Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

EYE ON PRIVACY

MARCH 2013

Welcome

Mobile has been on the minds of privacy regulators as of late, and this month we discuss mobile disclosure guidelines from the Federal Trade Commission, mobile privacy practice recommendations from the California attorney general, and lessons learned from the Dutch privacy investigation into the WhatsApp mobile application. We also examine several potential pitfalls for lawyers using social media, analyze the White House's recent executive order on cybersecurity, provide an update on a recent decision narrowing California's Song-Beverly Act, and address a recent Tenth Circuit ruling regarding the application of the Electronic Communications Privacy Act to online behavioral advertising.

Also, please keep an eye on the wsgr.com Events page, where we'll soon be announcing our April webinar providing practical and actionable guidance on managing and responding to security breaches.

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

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

FTC Releases Privacy Disclosure Guidelines for Mobile Ecosystem

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

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

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

Rachel Landy
Associate, New York
rlandy@wsgr.com

In February, the Federal Trade Commission (FTC) issued a report containing recommendations[1] for companies working in the mobile ecosystem to improve mobile privacy disclosures for consumers. Such guidelines can serve as an important and useful roadmap for future agency investigations and enforcement activity. As promised in its 2012 report titled "Protecting Consumer Privacy in an Era of Consumer Change: Recommendations for Businesses and Policymakers" (the Privacy Report),[2] the FTC has taken great interest in the mobile space.[3] It recently released two reports that surveyed mobile apps for children and brought enforcement actions against app

Continued on page 2...

[1] The FTC's Staff Report, titled "Mobile Privacy Disclosures: Building Trust Through Transparency," is available at http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

[2] See our WSGR Alert discussing the Privacy Report at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-FTC-final-privacy-report.htm. The FTC's Privacy Report is available at http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[3] See our WSGR Alert discussing the FTC's recent settlement with mobile app developer Path at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-social-networking-mobile-COPPA.htm.

In This Issue

developers. The Privacy Report called on companies to adhere to three core principles: privacy by design, simplified consumer choice, and greater transparency. The FTC acknowledged that the mobile industry faces unique challenges and complexities in implementing these core principles, and the guidelines in the February 2013 mobile report represent the agency's attempt to help mobile companies understand and adhere to the principles.

Importantly, the FTC focuses not just on app developers, but on all of the major participants in the mobile ecosystem: platforms/application (app) stores; app developers; advertising networks, analytics providers, and other third parties providing services to apps; and trade associations. The FTC expects these stakeholders to work together to develop better privacy disclosure practices to ensure that consumers are aware of how data about them is collected and shared. The report was released in conjunction with the FTC's "Mobile App Developers: Start with Security" online business guide for developers to evaluate their app's privacy practices.[4]

FTC's Concerns with Mobile Privacy Disclosures

The FTC's focus on mobile stems from a mobile device's ability to collect and share large amounts of information about consumers' activities, including sensitive information such as a user's precise location. After hosting a workshop and reviewing public comments on mobile privacy issues, the FTC concluded that consumers do not know or understand the data collection and usage practices occurring on mobile devices and that the screen size of mobile devices limits the options for effectively communicating important information. The FTC followed with these recommendations.

Platforms/App Stores[5]

The FTC identified platforms/app stores as the key actors with the ability to most improve mobile privacy disclosures and explained that it placed the primary onus on app stores because they can set requirements for app developers and control the interface between consumers and apps. The agency recommends several actions for these gatekeepers, as outlined below.

- **Improve Disclosures.** The report urges app stores to provide consistent disclosures across apps. Further, the FTC recommends that app stores consider providing the following:
  - *Just-in-Time Disclosures.* App stores could provide just-in-time disclosures of an app's collection of sensitive content through the platform's application programming interface (API), such as geo-location information, and obtain affirmative express consent from consumers. Such disclosures are provided to consumers just prior to collecting the data, which allows users to make informed choices about whether to permit the collection.
  - *Privacy "Dashboard."* A privacy dashboard could allow consumers to easily view and modify what data can be accessed by each app.
  - *Icons.* Icons could clearly communicate key terms and concepts.
- **Improve App Oversight and Impose Privacy Requirements.** The FTC encourages app stores to make visual space for privacy information and enforce apps' contractual requirements to have privacy policies. In addition, the FTC recommends that app stores add more privacy-related contract terms and enforce them.
- **Clearly Communicate the App Review Process.** The report encourages app stores to provide users with clear disclosures about their review and compliance processes.
- **Implement Do Not Track (DNT).** The report suggests that platforms implement a DNT mechanism consistent with the requirements listed in its Privacy Report.[6] The platform would provide a single destination for users to make selections related to data collection for all of the apps available on the platform.

