commission, solid legislative work may not restart until next year.

In this context, it is still unclear whether the ECJ's ruling at hand will be integrated in the new Regulation. What is sure is that the decision will be debated at the EU level, whereas it already has implications in the jurisdictions of the 28 Member States.

IMPLICATIONS

In addition to putting data protection authorities in a rather uncomfortable position of deciding on the question of what legitimate content should be easily searchable and accessible, this decision will have wide-ranging ramifications for organizations, not just for search engine providers.

First, there is a very broad interpretation of the jurisdictional reach of EU Member State law to cover organizations outside the EU whenever users in the EU are targeted.

Second, search engine providers, social media companies and other content providers may have obligations to comply with the data protection laws even where these providers are not involved in making decisions about the online content provided.

Third, the way in which organizations search for data will likely change due to the fact that certain information will now no longer be available by name.

CALIFORNIA AG OFFERS BEST PRACTICES FOR DO NOT TRACK DISCLOSURES; CRUCIAL COMPLIANCE QUESTIONS LEFT UNANSWERED

By Reed Freeman, Julie O'Neill and Patrick Bernhardt

California Attorney General Kamala Harris released a long-awaited report entitled *Making Your Privacy Practices Public* (Report) on May 21, 2014. The Report recommends "best practices" for compliance with the California Online Privacy Protection Act (CalOPPA).

It was originally intended to answer critical questions about exactly what website, online service, and mobile application operators (collectively, "site operators") must do to comply with CalOPPA's new do not track (DNT) disclosure obligations, which took effect on January 1, 2014. It does not accomplish that goal. Unfortunately, the Report leaves important questions unanswered *and* raises new questions.

The Report explains that "its recommendations . . . which in some places offer greater privacy protection than required by existing law, are not regulations, mandates or legal opinions." It fails, however, to clarify what the law actually requires, and we expect that trade associations will continue to seek guidance on important compliance issues. In the meantime, site operators may wish to comply with at least some of the Report's recommendations to the extent possible because such "recommendations" tend to harden into regulatory "expectations" over time.

DISCLOSURE OF CROSS-SITE TRACKING AND RESPONSES TO DNT CHOICE MECHANISMS

In order to assess the Report's recommendations, it is important to first understand CalOPPA's DNT disclosure obligations. As amended by AB 370, the law requires a site operator to make disclosures with respect to:

1. Its collection of personally identifiable information (PII) about its users' activities over time and across third-party sites or online services, if it engages in such cross-site tracking. (We note that the California Attorney General appears to broadly define PII to include not only names, physical addresses, email addresses, phone numbers and social security numbers, but also device identifiers and geo-location data.)
2. Any "other party's" tracking of the site operator's users over time and across third-party sites or services.

The law applies to cross-site tracking for any purpose, including, for example, analytics and advertising.

We discuss each of these obligations, as well as questions that the Report raises with respect to them, in turn as follows.

A. Disclosures relating to a site operator's own cross-site tracking

The law requires that a site operator disclose *how* it responds to browser DNT signals or other tracking choice mechanisms, *if* it engages in cross-site tracking. As the Report notes, "[t]he new provisions do not . . . depend on a standard for how an operator *should* respond to a DNT browser signal or to any mechanism that automatically communicates a consumer's choice not to be tracked." The law requires only disclosure, not substantive practices, and it can be breached by a failure to disclose, or to disclose accurately, the required information.

When it comes to compliance with California's new "do not track" disclosure requirements, the Report raises more questions than it answers.

What does this mean in practice and in light of the Report? And what questions does the Report raise?

