Skadden

PRIVACY & CYBERSECURITY UPDATE

MAY 2014

CONTENTS (click on the titles below to view articles)

EU Court of Justice Creates Broad Interpretation of the 'Right to be Forgotten' 1

White House Publishes Report on Risks and Opportunities Posed by 'Big Data' Practices. 3

California AG Provides Guidance on 'Do Not Track' Disclosures 6

California Federal Court Allows Video Privacy Protection Act Claims to Proceed Against Hulu 8

Snapchat Settles FTC Charges That It Misled Consumers About Disappearing Messages 11

LabMD Decision Solidifies FTC's Authority Over Data Security 11

Zynga Privacy Litigation — Ninth Circuit Issues Guidance on Meaning of 'Content' Under the ECPA 12

CFPB Proposes Rule to Allow Online Privacy Notices 14

Department of Energy Releases Cybersecurity Guidelines 14

Recent Decision Underscores That Traditional Insurance Policies May Not Cover Cyber / Privacy Losses 16

California District Court Dismisses Claims Arising From Surreptitious Copying of Contacts 18

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 20, or your regular Skadden contact.

EU COURT OF JUSTICE CREATES BROAD INTERPRETATION OF THE 'RIGHT TO BE FORGOTTEN'

On May 13, the European Court of Justice (ECJ) issued a landmark decision involving the privacy rights of EU citizens. In *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*,[1] the ECJ held that Internet search engine operators could be compelled to take down search results containing personal data if the data subject asked them to do so. By broadly interpreting the EU Data Protection Directive (Directive), the decision enforces a "right to be forgotten" and comes down firmly on the side of bolstering European privacy rights over free speech rights. The sweeping language used in the decision also may have significant ramifications for companies doing business in the European Union.

BACKGROUND

Spanish national Mario Costeja González learned that a Google search of his name generated a link to a 1998 newspaper article mentioning a real estate auction connected with attachment proceedings for the recovery of his social security debts. In 2010, González lodged a complaint with his country's data protection agency, the Agencia Española de Protección de Datos (AEPD), against the newspaper and Google and demanded that both parties remove or conceal the article; he claimed his debts had long been settled, and the information no longer was relevant.

The AEPD rejected the complaint against the newspaper because it had a legal obligation under Spanish law to publish the debt information. However, the AEPD upheld the complaint against Google Inc. and Google Spain and ordered Google to withdraw the relevant link from its index. In response, Google brought two actions before Spain's National High Court, which in turn referred a series of questions to the ECJ regarding the interpretation of the Directive. In June 2013, the ECJ advocate general delivered his opinion, which was in favor of rejecting González's claim. The ECJ, however, adopted a markedly different view in its decision this month.

THE ECJ'S DECISION: KEY FINDINGS

Google is a data processor — and a data controller. The Directive applies only to entities that process or control data. Google asserted it did neither; the company claimed it operates a passive search engine that collects data without any knowledge of what it is collecting and without the ability to exercise any control over that data. Google also maintained that the newspaper was the data controller because it made the decision to publish González's personal information.

The ECJ disagreed. It first found that the activities of a search engine operator constituted "processing of personal data" within the meaning of the Directive because a search engine "retrieves, records, organizes and stores" personal data. The court held that awareness of the personal nature of the data was not required to qualify an operation as personal data processing, and the fact that the data already had been published online was irrelevant to such a finding.

---

[1] *Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez*, Case C-131/12, 13 May 2014, *available at* http://curia.europa.eu/juris/documents.jsf?num=C-131/12.

The ECJ also found that Google was a "data controller" within the meaning of the Directive because it determines the purpose and means of the "processing" it undertakes. As part of its holding, the court noted that "controller" is to be defined broadly to ensure the protection of a data subject's privacy rights. In a theme to which it would return repeatedly, the ECJ emphasized that search engines play a "decisive role" in the dissemination of personal data:

> when users carry out their search on the basis of an individual's name, [it] result[s] in them obtaining through the list of results a structured overview of the information relating to that individual that can be found on the internet enabling them to establish a more or less detailed profile of the data subject.

The court acknowledged that the newspaper may, in fact, be a data controller, but noted that two entities (*i.e.*, the newspaper and Google) each could be controllers.

Google is operating in the EU for data protection purposes. According to the Directive, processing needs to be carried out in a EU member state or through the use of equipment within the territory of a member state to fall within the Directive's ambit. Google asserted it did neither because its search engine processing did not occur in Spain and its Spanish entity served merely as an advertising sales function.

To ensure effective data protection, the ECJ noted this jurisdictional limitation "cannot be interpreted restrictively." It ruled that the processing need not be carried out "by" an EU establishment itself, but merely "in the context of the activity" of an EU establishment.2 In this case, Google Spain's ad sales were dependent on the search capability, and Google's search offering was fueled by sales of ads by Google Spain (which appeared on the same page as the "processed data" of the search engine). This nexus therefore satisfied the "in the context" requirement.

The "right to be forgotten" under the Directive. Given that Google was found to be a data controller operating in an EU member state, the key question for the ECJ was whether, under the Directive, data subjects had a "right to be forgotten" and could compel search engines to take down results about them.

The court first addressed whether this right is available to data subjects. The ECJ noted that since the Directive grants data subjects the right to delete or block "incomplete or inaccurate" data, it reasoned that a data subject also could demand deletion of data that was no longer relevant. As the court explained, the Directive prohibits data from being held "for longer than is necessary for the purpose for which the data was collected."

Google maintained that even if such a right existed, the request should be made to the original publisher of the information. The newspaper, Google asserted, was the entity that could take down the article most effectively, thereby satisfying the data subject's interest in having the information expunged.

The ECJ disagreed, again highlighting the power of a search engine to compile easily a vast array of personal information about an individual. While the court tacitly acknowledged that it could be burdensome for search engines to comply with such takedown requests, it held that potentially serious privacy violations made possible by search engines "cannot be justified by merely the economic interest" of the operator. The power of search engines from a data gathering perspective also justified, in the court's view, requiring a search engine to take down a link, but allowing the original website to retain the content at issue.

Significantly, the ECJ also held that the data subject's right to be forgotten overrides the interest of the general public in finding information when searching for a data subject's name.

---

[2] *Id.*, §§ 52 and 60.

The court purported to craft a standard for when a search engine needed to honor a take-down request but provided operators with only scant guidance. In general, a data subject's interests overrides those of Internet users, and the data subject can demand a link be taken down without having to show they suffered any prejudice. However, the balance between data subjects and Internet users depends on the "information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information." On the latter point, the court effectively created a "public figure" exception by suggesting that public figures would not be able to demand the takedown of their own personal information. In González's case, the ECJ found that he could request the removal of the link from Google's search results given the age of information and that it was no longer relevant.

RAMIFICATIONS

This judgment may have far-reaching implications for privacy rights in the EU and for companies doing business there. At a broad level, the decision highlights the ECJ's determination to uphold strong privacy protection. The court refers repeatedly to the privacy and data protection rights enshrined in the EU Charter; interprets the Directive in a manner that maximizes data protection whenever possible; and interprets the Directive as guaranteeing an enforceable right to be forgotten. The decision also demonstrates the ECJ's perspective that data rights trump the free expression of information — itself a human right. This contrasts sharply with a U.S. vision in which free speech rights would carry the day.