App Developers

The FTC made several recommendations for app developers to improve the process of informing consumers about their privacy practices.

- **Publish a Privacy Policy.** The report states that all apps should have a privacy policy available through the app store. The FTC believes that app developers increasingly will create privacy policies now that many app stores have agreed with the California attorney general's office to include a data field through which an app developer can provide a hyperlink to the privacy policy, the text of the privacy policy, or a short statement describing the app's privacy practices.
- **Provide Just-In-Time Disclosures and Obtain Affirmative Express Consent to Collect Sensitive Information.** When an app collects or shares information deemed to be sensitive by the FTC, such as financial, health, or children's data, apps should provide just-in-time disclosures and

[4] The guide is available at http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

[5] In the report, the FTC seems to equate operating system platform providers with app store providers (e.g., Google, Apple, Microsoft, and Blackberry). However, some app store providers do not also provide an operating system platform. Some of these guidelines may pertain to app store providers regardless of whether they also provide an operating system platform.

[6] The FTC sets forth the following criteria for an effective DNT tool: that it (a) be universal, (b) be easy to find and use, (c) be persistent, (d) be effective and enforceable, and (e) limit collection of data.

Continued on page 3...

obtain affirmative express consent. These disclosures are separate from the just-in-time disclosures provided by the app store related to data, such as geo-location data, collected through a platform API.

- **Coordinate with Ad Networks and Third-Party Service Providers.** The FTC suggests that app developers often do not understand the data collection and usage practices of third parties whose codes they use to facilitate advertising or analytics within an app. The agency cautions that such a lack of understanding results in unclear or incorrect privacy disclosures. Therefore, the FTC recommends that app developers coordinate with third-party service providers to obtain clearer information about their data practices so that app developers can more accurately disclose them.

- **Participate in Self-Regulatory Programs and Trade Associations.** App developers should consider participating in self-regulatory programs, trade associations, and industry organizations to help draft uniform, short-form privacy disclosures. The FTC stated that it would view adherence to strong privacy codes of conduct favorably in connection with its law-enforcement work.

Third-Party Service Providers, Including Advertising Networks

The FTC made some recommendations specific to third-party service providers, such as ad networks.

- **Coordinate and Communicate with App Developers.** The FTC stated that third-party service providers should improve coordination and communication with app developers so that app developers can provide more accurate privacy disclosures.

- **Comply with DNT Systems.** The FTC recommends that advertising networks work with platforms to comply with the DNT systems.

App Trade Associations

The FTC concluded that trade associations can play an important role by developing privacy disclosure standards and educating app developers.

Mobile Security: FTC's "Start with Security" Website

Along with its privacy disclosure recommendations, the FTC launched a website with tips to help app developers with app security. The website states that the FTC "expects app developers to adopt and maintain reasonable data security practices and doesn't prescribe a one-size-fits-all approach." The website makes the following recommendations to app developers:

- Make someone responsible for security
- Take stock of the data you collect and retain
- Understand differences between mobile platforms
- Do not rely on a platform alone to protect your users
- Generate credentials securely
- Use transit encryption for usernames, passwords, and other important data
- Use due diligence on code libraries and other third-party code
- Consider protecting data you store on a user's device
- Protect your servers
- Do not store passwords in plain text
- You are not done once you release your app—stay aware and communicate with your users
- If you are dealing with financial data, health data, or kids' data, make sure you understand applicable standards and regulations

Implications

This report and website demonstrate the FTC's strong interest in privacy and data security in the mobile industry. In an effort to improve mobile companies' compliance with the privacy principles expressed in its Privacy Report, the FTC has provided more specific recommendations to the rapidly growing mobile industry. Given the additional guidance for mobile companies, the FTC likely will continue to monitor mobile companies' privacy practices. Therefore, any company directly or indirectly involved with providing mobile services should re-examine its privacy disclosure and consumer choice practices in light of the guidance and consider increasing its communication and coordination efforts with other stakeholders. The FTC made clear in its report that, to the extent the recommendations go beyond existing legal requirements, the recommendations are not intended to serve as a template for law-enforcement actions or regulations under laws currently enforced by it. However, entities that provide mobile services directly or entities that provide services for mobile apps should view this report and the security website as important sources of best practices when developing their privacy and data security practices. The agency has a history of active and aggressive exercise of its enforcement authority and investigations can be costly and time-consuming to defend.

Tip

Have you assessed how your website can be used to collect data? New technical tools are available to help organizations better understand how their services may collect, use, and share data.