- If a site operator engages in cross-site tracking, it must disclose how it responds to either browser DNT signals or another tracking choice mechanism.
    - *If a site operator engages in cross-site tracking and honors DNT signals*, it should explain *precisely* what it does in response to a DNT:1 header. Note that it may be a mistake to represent simply that a site operator "honors" DNT signals, as that representation could be interpreted to mean more than the operator's actions warrant. For example, there is not yet consensus among stakeholders across the spectrum of industry, academics and advocates on whether honoring an opt-out means that the site operator ceases the online tracking or merely ceases using the information collected through such tracking.
    - *If a site operator engages in cross-site tracking and honors some other means for users to express choice with respect to the tracking*, it should say so. The law permits a site operator to satisfy the DNT disclosure requirement by "providing a clear and conspicuous hyperlink in the operator's privacy policy to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice." The Report makes it clear that a site operator may disclose *either* how it responds to a browser's DNT signal *or* a link to another program or protocol that provides choice. The Report notes, however, that "[d]escribing your response in your privacy policy statement is preferable to simply providing a link to a related 'program or protocol' . . . because it provides greater transparency to consumers." It also recommends that site operators "[p]rovide the link *in addition to identifying the program with a brief, general description of what it does*." While following these recommendations would promote transparency, both go beyond the law's requirement of providing a link.

The Report further recommends that a site operator consider whether "*the page to which you link* contain[s] a clear statement about the program's effects on the consumer . . . [and] what a consumer must do to exercise the choice offered by the program."

This begs a couple of questions about linking to third-party choice programs:

1. **Must the link bring users directly to the program's opt-out page, or is a link to the program's website sufficient?** The Report does not make this clear and, again, may go beyond the law, which requires only a link to "an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice."
2. **The Report is silent as to which, if any, external choice programs are adequate.** In our judgment, industry self-regulatory programs such as those run by the Digital Advertising Alliance (DAA) and Network Advertising Initiative (NAI) should meet the law's requirements. But this is unsettled, and the AG has expressed concerns about whether either program meets the definition. We expect the NAI and DAA will seek further clarification on this point.
    - *If a site operator engages in cross-site tracking but does not honor browser DNT signals or any other choice mechanism*, it should say that it does not honor browser DNT signals. With respect to such site operators, the Report recommends that "[i]f you do continue to collect personally identifiable information about consumers with a DNT signal as they move across other sites or services, *describe your uses of the information*." While such a disclosure may be prudent—as a failure to make it could conceivably be deemed a material omission and thus deceptive under Federal Trade Commission law where such use may be unexpected by an ordinary user under the circumstances—the disclosure is not required by CalOPPA.
    - *If a site operator does not engage in cross-site tracking, no disclosure obligation is triggered.*

B. Disclosures relating to another party's cross-site tracking

CalOPPA requires that a site operator disclose "*whether* other parties may collect personally identifiable information about an individual consumer's online activities over time and across different Web sites when a consumer uses the operator's Web site or service." The law does not require the operator to make any disclosure regarding such "other party's" response to a DNT mechanism.

What does this mean in practice and in light of the Report? And what questions does the Report raise?

- **Is a service provider an "other party"?** Because neither the law nor the Report clarify the meaning of the term "other party," it is not completely clear whether it includes a site operator's service provider or whether, on the other hand, a service provider stands in the site operator's shoes for purposes of the law. During a December 10, 2013 call with industry representatives, consumer advocates, and other interested parties, a representative of the AG's office suggested that a service provider is not the same as a site operator but instead should be treated as an "other party" for purposes of the law. This position is consistent with the law's definition of an "operator," which appears to exclude service providers. In our judgment, it follows that a site operator *does not* have to disclose a DNT response or choice mechanism with respect to the cross-site tracking activities of its service providers, but it *does* have to disclose whether any service provider or other third party is engaged in the cross-site tracking of the site operator's users. As a practical matter, this distinction may be of no consequence: a site operator that uses a service provider for cross-site tracking (e.g., for analytics or behavioral advertising services) is typically contractually required by the service provider to both disclose the tracking and tell its users how they can opt out of it, such as through the DAA or NAI.
- **The Report recommends that a site operator explain how a third party's practices may diverge from the site operator's DNT policy.** This recommendation goes beyond the law's requirements. As discussed above, the law requires only that a site operator disclose *whether* third parties engage in cross-site tracking. It does not impose any requirement to address the third party's response to DNT signals or other choice mechanisms. The recommendation, however, raises the question of whether the AG believes there is a duty under the law for a site operator to vet the practices of third-party trackers on its site and to disclose whether such practices diverge from the site operator's own.

OPPORTUNITY TO CURE?