It remains to be seen how search engines will address the ECJ's mandate. However, the decision arguably opens the floodgates to thousands of people requesting that links about them be taken down from search results by asserting that such links are to personal data that is "inadequate, irrelevant or no longer relevant" — even when the information is published legally. The court seems to imply that each request might require a case-by-case decision, a process that would be wholly unworkable.

The decision also broadly interpreted the Directive's extraterritorial coverage by finding that the law applied even where the processing occurs outside the EU, as long as there is some supporting activity (in this case, ad sales) taking place within a member state. Therefore, the decision may result in more companies being subject to the Directive.

Finally, it is ironic that González arguably defeated the very purpose of his suit. The ECJ ruling, and the tremendous publicity it has engendered, means that Google searches of González will turn up information about his past financial troubles — as reflected in the Court's opinion — for years to come.

Return to Table of Contents

WHITE HOUSE PUBLISHES REPORT ON RISKS AND OPPORTUNITIES POSED BY 'BIG DATA' PRACTICES

On May 1, the White House released two reports on "big data" issues. In the first, entitled "Big Data: Seizing Opportunities, Preserving Values" (the Report), the administration described how big data can provide key benefits to the government and the public, but also how it presents new risks for consumers.[3] In the second, entitled "Big Data and Privacy: A Technological Perspective" (PCAST Report),[4] the President's Counsel of Advisors on Science and Technology (PCAST) focused more narrowly on technology issues and solutions. The

[3] The Report is available online at http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.
[4] The PCAST Report is available online at http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

Report, with support in the PCAST Report, makes a number of specific recommendations for legislation and other government intervention measures which, if followed, could have a profound impact on data practices today.

BACKGROUND

President Obama commissioned both reports on January 17, 2014, asking adviser John Podesta and PCAST, respectively, to lead a working group of administration officials to conduct a 90-day study of big data practices and their implications for government and the public. Although the president called for the Report in a speech addressing controversies regarding United States intelligence practices, the Report largely omits discussion of National Security Agency or other intelligence uses for big data. Instead, the working group met with hundreds of stakeholders from industry, academia, public advocacy groups and government, conducted public surveys, attended symposia and solicited input from the public on what it saw as key nonmilitary, nonintelligence issues posed by big data. The result is 78-page report describing a number of benefits and risks posed by the use of big data in the modern world.

For the purposes of the Report, big data refers to an amorphous concept of very large, diverse, complex data sets generated from a variety of different sources, including credit card histories, online browsing and Internet-enabled home appliances. Big data is distinct from "small data," which are data sets that may cover millions of people but are limited in the scope of information they capture, such as the financial records that are so frequently the target of well-publicized cyberattacks. It was in the context of discussing the rise of big data and the perceived associated risks that the president called for the Report.

BIG DATA: BENEFITS AND PROBLEMS

The Report describes the benefits of big data in government with an emphasis on nonmilitary applications such as medical research, education, law enforcement and even road condition analysis. The Report encourages continued growth in these areas, while calling for some legislative changes and continued study and policy review (such as using predictive analytics for law enforcement purposes).

Of greater interest to businesses and consumers, however, will be the Report's findings with respect to commercial use of big data. The Report identifies some of the benefits of big data for companies and consumers and describes how its use can be an engine for economic growth and innovation. Companies can use big data tools to analyze operational and transactional information, to glean insights into consumer behavior and to bring more complicated products to market. Consumers benefit from big data because it fuels an expansion of products and services that benefit them. It enables improved cybersecurity tools through, among other methods, near real-time monitoring for anomalous activity, and allows for the targeted advertising that funds "free" content online and in smartphone applications. Big data even can be used to establish creditworthiness for those who do not have bank accounts.

With the benefits of big data come risks, however, most of which are borne by the consumer. The Report identifies a number of concerns, including a lack of transparency, which means consumers do not know how businesses use information about them to drive decisions, and a lack of accountability as to how this information is used. Consumers also are unlikely to have any direct relationship with data brokers to fully understand the scope of information gathered or how brokers use this information to drive important decisions, or to have any opportunity to try to correct inaccuracies.

The Report describes how some of these practices fall outside of the current legal framework. Data brokers, for example, compile information from sources such as social media, ad network interactions, browsing habits, public records and customer support interactions to develop profiles and groupings of individuals to enable businesses to identify consumers for targeted marketing or special offers. Whereas use of this kind of information to determine eligibility for employment, credit or insurance is subject to regulation under the Fair Credit Reporting Act, data brokers' practices in all other areas are not subject to any regulatory oversight.

The Report also discusses how big data can — unintentionally or otherwise — encode discrimination through automatic decision-making. As an example, some retailers were found to be using an algorithm that generated different discounts for the same product based on the customer's location. In practice, higher-income neighborhoods received greater discounts than lower-income neighborhoods. Although the Report notes that there could be legitimate reasons for this disparity, it does suggest that further study is needed of how companies use big data to make these types of decisions to see whether these algorithms perpetuate existing socio-economic disparities, including in workforce and education settings. Ironically, big data tools also can be invaluable in identifying where these types of disparate impacts develop.

Finally, the Report notes some of the efforts made to address big data issues in recent years, as well as some of the problems presented. The Report cites with approval, for example, the advertising industry's efforts to provide simplified disclosure and opt-out capability for certain types of online advertising, but notes that only a small portion of consumers have actually taken advantage of these initiatives.

Similarly, the Report describes how the focus on consumer disclosure and consent notices imposes on the consumer the burden of deciding how information should be used, and suggests that the emphasis should shift to responsible use of information by data brokers, including a respect for the context in which information is gathered. To this end, the Report contemplates a "no surprises" rule to protect consumers against information being used in a fundamentally different context from that in which it was gathered.

The PCAST Report echoed the Report's concerns with the current disclosure and consent paradigm, and describes a variety of possible complementary systems to replace it. These include a standardized set of privacy profiles from which consumers could select that would apply to a wide range of data collectors (*e.g.*, one profile for all app store applications and one for online advertising). The PCAST Report also calls for a heightened respect for information context by using data tags to identify when and how information was collected and limitations on how it should be used. PCAST cites a variety of examples of where similar structures are in use today, including the United States intelligence community, and a variety of companies with experience building these types of systems.

RECOMMENDATIONS

With these and other concerns in mind, the Report makes a number of specific recommendations in relation to big data. A number of these recommendations relate primarily to government and law enforcement matters, such as making government data more readily available and changing existing rules on when a warrant is required to review stored emails.

If implemented, many of the other recommendations will have a direct impact on consumers and businesses. These include:

- **Enact the Consumer Privacy Bill of Rights.** In February 2012, President Obama unveiled a proposed "Consumer Privacy Bill of Rights," which identified a number of proposed consumer rights with respect to data privacy, including respect for context, security, accountability, individual control, transparency, and access and accuracy. The Report recommends that the

Department of Commerce should solicit input on how big data affects these principles and propose legislation to Congress.