The Report acknowledges that CalOPPA includes a 30-day notice and cure period for non-compliance, but it does not squarely address whether that 30-day period applies to companies that have posted a privacy policy that fails to include required DNT disclosures but otherwise complies with the law. In a December 2013 call with interested stakeholders, a representative of the AG's office stated that the 30-day period *does not apply* in this situation, and this interpretation seems to be supported in the Report, which notes that "[t]he law provides an operator with a 30-day period *to post a policy after being notified of failure to do so. An operator subject to the law is in violation for failing to comply with the legal requirements for the policy* or with the provisions of its policy either knowingly and willfully or negligently and materially." The AG's apparent

interpretation is that the notice and cure provision applies only if there is *no policy whatsoever*, but that if there is any policy—even one that is almost completely compliant—then no notice and cure period is required. As a matter of public policy, this position makes no sense: the operator who did nothing should not be entitled to greater protection than the operator who tried hard and just missed the mark.

ONLINE TRANSPARENCY "BEST PRACTICES"

Finally, the Report recommends other "best practices" aimed at ensuring that a site operator's privacy policy is transparent to its users. While many of these go beyond the law's requirements, it is worthwhile to consider them, as "best practices" tend over time to harden into regulatory expectations. They include the recommendations to:

- Prominently label the section of your policy regarding online tracking. For example: "California Do Not Track Disclosures."
- Disclose whether third parties collect PII from your users.
- Explain your uses of PII beyond what is necessary for fulfilling a customer transaction or for the basic functionality of the website or app.
- Describe what PII you collect from users, how you use it, and how long you retain it.
- Describe the choices a consumer has regarding the collection, use, and sharing of his or her PII.
- Use plain, straightforward language that avoids legal jargon, and use a format—such as a layered approach—that makes the policy readable. Use graphics or icons instead of text.

CONCLUSION

When it comes to compliance with the new CalOPPA DNT disclosure requirements, the Report raises more questions than it answers. It acknowledges that its recommendations are not necessarily legal requirements, but, in so doing, fails to clarify what the law itself requires. In light of this uncertainty, a site operator may wish to implement the Report's recommendations to the extent possible.

SNAP JUDGMENT: FTC ALLEGES SNAPCHAT DID NOT KEEP ITS PRIVACY AND SECURITY PROMISES, BUT SUGGESTS BROAD NEW DUTY IN THE PROCESS

By Reed Freeman, Libby Greismann and Adam Fleisher

Snapchat's recent settlement with the Federal Trade Commission (FTC) generally provides a comprehensive but not groundbreaking roadmap to the FTC's privacy and data security expectations in the mobile environment under Section 5 of the FTC Act, with two very notable exceptions:

1. It now appears that companies are required to follow researchers' blogs and other writings to see if there are any privacy or data security vulnerabilities, and to act on any such information promptly; and

2. It also appears that the FTC expects companies to be aware of all third parties who have technology that can interact with an app, and to make sure that when consumers engage in any such interaction, all of the company's privacy and data security representations remain true. If the FTC continues down this path, it will create unsustainable new burdens on app developers, many of which have very few resources to begin with. Furthermore, if this is the new standard, there is no reason it should be limited to the app environment—analytically, this would lead to a rule of general application.

THE BASIC ALLEGED MISREPRESENTATION

The Snapchat app became very popular because of its branding as an "ephemeral" mobile messaging service. Among other things, the app promised its users and prominently represented—in its privacy policy and an FAQ, among other places—that the "snaps" (e.g., messages) users sent would "disappea[r] forever" after ten seconds (or less). However, according to the FTC's complaint, in addition to other problems with the app's privacy and security features, it was much too easy to capture these supposedly ephemeral messages, making the company's claims false and misleading in violation of Section 5. And since the company's representations were not consistent with the app's practices, now it's the FTC that won't be disappearing any time soon.

In addition, Snapchat drew the attention of the Maryland Attorney General (AG), who announced a settlement with the company in June. The basis of this settlement is similar to the FTC settlement: Snapchat misled consumers by representing that snaps are temporary. However, the AG also evidently alleged that Snapchat failed to comply with the Children's Online Privacy Protection Act because it knowingly collected personal information from users under the age of thirteen without verifiable parental consent. All that said, the biggest difference between the two matters is $100,000—the amount that Snapchat is required to pay to the State of Maryland under the settlement (the FTC does not have civil penalty authority in Section 5 enforcement actions).