- **Establish National Data Breach Legislation.** The Report echoes the calls from the industry and the Federal Trade Commission to enact a federal data breach notification law to replace differing state laws on the subject.
- **Ensure Data Collected on Students Is Used Only for Educational Purposes.** The Report recommends that regulators ensure that laws protect students against having their information used for inappropriate purposes, especially when this information is gathered in an educational context.
- **Expand Technical Expertise to Stop Discrimination.** The Report recommends that civil rights and consumer protection agencies expand their expertise to identify discriminatory practices and outcomes arising out of the use of big data, and to develop a plan for investigating and resolving violations of law.
- **Lead International Conversations on Big Data.** The Report recognizes that the benefits of big data require a free flow of information, but also present global challenges, and recommends that the United States take the lead in discussing and addressing these issues on an international basis.

The recommendations are, of course, aspirational and there is no guaranty that any will be followed. The president proposed the Consumer Privacy Bill of Rights two years ago; to date, no legislation has been passed. Similarly, there has been widespread agreement for some time on the need for federal data breach legislation, but Congress has yet to pass a bill. Whether these recommendations will fare any better in the current climate remains to be seen. Nevertheless, should any of these be implemented, they could have a significant impact on today's data practices.

Companies that collect or use big data for products and services should examine their practices to see whether they present the types of problems described in the Report, in particular whether these practices result in unintentional discrimination against disadvantaged groups.

Return to Table of Contents

CALIFORNIA AG PROVIDES GUIDANCE ON 'DO NOT TRACK' DISCLOSURES

In late 2013, California amended its landmark California Online Privacy Protection Act (CalOPPA) to require websites and mobile operators to indicate how they handled "do not track" (DNT) signals (*i.e.*, the signals users can set through their browsers or other settings to opt out of tracking by websites they do not visit, including analytics services, advertising networks, and social platforms). California enacted this amendment because there was no requirement that websites or mobile devices actually adhere to a customer's preferences.[5] The amendment does not prohibit tracking or direct sites on how to respond to tracking; but that they disclose how they respond so that consumers make informed decisions.

Although COPPA only applies to California residents, the national reach of almost every online service meant that the DNT requirement effectively became a nationwide requirement. However, online services seeking to comply with the DNT requirement were left with little to no guidance on what types of disclosures they needed to make.

---

[5] As noted in our April 2014 *Privacy & Cybersecurity Update*, the World Wide Web Consortium (W3C), which facilitates collaborative efforts to develop web standards, created a Tracking Protection Working Group, which has been working since 2011 to develop DNT standards. However, the W3C group has not yet agreed upon a number of aspects of this standard, including what a site should do when they receive a DNT signal.

On May 21, 2014, California Attorney General Kamala D. Harris released a new guide, *Making Your Privacy Practices Public*,[6] to address this issue. The guide includes the following important steps for companies to follow:

- The disclosure should be in plain nonlegal language and in a format that is readable, such as a layered format.
- There should be a clearly labeled section to address this issue, such as "How We Respond to Do Not Track Signals."
- The disclosure should describe how the site responds to a browser's DNT signal. In this regard, the guide suggests that the disclosure be included within the privacy policy itself rather than providing a link to a separate program or protocol, even though the latter approach is permitted by the amendment.
- The disclosure should state whether other parties are or may be collecting personally identifiable information of consumers while they are on your site or service.

The guide includes a series of questions that sites should ask themselves when crafting a disclosure on how they respond to DNT signals, including:

- Do you treat consumers whose browsers send a DNT signal differently from those without one?
- Do you collect personally identifiable information about a consumer's browsing activities over time and across third-party web sites or online services if you receive a DNT signal?
- If 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.

In cases where a site decides not to describe its response to a DNT signal, and instead opts to provide a link to a program that offers consumers a choice about online tracking, it should:

- Provide a brief, general description of what the program does.
- Indicate that the company complies with that program.
- Consider whether the program clearly informs consumers about the effects of the program. For example, does participation result in stopping the collection of the consumer's personally identifiable information across web sites or online services over time?
- Does the program make clear what a consumer must do to exercise the choice offered by the program?

If the company is allowing third parties to collect information on its site or service, it should disclose the presence of such parties and whether they may be conducting online tracking. When making statements about such parties in the privacy policy, companies should consider:

- Are all of those parties approved to collect information?
- Is there a way to ensure that authorized third parties are not bringing unauthorized parties to the site or service to collect personally identifiable information?
- Can the company ensure that authorized third-party trackers comply with the site's DNT policy? If not, companies should disclose how they might diverge from the policy.

---

[6] *Available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.

Finally, companies should confirm with IT or other personnel that their actual tracking practices are consistent with what is stated in the policy.

While most of the guide deals with DNT, it also includes pointers for crafting a privacy policy more generally, including disclosing how companies use personally identifiable information beyond what is necessary to fulfill a customer transaction or for the basic functionality of an online service; and providing a link to the privacy policies of third parties with whom the site shares personally identifiable information. In addition, the guide states that sites should describe any choices a consumer has regarding the collection, use and sharing of his or her personal information; and include who they can contact with questions or concerns about the site's privacy policies and practices.

Return to Table of Contents

CALIFORNIA FEDERAL COURT ALLOWS VIDEO PRIVACY PROTECTION ACT CLAIMS TO PROCEED AGAINST HULU

In *In re: Hulu Privacy Litigation*,[7] Magistrate Judge Laurel Beeler of the U.S. District Court for the Northern District of California denied summary judgment as to claims alleged against Hulu under the Video Privacy Protection Act, 18 U.S.C. § 2710 (VPPA) with respect to disclosures of alleged personally identifiable information (PII) to Facebook. The *Hulu* ruling underscores the need for online video service providers to tightly monitor and control their disclosure of user information to third parties.

BACKGROUND

Hulu is an online video streaming service that allows registered users to view TV episodes or movies on-demand through its website. To register for a Hulu account, users supply a first and last name, date of birth, gender and email address. Paying subscribers also must supply payment information and a billing address. Hulu assigns each registered user a unique numerical identifier (Hulu User ID).

Hulu derives the majority of its revenue through online advertising based on the number of users who view each advertisement. This number is determined through comScore, a company that collects data and provides verified reports regarding digital media consumption.

During the alleged class period, each time a user watched a video on Hulu, code written by Hulu sent comScore, among other things, the following information:

- A Hulu User ID.
- A code that Hulu used to identify the user's web browser.
- The name of the video program being viewed.

In addition, the Hulu code prompted the user's browser to send to comScore a web cookie stored on the user's web browser that had been created and was accessible only by comScore. The comScore cookie contained a unique but anonymized comScore user ID assigned to that copy of the web browser (the comScore User ID). The comScore User ID allowed comScore to track the user's activity across other websites and over time. Hulu did not disclose the name of the user to comScore.

[7] No. C 11-03764 LB (N.D. Cal. Apr. 28, 2014).

Hulu's code also caused the user's web browser to send a request to Facebook to load the Facebook "Like" button on the page so that the user would have the option to "Like" the video on Facebook. In addition, Facebook received multiple cookies associated with the facebook.com domain.

As a result, during the relevant period, each time a user viewed a watch page, Facebook received, among other things, the following information:

- The title of the video watched (in the Hulu URL).
- A unique identifier for the user's web browser.
- The identity of the most recent user to log into Facebook using that browser.
- If the registered Hulu user was also logged into Facebook, the user's Facebook ID.

This transfer of information occurred automatically when the user loaded the watch page; no action by the user (such as clicking the "Like" button) was required. Hulu never sent Facebook a user's Hulu User ID or the name supplied by the user upon registration with Hulu.

The plaintiffs, on behalf of two putative classes of registered Hulu users and subscribers, alleged that Hulu violated the VPPA by disclosing users' PII to comScore and Facebook. PII is defined under the VPPA to include "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." The VPPA generally prohibits videotape service providers from knowingly disclosing PII without the written consent of the consumer, and permits a court to award punitive damages and attorneys' fees, in addition to statutory damages of at least $2,500 per violation.[8] The plaintiffs' bar has recently invoked the VPPA to attack the alleged disclosure of PII by a variety of online video providers to third party data trackers like comScore.[9]

The primary question addressed by the court opinion was whether the information transmitted to comScore and Facebook constituted PII — *i.e.*, whether it linked a particular person and the video selected by that person.

THE COURT'S RULING

Examining the plain language of the VPPA and its legislative history, the court held that disclosure of video viewing information "must be pegged to an identifiable person (as opposed to an anonymous person)" in order to be actionable. However, the court rejected Hulu's argument that the VPPA prohibits only disclosure of the person's actual name. The court held that a unique, "anonymized" ID could constitute PII if, under the facts of a particular case, the context of the transmission rendered it "not anonymous and the equivalent of the identification of a specific person."

With respect to comScore, the plaintiffs alleged that Hulu's disclosure of a video title with the Hulu User ID constituted the disclosure of PII because comScore could search Hulu profile pages using the Hulu User ID to identify the Hulu user and link him or her to the video selection. The court rejected the plaintiffs' hypothetical theory of liability, holding that there was no evidence that suggested comScore actually tried to "reverse engineer" the Hulu data in this fashion. While recognizing that the transmission of the comScore cookie allowed comScore

---

[8] 18 U.S.C. § 2710(c)(2).

[9] *See Perry v. Cable News Network, Inc., et al.*, Case No. 1:14-cv-01194 (N.D. Ill.) (filed Feb. 18, 2014, alleging disclosure of iPhone MAC address to Bango); *Ellis v. Cartoon Network, Inc.*, Case No. 1:14-cv-00484 (N.D. Ga.) (filed Feb. 19, 2014, alleging disclosure of Android ID to Bango); *Locklear v. Dow Jones Co., Inc.*, Case No. 1:14-cv-00744 (N.D. Ga.) (filed Mar. 13, 2014, alleging disclosure of Roku identifier to mDialog); *Eichenberger v. ESPN, Inc.*, Case No. 2:14-cv-00463 (W.D. Wash.) (filed Mar. 28, 2014, alleging disclosure of Roku identifier to Adobe).

to link the user's video viewing choices to an anonymous comScore User ID, gather a lot of information about the user, and target advertising at that user, because such disclosure did not "reveal[] an identified person and his video watching," there was no VPPA violation.

The court reached a different conclusion with respect to Hulu's disclosures to Facebook, finding that the link between user and video was "more obvious" because the video information and identifying cookies were sent in a single transmission. The court determined that Facebook could identify the user through his or her Facebook page (using the Facebook cookies) and the video he or she had watched (using the Hulu URL). The court also focused on the fact that the Hulu code automatically loaded the "Like" button and transmitted the URL and Facebook cookies to Facebook without any decision by the user. The court noted that "[t]he analysis would be different if the Facebook cookies were sent when a user pressed the Like button," since information transmitted as a necessary part of a user's decision to share his or her views about a video with friends on Facebook would not support a VPPA violation.

The court further noted that, although the transmission of cookies created by Facebook from the user's browser was a normal part of Internet communication with Facebook, Hulu easily could have developed a web page that did not communicate information to Facebook at all — *i.e.*, it was Hulu's decision to do business with Facebook. The court brushed aside Hulu's argument that the plaintiffs presented no evidence that Facebook in fact linked its cookies to the Hulu users' Facebook identities, noting that the VPPA focuses on the knowing disclosure of PII, not on the comprehension of that disclosure by the person receiving the PII.

The court also found fact issues with respect to Hulu's knowledge of the disclosures and as to whether Facebook user's had consented to the disclosures by agreeing to Facebook's privacy policies during the relevant periods. With respect to knowledge, the court noted that, under the VPPA, "[i]f Hulu did not know that it was transmitting both an identifier and the person's video watching information, then there is no violation of the VPPA." The court's ruling with respect to Hulu's knowledge was based in part on the fact that the motion for summary judgment was brought early in the discovery process, and discovery had already revealed emails suggesting that Hulu recognized the VPPA implications of allowing third parties to place cookies and other web-based technologies on Hulu's watch pages, thus enabling the third parties to "collect data and use it for other purposes to build a profile or 'identify a user in the real world.'"

PRACTICE POINTS

The court's contextual and fact-driven approach may spur more litigation in this area. To reduce the risk of liability, online video and other service providers should place themselves in the position of the parties receiving their data to evaluate whether such data is adequately scrubbed, aggregated or otherwise "anonymized," and to determine whether such user data could be reverse engineered or "de-anonymized" to reveal the identities of the actual users associated with that data. Ideally, these questions should be posed to engineering teams early and often as part of the company's implementation of a "privacy by design" approach to product development. This lawsuit highlights the importance of the legal team working closely with engineers to understand and verify the content of and purpose behind data flows to and from third parties.

Return to Table of Contents

SNAPCHAT SETTLES FTC CHARGES THAT IT MISLED CONSUMERS ABOUT DISAPPEARING MESSAGES

On May 8, the mobile messaging service Snapchat settled claims brought by the FTC alleging that the company made representations to consumers that were at odds with how the application actually worked.

Snapchat offers a messaging service through which photo and video messages are erased shortly after being viewed. However, the FTC objected to Snapchat's touting of the ephemeral nature of its messages, given the existence of third-party apps and simple workarounds that allowed photos and videos to be permanently saved. The FTC also objected to Snapchat's assurances that consumers would be notified if a message recipient took a screenshot of the image, given that this notification easily could be disabled on Apple devices running certain operating systems. Finally, the FTC took issue with Snapchat's claims that it took reasonable security steps to secure its "Find Friends" feature prior to the January 2014 security breach that permitted hackers to access usernames and phone numbers.