A NEW DUTY TO DISCOVER POSSIBLE VULNERABILITIES

Given the app's popularity, along with its unqualified claims ("snaps disappear . . ."), maybe it shouldn't be surprising that creative users and other opportunistic individuals found ways to preserve these supposedly fleeting messages. As the FTC complaint put it, "several methods exist by which a recipient can use tools outside of the application to view and save snaps indefinitely." The FTC noted in particular "widely publicized" methods for saving video files sent through Snapchat and for using smartphones' "screenshot" functionality to capture a snap. With regard to the screenshot work-around, Snapchat also represented that the app would "let you [the sender] know if [recipients] take a screenshot." But this representation was allegedly misleading because of the well-known means for circumventing the app's alert mechanism.

But the FTC also seems to have collapsed a subtly different type of problem with the app into the discussion of these allegedly "widely publicized," albeit ad hoc, means to preserve supposedly ephemeral snaps. As the complaint (and press release) put it, a "security researcher" warned the company in 2012 that the way its application programming interface (API) functioned made it possible for third-party apps to download and save photo and video messages sent through the Snapchat service, since the deletion function was wholly dependent on the Snapchat application itself.

The fact that this "warning" to Snapchat—note that the complaint does *not* say *if* or *how* Snapchat *actually received or learned about this warning, if at all*, or that the warning was "widely publicized"—evidently should have been sufficient to put the company on notice that its app had a vulnerability suggests that the FTC may be trying to create a very broad "duty to discover" potential privacy or security vulnerabilities. It's one thing for this type of flaw to lead to a misrepresentation based on the ephemeral nature of the snaps (since Section 5 is a strict liability statute, and Snapchat's representations allegedly were facially misleading), but it's quite unprecedented for the FTC to suggest a duty to be aware of (and therefore respond to) the warnings of "security researcher[s]," especially if those warnings are not "widely publicized."

> As more app developers offer consumers privacy options, they need to be certain that they can live up to the promises they make—for every user, every time, under all conditions and use cases.

There is, of course, no guidance in the Snapchat settlement about *which* researchers companies are supposed to pay attention to, or which warnings they must quickly heed. Evidently, the FTC thinks that Section 5 requires app developers to proactively monitor the online community for possible security vulnerabilities. There is no analytical reason to limit this new expectation to app developers. As a result, the FTC risks creating considerable compliance costs for all kinds of companies, and not just mobile app companies.

ADDITIONAL SECTION 5 VIOLATIONS—A CHECKLIST FOR MOBILE APP COMPLIANCE

Geolocation. The complaint also alleges that the company deceived users about the amount of personal data it collected, and about the security measures in place to protect that data. Until February 2013, Snapchat's privacy policy claimed that the app did not ask for, track, or access any location-specific information from users' devices at any time. However, according to the FTC, Snapchat integrated a third-party analytics tracking service in October 2012 that collected users' WiFi-based and cell-based location information from the app.

Accessing contacts. The privacy policy further claimed that the app only collected users' email, phone number, and Facebook ID for its "Find Friends" feature, which is a way to find other users of the app. But Snapchat collected the names and phone numbers of all contacts in the users' mobile device address book who utilized the Find Friends feature. (The Maryland settlement also addressed the collection of contact information without affirmative consent.)

Reasonable security. The last count of the complaint alleges that the company failed to secure the Find Friends feature, both by failing to verify that the phone number that a user entered did, in fact, belong to the mobile device being used by that individual, and by failing to implement restrictions on the number of Find Friend requests that any one account could make. Hackers were allegedly able to exploit flaws in the app's security to access 4.6 million Snapchat usernames and phone numbers. In light of these vulnerabilities, the FTC alleged that the company's representations about how it secures users' data (e.g., "Snapchat takes reasonable steps to help protect your personal information") were false and misleading as well.