Pursuant to the consent decree, which is subject to public comment before becoming final, Snapchat does not admit fault, but agrees to certain terms. These terms include making accurate representation of its privacy or security features going forward. The company also agrees to implement a comprehensive privacy program, and to obtain security and privacy assessments twice per year for the next 20 years from an independent third-party professional.

The FTC's complaint and the proposed settlement highlight the FTC's continuing use of Section 5 as a hammer against companies that misrepresent their privacy and security protections. What makes the Snapchat action so unique is that the company was charged with misrepresenting its privacy claims not because of its actions, but because of offerings by third parties. The case therefore is a warning signal to companies to monitor whether their privacy claims stand up against what is going on in the marketplace.

PRACTICE POINTS

- As companies increasingly use "privacy and security" as a selling point for their products and services, they need to be mindful that their representations are accurate.
- When making privacy representations and when marketing their products and services, companies should take into account third-party offerings that render the company's privacy representations or marketing statements to be inaccurate.

Return to Table of Contents

LABMD DECISION SOLIDIFIES FTC'S AUTHORITY OVER DATA SECURITY

On May 12, a Georgia federal judge dismissed LabMD's lawsuit challenging what the company called the FTC's "abuse of power" in bringing a security complaint against the company under Section 5. This setback for LabMD marked the second time in the last month that a company's challenge to the FTC's authority was rejected. As we reported in our *April Privacy & Cybersecurity Update*, Wyndham Hotel recently confronted a similar defeat.[10]

LabMD had argued that Section 5 of the FTC Act does not give the FTC authority to determine whether data security protections are "unfair" in the absence of definitive federal legislation in this area. LabMD also argued that even if the FTC has authority to regulate data privacy under Section 5, it does not have authority in the health information arena since Congress,

[10] *Available at* http://www.skadden.com/insights/privacy-cybersecurity-update-april-2014.

in passing HIPAA and HITECH, delegated sole enforcement authority to the Department of Health and Human Services. The potential regulation of cybersecurity by yet another agency renders this decision of particular note for health care companies.

The FTC's initial complaint, filed in August 2013, alleged that LabMD's failure to implement security measures sufficient to prevent a 2012 data breach violated Section 5. The data breach involved a file of billing information for approximately 10,000 customers being uploaded to a P2P sharing site. Police subsequently discovered the information of a subset of these customers being used by identity thieves. After the FTC initiated its administrative action, LabMD challenged the FTC's authority on several fronts. First, LabMD asserted within the context of the FTC's own enforcement action that the FTC lacked appropriate authority. The FTC denied this challenge, issuing a ruling in January 2014 affirming its data security authority. LabMD then filed an action in the District of Columbia seeking an injunction preventing the FTC from proceeding in the administrative action. It also filed a petition for review of the FTC's order in the U.S. Court of Appeals for the Eleventh Circuit, which ruled that it had no jurisdiction to consider the petition because the statute "only gives courts of appeal authority to review an order of the commission to cease and desist from using any method of competition or act or practice, [and] there is no such order here."

This ruling prompted the company to abandon its District of Columbia suit and file a new suit for an injunction in Georgia. The Georgia court deemed there to be no final underlying agency action, and therefore dismissed the case without it did not reach the merits of the dispute. LabMD has filed for an emergency appeal to the Eleventh Circuit, arguing that the January FTC ruling affirming its authority was in fact a final agency action. In support of its argument, LabMD contends that when the FTC argued for *Chevron* deference of its ruling during the Georgia court suit, the FTC itself was categorizing the ruling as a "final agency action." This Eleventh Circuit appeal is still pending, as is the underlying agency action.

The Georgia court's ruling is a victory for the agency since it allows the administrative action to proceed, and shuts down other avenues for LabMD to challenge the FTC's data security authority. While the dismissal was a setback for LabMD, the ruling in this case does not mean that the FTC has definitive data security authority, but rather postpones determination until after the final agency decision is reached. In the meantime, the FTC likely will continue its aggressive pursuit of companies that it deems to have failed to maintain sufficient privacy and security precautions. LabMD's procedural loss, coupled with last month's holding against Wyndham Hotels, may discourage other companies from challenging the FTC's authority over cybersecurity matters.

Return to Table of Contents

ZYNGA PRIVACY LITIGATION — NINTH CIRCUIT ISSUES GUIDANCE ON MEANING OF 'CONTENT' UNDER THE ECPA

On May 8, the U.S. Court of Appeals for the Ninth Circuit issued its opinion in *In re Zynga Privacy Litigation*,[11] rejecting attempts by plaintiffs to expand the definition of "contents" of a communication under the Electronic Communication Privacy Act of 1986 (ECPA). However, the opinion revived certain state law claims by finding that the plaintiffs potentially suffered damages by losing their ability to sell their personal information.

[11] No. 11-18044 (9th Cir. May 8, 2014).

BACKGROUND

The plaintiffs alleged that Facebook's and Zynga's transmissions of their "referer header" information to third parties violated the plaintiffs' privacy rights protected under the Wiretap Act and Stored Communication Act. A referer header informs a website of the last site the user was on before they linked to the website. The plaintiffs alleged that when a Facebook user clicked on an advertisement or icon of an advertisement on a Facebook page, the referer header informed the advertiser of the specific Facebook page the user was on when they clicked on the advertisement. Similarly, when a user launched a Zynga game from a Facebook page, the referer header displayed the user's unique Facebook ID and the address of the Facebook page the user was viewing before clicking on the game icon. Zynga allegedly programmed its gaming applications to then further transmit information contained in the referer header on to advertisers and other third parties. The plaintiffs claimed that these actions by Facebook and Zynga violated the ECPA's Wiretap Act and Stored Communications Act because these laws prohibit electronic communication service providers and providers of remote computing services from making unauthorized disclosures of the "contents" of users' communications to any person other than the intended recipient of the communication. The district court dismissed with prejudice the plaintiffs' claims.

FEDERAL LAW CLAIMS

In affirming the dismissals, the Ninth Circuit held that the referer information at issue — *i.e.*, a user's Facebook ID and the address of the webpage from which the request was sent — did not constitute the "contents" of a communication for the purposes of the ECPA.[12] Analyzing the plain language, structure and legislative history of the ECPA, the court held that "contents" means the "intended message conveyed by the communication and does not include record information regarding the characteristics of the message that is generated in the course of the communication."[13] The court reasoned that because the Facebook ID functions as a name or subscriber number or identity, and the web address functions like an address, the referer header contained only "record" information specifically excluded from the protections of the ECPA.

STATE LAW CLAIMS

In an unpublished opinion, the panel revived the plaintiffs' California state law fraud and breach of contract claims against Facebook, holding that in the absence of any contravening state law, the plaintiffs had sufficiently pled damages by alleging that they lost the sales value of their personal information. The decision is significant because it is contrary to the holdings of district courts that have dismissed breach of contract claims on the grounds that disclosure of personal information did not constitute legally cognizable damages.

However, the court opinion did not salvage all of the plaintiffs' state law claims. The Ninth Circuit affirmed the district court's dismissal of the plaintiffs' California Unfair Competition Law (UCL) claim because the plaintiffs failed to allege they "lost money or property as a result of the unfair competition," holding that personal information did not constitute "lost property" for purposes of the UCL. Similarly, the plaintiffs' California Consumer Legal Remedies Act claim failed because they did not "purchase" anything from or engage in a "consumer transaction" with Facebook.

Return to Table of Contents

---

[12] 18 U.S.C. §§2511(3)(a) and 2702(a)(2).

[13] The Stored Communication Act specifically excluded customer record information such as the name, address, and subscriber number or identity from the meaning of "contents."

CFPB PROPOSES RULE TO ALLOW ONLINE PRIVACY NOTICES

The ubiquitous annual privacy notice from financial institutions to which consumers have grown accustomed may soon be a thing of the past. The Consumer Financial Protection Bureau (CFPB) recently issued a proposed rule that, subject to the bureau's jurisdiction, would allow banks and financial institutions subject to replace these written documents with online notices in most situations. The CFPB proposal is a reflection of the pervasive use of online services, including to receive financial statements and to conduct banking transaction, and the reality that written privacy notices have been relegated to "junk mail" that is being disregarded by many consumers.

The written privacy notices that are provided today satisfy the requirement under Gramm-Leach-Bliley Act to provide customers with an initial, and then annual, notice as to how their nonpublic personal information is used and shared.[14] Electronic notices are not permitted unless customer consent was first obtained.

Under the CFB's proposed rule, financial institutions can switch from a paper notice to an online notice as long as they do not share information in a manner that trigger a customers' opt-out rights, and as long as the notice has not changed since the last year. Such opt-out rights exist when information is being shared with third parties that are not, for example, simply providing services to the financial institution. Financial institutions that do share information with third parties would be required to keep using the paper notice method of communication.

When using the online posting approach, financial institutions also have to provide customers with an annual disclosure that (i) states the privacy notice has not changed, (ii) directs consumers as to where they can find the notice online and (iii) informs the customer they can request a copy of the notice by mail if they call a toll-free number. This information could be included as an insert to an existing monthly communication, such as in a monthly billing statement. Currently, privacy notices cannot be included in such communications and must instead be their own separate mailing, a costly and cumbersome process for financial institutions.

The CFPB proposed rule balances this easier and cheaper method of distribution with a requirement that the financial institution use the CFPB Model Privacy Notice. The challenge that many institutions will face is whether the "one-size-fits-all" Model Privacy Notice is applicable to their own institution.

Return to Table of Contents

DEPARTMENT OF ENERGY RELEASES CYBERSECURITY GUIDELINES

The U.S. Department of Energy (DOE), in conjunction with private energy companies, has issued guidance on how the energy sector and its technology suppliers can minimize cybersecurity risk when they buy and sell energy delivery systems.

The new guidance, the *Cybersecurity Procurement Language for Energy Delivery Systems*, includes sample contractual provisions that energy sector companies can use to ensure that cybersecurity is a key consideration when procuring such systems or components thereof. In 2009, the DOE and the U.S. Department of Homeland Security (DHS) collaborated with industry cybersecurity and control system subject matter experts to publish their Cyber Security Procurement Language for Control Systems. The new DOE document provides critical updates to that 2009 DHS language, taking into account new cyberthreats and the evolution of the energy sector.

[14] The notices are required under Regulation P, which implements the act's financial privacy requirements.

The guidance focuses on the cybersecurity of energy delivery systems, which include various types of control systems, including SCADA and EMS systems, as well as fully assembled energy delivery systems with information technology components. The new DOE document does not address the procurement of general information technology systems for the energy industry except to the extent integrated into systems specifically associated with energy delivery.

This guidance notes that it is only providing a starting point for energy sector cybersecurity procurement, and that as the cybersecurity landscape continues to evolve, "new threats, technologies, techniques, practices, and requirements may need to be considered during the energy sector procurement process." The guidance is geared at three categories of energy sector stakeholders: "Acquirers" that procure energy systems; "Suppliers" that sell and deliver such systems; and "Integrators" that provide customized features such as combining components.

This guidance specifies that it is intended for use by the following:

- Acquirers seeking to incorporate cybersecurity into the procurement of energy delivery systems or components. Requests or specifications may be issued by the Acquirer through requests for proposal or requests for information.
- Acquirers seeking to evaluate the cybersecurity maturity of energy delivery systems or components offered by Suppliers and Integrators.
- Suppliers and Integrators designing or manufacturing systems, components and services that will meet cybersecurity features requested by Acquirers (or in some cases, Integrators).
- Acquirers, Integrators and Suppliers negotiating procurement contracts that outline cybersecurity features and responsibilities for each party involved in the procurement.[15]

The document provides "baseline cybersecurity procurement language" in the following areas:

- Individual components of energy delivery systems (*e.g.*, programmable logic controllers, digital relays, or remote terminal units).
- Individual energy delivery systems (*e.g.*, a SCADA system, EMS or DCS).
- Assembled or networked energy delivery systems (*e.g.*, an electrical substation (transmission and distribution) or a natural gas pumping station).[16]

Separately, Rep. Henry A. Waxman (D-Calif.) and Sen. Edward J. Markey (D-Mass.,) recently introduced the Grid Reliability and Infrastructure Act (the GRID Act), which would authorize the Federal Energy Regulatory Commission (FERC) to issue emergency orders or regulatory rules to address key threats to the U.S. electrical grid, including cyberattacks.

PRACTICE POINTS

The DOE guidance provides an important foundation document for those responsible for system procurement, operation and compliance within the energy sector, and demonstrates the government's expanding commitment to protecting the nation's critical infrastructure against cyberattacks. However, companies implementing the guidance likely will need to tailor the suggested language to the products and services they are procuring since not every device or piece of software can realistically support all of the listed controls. Companies may therefore want to consult a security expert before imposing all of these requirements on a supplier in every case.

---

[15] Energy Sector Control Systems Working Group, *Cybersecurity Procurement Language for Energy Delivery Systems* (2014), at 6-7.
[16] *Id.* at 4.

A broader question is whether acquirers will in practice demand that these requirements are met, especially if suppliers raise prices dramatically to accommodate any new suggested security improvements not already incorporated into their products. Suppliers also may push back against the guidance's broad audit provisions, which when read broadly, could require them to identify every country in which each component originates or in which software modules are developed, to allow customers to conduct on-site investigations at supplier development facilities, or to allow customers to approve their suppliers' employee background check methodologies. These provisions and a number of others may cause suppliers to raise concerns with the wholesale adoption of the DOE suggested language.

Return to Table of Contents

RECENT DECISION UNDERSCORES THAT TRADITIONAL INSURANCE POLICIES MAY NOT COVER CYBER / PRIVACY LOSSES

In the wake of numerous high-profile and costly data breach and other cyber incidents, many insureds and insurers alike have sharpened their focus on the question of coverage. A recent Pennsylvania district court decision, *Am. Ins. Co. v. Urban Outfitters, Inc.*,[17] highlights that insureds that rely on such policies to respond to cyber / privacy claims may do so at their peril. The case adds to the body of conflicting case law regarding potential coverage under traditional "non-cyber" insurance policies.