Privacy by design. As the FTC has made clear, developers must implement privacy-by-design by building privacy and security into an app's structure from the outset. A privacy-by-design program should address privacy risks, protect the privacy and confidentiality of personal information, and provide policies and procedures sufficient to cover the nature and scope of the app and the sensitivity of the information collected.

The FTC's allegations in the Snapchat complaint epitomize the FTC's ongoing and broadening efforts to ensure that companies market their apps truthfully

and protect user information. For an app to be in compliance with Section 5, it is clear that: (1) consumer controls must work for every consumer, every time, under all conditions and use cases, *even ones that the developer is unaware of*; (2) collection of information from users' address books requires clear disclosure and an opt-out preference; and (3) representations about "reasonable" security create specific legal obligations to protect user data, just as representations about privacy create legal obligations to use information in a manner consistent with those representations.

But given the way that the Snapchat app interacted with third-party apps, and the FTC's allegations relating to those interactions, the Snapchat settlement also suggests that: (1) app developers need to pay attention to privacy and data-security bloggers, and promptly remedy bugs found by these third parties; and (2) representations about which data is or is not collected by an app must extend to third-party tools that can use information generated by the users of that app.

CONCLUSION

Though in many ways the FTC's complaint and consent order are similar to those the FTC has issued recently, the settlement is significant because of its breadth.

The Snapchat app itself illustrates current expectations of consumer controls, as well as the notion of privacy as a marketable concept in its own right. The app's popularity was driven by the idea of privacy itself as a desirable commodity. But, according to the FTC, the app couldn't deliver on its unqualified promises, and that made it a fairly easy target for the FTC.

As more app developers offer consumers privacy options, they need to be certain that they can live up to the promises they make, for every user, every time, under all conditions and use cases; follow researchers' "warnings"; and understand all use cases continuously, because the FTC's interest in mobile applications is not ephemeral.

FRENCH CONSUMER ASSOCIATION TAKES ON INTERNET GIANTS

By Delphine Charlot and Karin Retzer

Earlier this year, the French consumer association UFC-Que Choisir initiated proceedings before the Paris District Court against Google Inc., Facebook Inc. and Twitter Inc., accusing these companies of using confusing and unlawful online privacy policies and terms of use agreements in the French versions of their social media platforms. In particular, the consumer association argued that these online policies and agreements provide the companies with too much leeway to collect and share user data.

In a press release published (in French) on its website, UFC-Que Choisir explains that the three Internet companies ignored a letter that the group had delivered to them in June 2013, containing recommendations on how to modify their online policies and agreements. The group sought to press the companies to modify their practices as part of a consumer campaign entitled "Je garde la main sur mes données" (or, in English, "I keep my hand on my data").

According to the press release, the companies' refusal to address UFC-Que Choisir's concerns prompted it to initiate court proceedings. The group has requested that the court suppress or modify a "myriad of contentious clauses," and alleged that one company had included 180 such "contentious clauses" in its user agreement.

The group has also invited French consumers to sign a petition calling for rapid adoption of the EU Data Protection Reform that will replace the current Directive on data protection with a Regulation with direct effects on the 28 EU Member States. UFC-Que Choisir published two possibly NSFW videos depicting a man and a woman being stripped bare while posting to their Google Plus, Facebook and Twitter accounts. A message associated with each video states: "Sur les réseaux sociaux, vous êtes vite à poil" (or, in English, "On social networks, you will be quickly stripped bare").

The campaign is obviously aimed at catching the attention of the French public, and its timing is not coincidental. In April 2013, the French data protection authority (DPA) started coordinating a joint action among France, Germany, Italy, the Netherlands, Spain and the United Kingdom to investigate and launch penalty proceedings against Google's new privacy policy. That policy, issued in March 2012, permitted the company to merge data from different Google services and to use that data across different platforms. So far, the French, Spanish and Italian DPAs have issued record fines and the Dutch DPA has condemned the policy.

The DPAs observed that any processing of personal information is covered by the national laws of the country where the user resides; this assertion was contested by Google. The DPAs found that Google does not sufficiently inform its users of the conditions under which their personal information is processed, or of the purposes for the processing; as a consequence, users are not able to correctly exercise their rights of access, correction or deletion. Further, the DPAs held that Google doesn't comply with the obligation to obtain user consent prior to the storage of cookies on their terminal devices, and that it fails to define retention periods applicable to the different data sets it processes, as required under applicable national laws.