In *Urban Outfitters,* OneBeacon America Insurance Company and the Hanover Insurance Company sought a declaration that they had no duty to defend clothing retailers Urban Outfitters, Inc. and its Anthropologie, Inc. subsidiary (collectively, Urban Outfitters) in three putative class actions — *Hancock* (District of Columbia), *Dremak* (California) and *Miller* (Massachusetts) — where the retailers faced allegations that their collection of customer ZIP codes during credit card transactions violated various state common and statutory privacy laws.

Urban Outfitters argued that OneBeacon and Hanover had a duty to defend the underlying litigations pursuant to Coverage B of certain primary and excess umbrella commercial general liability policies, which provided coverage for "personal and advertising injury." The insurers countered that they had no such duty because the complaints failed to allege an "invasion of privacy," a "publication" or "damages," all of which were required by the policies, in addition to raising a number of coverage exclusions. After noting that the underlying allegations and terms of the insurance policies control the existence of the duty to defend, the court analyzed each of the underlying complaints individually.

The *Hancock* complaint alleged that Urban Outfitters collected customers' ZIP code information, which, when bundled with other information, enabled the retailers to engage in direct marketing campaigns without customers' permission in violation of District of Columbia statutory bans. Resorting to dictionary definitions of "publication," a term undefined in the insurance policies, the court agreed with the insurers that there was no coverage because no "publication" was alleged under Pennsylvania law. "Our dictionary of choice likewise makes clear that promulgation to the public, even to a limited number of people, is the essence of publication." Here, the *Hancock* plaintiffs "allege only that the retailers used their ZIP code information 'to determine their home or business addresses,' where '[d]efendants sent unsolicited mailings or other material.'"

With respect to the *Dremak* action, the sole remaining count was the retailers' alleged violation of California's Song-Beverly Credit Card Act, which proscribes businesses from collecting supplemental personal identification information unnecessary for processing credit card

[17] No. 13-5269, 2014 WL 2011494 (E.D. Pa. May 15, 2014).

transactions. According to the *Dremak* plaintiffs, Urban Outfitters did exactly that in collecting customers' ZIP code data. Unlike the *Hancock* complaint, however, the *Dremak* complaint contained the additional allegation that "Urban Outfitters shared the ZIP code information with third parties (including vendors and retailers) or sold it to them for marketing purposes, without informing the customers." The court found that this allegation "although generalized, suffices to fall within Pennsylvania's definition of 'publication' in the context of an invasion of privacy claim, because plaintiffs allege communication to so many people that the matter must be regarded as likely to become public knowledge."

Relying on precedent from the California Supreme Court that "a ZIP code constitutes 'personal identification information' as that phrase is used" in the statute and "[t]hus, requesting and recording a cardholder's ZIP code, without more, violates the Credit Card Act," the court also rejected the insurers argument that the *Dremak* plaintiffs failed to allege a privacy violation within the scope of the policies' "personal and advertising injury" coverage part. Nonetheless, the court found applicable an exclusion present in each of the policies, which barred coverage for "'[p]ersonal and advertising injury' arising directly or indirectly out of any action or omission that violates or is alleged to violate … [any] statute … that … prohibits … the … collecting [or] recording … of … information." Because the *Dremak* allegations arose out of the alleged violation of the statutory right to privacy under the Song-Beverly Act that prohibits collecting or recording personal information, the court agreed with the insurers that this exclusion barred coverage.

The court then turned to the *Miller* action where the Massachusetts analog to California's Song-Beverly Act was at issue. The *Miller* plaintiffs alleged that Urban Outfitters violated their statutory right to privacy "by recording ZIP code information and using that data for its own marketing and promotions – including sending junk mail to the plaintiffs." This, according to the court, was "quite different" than *Miller* where the plaintiffs alleged dissemination to third parties. Relying on Pennsylvania state and federal lower court precedent, the court drew a somewhat fine distinction by confining the term "privacy" as used in the insurance policies to afford coverage against violations of one's right to "secrecy" versus "seclusion," the latter of which was allegedly violated by the unsolicited "junk mail" allegations in *Miller*. The court thus held that the insurers had no duty to defend Urban Outfitters in this case either.

When faced with costly cyber or privacy losses, policyholders certainly should thoroughly consider which of their traditional insurance policies might respond to a particular incident and aggressively pursue all available coverage. However, Judge Dalzell's recent opinion in *Urban Outfitters* serves as a reminder that there may not be coverage under these policies, the question may turn rather fortuitously on the nuanced manner in which plaintiffs plead their allegations, and, even where successful, an insured may be mired in protracted litigation to enforce its policy rights.

In addition, an increasing majority of insurers have taken the position that traditional insurance policies are not intended to cover cyber / privacy losses and are imposing broad exclusions to that effect. A growing number of insurers, however, are offering cyber / privacy insurance, whether as an optional enhancement to traditional insurance policies or on a standalone basis. Risk managers and other relevant personnel should evaluate their company's exposures and consider cyber / privacy insurance as one potential component of a comprehensive risk management plan. In this regard, no standard coverage form has emerged; and the policies that are out there are not all created equally. If the decision is made to procure cyber / privacy coverage, it is important that the policy be reviewed carefully in advance to ensure that it meets the company's needs and expectations.

Return to Table of Contents

CALIFORNIA DISTRICT COURT DISMISSES CLAIMS ARISING FROM SURREPTITIOUS COPYING OF CONTACTS

On May 14, Judge Jon S. Tigar of the U.S. District Court for the Northern District of California dismissed nearly all claims asserted against Apple and several developers of popular applications, including Facebook, arising from the allegedly surreptitious copying by certain Apple App Store apps of contacts stored on Apple's iPhone, iPod Touch and iPad (the iDevices). The comprehensive ruling in *Opperman v. Path* reaffirmed the liberal standing requirements of the U.S. Court of Appeals for the Ninth Circuit, but rejected the plaintiffs' vague claims of reliance on alleged misrepresentations by Apple and dismissed a variety of other statutory and common law privacy claims.

BACKGROUND

When the App Store was launched in 2008, Apple reviewed each app and decided which would be sold in the App Store. Apple published its App Store Review Guidelines, which prohibited the transmission of user data without prior permission. The plaintiffs alleged, however, that Apple's "iOS Human Interface Guidelines" encouraged data theft by teaching app developers how to design their apps to steal a user's contacts without the user's knowledge.

The plaintiffs alleged that certain apps copied the user's contacts without prompting while others utilized the app's "Find Friends" feature. In September 2012, under pressure from Congress and amid calls for an FTC investigation, Apple released its iOS6, which updated privacy settings on iDevices in a manner that disclosed which apps accessed users' contacts and allowed users a way to prevent the copying of information.

THE COURT'S RULING

The plaintiffs asserted 26 claims under federal, California, and Texas statutory and common law against 15 defendants on behalf of a putative class of iDevice purchasers from 2008 to the present. In general, the plaintiffs' claims can be divided into two categories: (i) misrepresentation claims alleging that Apple misrepresented the security of its iDevices and that the plaintiffs either would not have purchased or would have paid less for the iDevices had they known the iDevices permitted the surreptitious copying of contacts; and (ii) invasion of privacy claims under statutory and common law.

Ninth Circuit's Liberal Standing Requirements Reaffirmed. The court held that the plaintiffs' generalized claims of economic loss as a result of Apple's alleged deception sufficiently alleged injury-in-fact and causation for standing purposes. In addition, citing the Ninth Circuit's decision in *Edwards v. First American Corp.*,[18] the court noted that the plaintiffs' allegations of statutory violations independently established standing. Finally, analogizing to claims against Toyota that advertisements touting the reliability of Toyota's vehicles fraudulently induced consumers to purchase defective Toyota cars, the court held that the claim that iDevice purchasers would have paid less for the iDevices was sufficient to establish standing.

On the other hand, the court dismissed certain claims against the app developers for lack of standing. The court rejected the plaintiffs' theory that the "use" by app developers of a user's iDevice battery and other resources constituted the "injury-in-fact" required for standing because the plaintiffs failed to quantify or articulate such usage. The plaintiffs' request for injunctive relief did not support standing because the change in Apple's privacy controls eliminated any realistic threat of repetition of the allegedly unlawful act. The court held the alleged interference with property rights in the contacts insufficient because the plaintiffs failed to

[18] 610 F.3d 514 (9th Circ. 2010).

allege how they lost value from the alleged theft: "'[A] plaintiff must do more than point to the dollars in a defendant's pocket; he must sufficiently allege that in the process he lost dollars of his own.'" The court nevertheless found standing with respect to the statutory claims (under *Edwards*) and the plaintiffs' common law claims for invasion of privacy. With respect to the latter, the court held the alleged invasion of privacy was itself sufficient to confer standing.

No Immunity for Apple Under the Communications Decency Act. The Communications Decency Act (CDA) immunizes the provider of an interactive computer service for liability linked to the conduct of an information content provider. While acknowledging that courts construe the definition of service provider broadly and content provider narrowly, the court rejected Apple's claim to CDA immunity because the plaintiffs alleged that Apple encouraged the data theft in its "iOS Human Interface Guidelines." Assuming these allegations to be true, the court found such activity went beyond the ordinary editorial functions of a publisher or the provision of neutral tools used to carry out unlawful conduct, and could constitute contribution to the allegedly illegal activity of the app developers.

Misrepresentation Claims Against Apple Dismissed. The plaintiffs asserted misrepresentation claims against Apple under the Unfair Competition Law, California's False and Misleading Advertising Law, California's Consumer Legal Remedies Act and for common law negligent misrepresentation. The plaintiffs pointed to alleged statements by Apple on its website, in in-store advertisements and elsewhere to the effect that its iOS was "highly secure" and alleged that Apple "attempted to cultivate a perception that its products are safe and that Apple strives to protect users." The plaintiffs alleged that they visited Apple's website at some point during the class period. The court dismissed the plaintiffs' misrepresentation claims because the plaintiffs failed to allege a specific representation by Apple, or that each named plaintiff read or actually relied upon the misstatement.

The plaintiffs claimed they were the victims of a long-term and extensive advertising campaign and, thus, need not plead actual reliance on specific misrepresentations by Apple. After reviewing and synthesizing the case law in this area, Judge Tigar rejected the plaintiffs' theory because (i) the plaintiffs failed to allege they were actually exposed to the campaign; (ii) the complaint lacked sufficient details as to the extent of the advertising; (iii) the plaintiffs failed to attach a representative sample of the advertisements, leaving the court unable to determine whether they were sufficiently similar; (iv) the claim that the plaintiffs "viewed Apple's website" gave defendants insufficient detail as to how the plaintiffs were exposed to the campaign; and (v) plaintiffs failed to allege when they purchased their iDevices, making it impossible to determine whether such purchases were before or after the alleged advertisements.

Finally, the court rejected the plaintiffs' pure omission/nondisclosure claims on the ground that a manufacturer's duty to speak is limited by its warranty obligations absent some affirmative misrepresentation or a safety issue. The plaintiffs failed to allege Apple's warranty terms.

Other Privacy Claims Dismissed. The court also dismissed claims against Apple and the App Developers under the California Comprehensive Computer Data Access and Fraud Act, and against the App Developers under the Computer Fraud and Abuse Act, on the ground that these statutes require access to computer data "without permission," meaning "'in a manner that circumvents technical or code based barriers in place to restrict or bar user's access.'" The plaintiffs made no such allegations. The court also dismissed claims under federal, California and Texas wiretap statutes, including the Electronic Communications Privacy Act, on the ground that the plaintiffs did not allege the interception of a communication in the course of the allege theft of iDevice contact lists.

Products Liability and Negligence Claims Dismissed. The plaintiffs claimed the iDevices were defective in that they permitted the alleged invasion of private contact lists. The court

dismissed these strict products liability and negligence claims against Apple because recovery of economic harm is not permitted under these theories. The court rejected the plaintiffs' theory that the invasion of privacy itself constituted a "physical harm to person or property" to support the claims.

Common Law Invasion of Privacy Claim Against App Developers Survives. The plaintiffs asserted claims against the app developers for "intrusion upon seclusion" and "public disclosure of private facts." The court dismissed the latter claim because the plaintiffs failed to allege a public disclosure of their contacts. The alleged exposure of the contacts by transmission over public Wi-Fi networks was held insufficient. The court allowed the "intrusion upon seclusion" claim to proceed, finding that the plaintiffs had a reasonable expectation of privacy in their contacts and that the court could not conclude, as a matter of law, that the invasion was not "highly offensive." Distinguishing a case involving the commercial use of zip codes gathered from customers to obtain an address list for direct mail advertising, the court held: "[W]hile the Court recognizes that attitudes toward privacy are evolving in the age of the Internet, smartphones, and social networks, the Court does not believe that the surreptitious theft of personal contact information — which is what the CAC alleges — has come to be qualified as 'routine commercial behavior.'" As for damages, the court held that no allegation of economic injury was required; allegations of anxiety, embarrassment, humiliation and the like were sufficient.

LOOKING AHEAD

Judge Tigar's decision in *Path* represents a victory for defendants and serves to clarify and synthesize decades of false advertising law. However, the court reaffirmed the Ninth Circuit's liberal standing requirements, which may further encourage plaintiffs asserting privacy violations to file in California courts. The court granted leave to amend within 30 days of the order.

Return to Table of Contents

SKADDEN CONTACTS

STUART D. LEVI
Partner / New York
212.735.2750
stuart.levi@skadden.com

JAMES S. TALBOT
Counsel / New York
212.735.4133
james.talbot@skadden.com

TIMOTHY A. MILLER
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

GREGOIRE BERTROU
Counsel / Paris
33.1.55.27.11.33
gregoire.bertrou@skadden.com

TIMOTHY G. REYNOLDS
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

OLIVIER BOULON
Associate / Paris
33.1.55.27.11.32
olivier.boulon@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000