UFC-Que Choisir also alleges that the three Internet companies provide insufficient information regarding their

practices to users. For example, the group argues that the contractual terms displayed on the three companies' web pages are "inaccessible, unreadable, and full of hyperlinks—between 40 and 100 hyperlinks—sometimes sending back to pages in English." The group argues in its press release that this allows for the "widespread collection, modification, retention and exploitation of data related to users and their contacts." The group contrasts Twitter and Facebook policies, which are allegedly "very long and fragmented," with the Google Plus policy and its "laconic wording." The group wants the companies to shorten their contractual terms and notify users when they change their conditions, in order to obtain new and valid consent.

Also according to the group, the three companies afford a "worldwide, unlimited and unremunerated license" to share information with their commercial partners without obtaining valid consent. The group warns consumers: "In short, you are not only being targeted with advertising, but your data may also be commercially exploited without your express consent and without receiving compensation." UFC-Que Choisir released to the press some examples of allegedly unfair clauses that are currently accessible online.

Consumer associations everywhere in Europe want to gain influence over data protection issues. As we reported previously, in November 2013, the Berlin District Court upheld similar arguments by the German Federation of Consumer Organisations (VZBV) in proceedings against Google. Germany is expected to pass a bill in the near future that will allow consumer associations to initiate summary proceedings to defend individual rights against infringement of data protection laws. So far, they can only rely on the German Unfair Competition Act where data protection breaches create an economic disadvantage.

Consumer associations also think their role will be strengthened by rapid adoption of the EU reform. In its petition (in French), UFC-Que Choisir states that consumers' control over their own personal information will be put in place as a general principle under the new Regulation. In the provision adopted on March 12, 2014, Parliament increased the fines for companies that violate privacy rules up to EUR 100 million (approximately USD 138 million) or 5 percent of their annual worldwide turnover. Further, the provision reinforces the application of national laws to activities of global companies operating from the U.S. More specifically, the bill clarifies that not only data controllers established outside the EU but also data processors established outside of the EU are subject to EU laws whenever they offer goods or services, regardless of whether payment is required.

> The DPAs found that Google does not sufficiently inform its users of the conditions under which their personal information is processed, or of the purposes for the processing; as a consequence, users are not able to correctly exercise their rights of access, correction or deletion.

However, it is questionable whether these developments will be upheld by the Council, as many Member States have stated that they want to remove administrative burdens from companies. While Parliament has expressed the need to rapidly adopt reforms, the Council has not yet started official negotiations to reach a common position. The likelihood of having the proposed Reform adopted by the end of the year is uncertain.

As for the case at hand, it may be months before the judge makes a ruling. Paradoxically, the UFC-Que Choisir publicly criticized the much-debated May 13 ruling of the European Court of Justice stating that individuals may compel Google to remove links to contested information based on their right to be forgotten. The association said that publishers are responsible for the personal data on their web pages, and not Google. Neutrality goes along with transparency, free movement and freedom of expression on the Internet, all principles that the association says it wants to promote.

"DO YOU WANT TO KNOW A SECRET?" THE RISKS POSED BY ANONYMOUS SOCIAL APPS

By Susan McLean

First we had social media platforms, but recently a variety of "anti-social" media platforms have emerged—well, anti-social in a sense. For years, social media platforms have encouraged (or even, in some cases, required) us to use our real identities, with the aim of building friendships and networks in the online world. But these new social media apps (such as "Secret," "Whisper" and "Yik Yak") are designed specifically to enable users to share posts anonymously. The types of "secrets" disclosed on these apps vary enormously—from teenage angst, fantasies and gossip, to the experiences of soldiers and survivors of abuse.

With these apps, one might say that we have gone full circle back to the early days of the Internet when anonymous posts on message boards were standard. Even Mark Zuckerberg, who in 2010 stated that he believed the social norms on privacy had changed, may now see some merit in anonymity. In January 2014, when discussing certain new Facebook apps that can be accessed with anonymous

sign-in, he stated, "If you're always under the pressure of real identity, I think that is somewhat of a burden."

People sometimes complain that much of social media is fake, with users presenting themselves in the best possible light. Some argue that these apps are different because they encourage authenticity by allowing people to say what they really think without worrying about damage to their digital reputation or posts coming back to haunt them. Fans of the apps also talk of their voyeuristic and addictive nature. And media outlets have even started using anonymous posts as news sources (sometimes to their dismay when the posts turn out to be false).

Users should not be lulled into a false sense of security simply because these apps purport to be anonymous.

Whether these apps have longevity or are just a short-term fad remains to be seen. It is clear, however, that users should not be lulled into a false sense of security simply because these apps purport to be anonymous. Such apps present risks similar to any other social media platform. Indeed, these purportedly anonymous platforms may even be riskier than traditional social media platforms because anonymity may create an environment where users feel free to behave recklessly.

The truth is that "anonymous" doesn't necessarily mean anonymous. Even if users are not required to provide any form of contact details to use an anonymous app, the app is very likely to collect certain information that will help identify the user (e.g., the unique digital ID of the user's mobile device, location information, etc.). Therefore, it may not be very difficult to trace a user if required (e.g., by subpoena/court order). Indeed Secret's Terms of Service state, along the lines of countless other terms of service, "We may share information about you . . . in response to a request for information if we believe disclosure is in accordance with any applicable law, regulation or legal process, or as otherwise required by any applicable law, regulation or legal process." Also, it is worth noting that the extent to which a user can maintain anonymity from other users will depend on how the app works. With Secret, a user's posts are shown to the user's network of phone contacts, and so, depending on what information a user posts, it may not take much for those contacts to figure out who posted a particular secret.

Accordingly, users of anonymous apps need to think carefully about what they post, just as they would when using any social media platform. For example, users should be careful to avoid posting:

- Information that could cause them to breach a court order or be in contempt of court;
- Information that could breach regulatory rules, e.g., in terms of insider trading or market abuse;
- Information that could constitute confidential information or a trade secret;
- Information that breaches a third party's intellectual property rights;
- Defamatory statements;
- Statements that could be considered threatening, abusive, discriminatory or in breach of applicable laws;
- Information that would be a breach of their terms of employment or otherwise constitute misconduct; or
- Anything that violates the app's terms of use.

Using anonymous apps as a vehicle for whistleblowing is particularly problematic. Whisper's editor-in-chief, Neetzan Zimmerman, has publicly advocated such use of Whisper, stating, "We're talking about whistleblowing, exposing secrets at corporations . . . on the government level." But many countries, including the UK and U.S., have specific whistleblower laws in place to protect employees, and companies may also have formal whistleblowing policies that prescribe how employees should report issues. An employee who blows the whistle using an anonymous app rather than through the proper channels may not be able to take advantage of the protections provided by such laws and policies if a disciplinary action is brought against the employee based on such action.

Companies will need to consider these new types of apps when formulating social media policies and educating their employees on social media use. (In the future, companies may even consider subscribing to an enterprise form of anonymous platform. In fact, Secret has just announced a new feature, "Secret Dens," which is focused on anonymous sharing in the workplace.) But it's not just an employee issue. As with other social media platforms, organizations need to be aware of the risks to the company of any criticism or attack via such apps (e.g., from a disgruntled user or competitor) and put in place appropriate monitoring and crisis management procedures to deal with such events.

That said, anonymous apps pose opportunities as well as risks, particularly in terms of targeting consumers who don't use the more traditional social networks. Indeed, in February 2014, Gap Inc. claimed to be behind the first marketing post on Secret. Gap's post asking, "This is the first Fortune 500 company to post on Secret. Guess who?" drew a lot of attention . . . and a few correct guesses.

If you wish to receive a free subscription to our Socially Aware newsletter, please send a request via email to sociallyaware@mofo.com. We also cover social media-related business and legal developments on our Socially Aware blog, located at www.sociallyawareblog.com.

For breaking news related to social media law, follow us on Twitter @MoFoSocMedia. To review earlier issues of Socially Aware, visit us at www.mofo.com/sociallyaware.