California Attorney General Issues Privacy Practice Recommendations for Mobile Ecosystem

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

Sharon Lee
Associate, Palo Alto
shlee@wsgr.com

California Attorney General Kamala Harris continues to position herself as one of the most active enforcers of consumer privacy rights. In January, the attorney general's office issued *Privacy on the Go: Recommendations for the Mobile Ecosystem,*[1] a set of privacy best practices for the mobile space. The report is targeted primarily to developers of mobile applications (apps), but also includes recommendations for app platform providers, ad networks, operating system developers, and mobile carriers. The report acknowledges that the recommended privacy practices, in some respects, exceed what is required by the law, but are motivated by the goal of encouraging players in the mobile marketplace to consider privacy implications at the outset of the design process and to follow the Fair Information Practice Principles[2] in their decision-making.

The report highlights Attorney General Harris's view of the privacy and security risks posed by the use of mobile devices. In addition to addressing the risks common to networked computers and mobile devices (e.g., the collection of large amounts of personal information and malware threats), the report details the risks unique to mobile devices, such as:

- their storage of user information not usually found on personal computers (e.g., telephone call logs, text messages, and history location);
- their small screens (which present additional challenges for effective communication of privacy practices and user choices); and
- the relatively early development stage of the app industry (which may result in less attention to privacy considerations).

The report is yet another step in a series of actions that Attorney General Harris has taken to augment privacy enforcement in California. In the last year, she reached an agreement with several major mobile app platform providers under which the companies agreed to a Joint Statement of Privacy Principles designed to ensure that mobile apps post privacy policies in accordance with California's Online Privacy Protection Act. She also announced the creation of a Privacy Enforcement and Protection Unit, and brought a privacy enforcement action against a company that failed to include a privacy policy within its mobile app.

General "Surprise Minimization" Approach

A theme running through the report is that companies should embrace "surprise minimization"—the concept that companies should minimize surprises to users from unexpected privacy practices. The report coined the new privacy phrase and encouraged companies to adopt this approach, including by:

- refraining from collecting personally identifiable data that is not needed for an app's basic functionality;
- making an easily understood privacy policy readily available prior to app download;[3] and
- using enhanced measures (i.e., outside of the privacy policy) to both alert and give control to users over data practices that are either not related to an app's basic functionality or that involve sensitive information.

The report encourages app developers to put this concept into practice by using in-context and just-in-time privacy notices and choices regarding unexpected privacy practices. The implementation of the concept could prove to be challenging, however, as it requires app developers to make judgments regarding consumer expectations about the collection and use of their data.

Broad Definition of "Personally Identifiable Data"

The report sets forth Attorney General Harris's broad view of what constitutes "personally identifiable data." In addition to information customarily considered personal, such as name, phone number, email address, and financial information, the report includes in the definition such information as unique device identifiers, geo-location data, web-browsing history, photos, and apps downloaded or used. This broad definition, if enforced, could have a considerable impact on companies' privacy and security practices. For example, the report recommends that companies develop mechanisms to give users access to the personally identifiable data that the app collects and retains, and encrypt in transit and storage all personally identifiable data.

Specific Privacy Practice Recommendations

The report makes specific privacy practice recommendations for various players in the mobile system, as summarized below.

---

[1] *See* http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

[2] The Fair Information Practice Principles (FIPPs) are guidelines that represent widely accepted concepts concerning fair information practices. The FIPPs are grounded in five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress. For more information about the FIPPs, please visit the FTC's web page on the FIPPs at http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

[3] Attorney General Harris has taken the position that the California Online Privacy Protection Act (CalOPPA) applies to apps. CalOPPA requires operators of commercial websites to "conspicuously" post on their websites, and operators of online services (including apps) to make reasonably accessible, a privacy policy that informs consumers about the categories of personal information collected by the operators and the categories of third parties with which the data is shared. CalOPPA, Cal. Bus. & Prof. Code §§ 22575-22579.

Continued on page 5...

California Attorney General Issues . . . *(continued from page 4)*

For app developers, the report emphasizes that the most efficient way to build privacy into an app is to consider it at the outset of the development process. To that end, the report recommends creating a "data checklist" to assess the types of personally identifiable data that an app collects. The app developer could then use this checklist and resulting assessment of the use and disclosure of the data to inform its design and privacy practice decisions and to prepare the apps' privacy policies, enhanced notices, and controls. The report also encourages app developers to limit the collection and retention of sensitive and personally identifiable information for uses not related to an app's basic functionality, give users access to their personally identifiable data, and use security safeguards.

For app platform providers, the report reiterates the privacy practices agreed to in the Joint Statement of Principles, including making app privacy policies accessible on the app platform so that users may review them before downloading an app.[4] The report further encourages app platform providers to educate app developers and consumers on mobile privacy.

For ad networks, the report recommends implementing or supporting an app developer's implementation of the "surprise minimization" approach by: preparing a privacy policy; providing the privacy policy and corresponding link to the app developer for the developer to make them available to users before download; informing the app developer of the impact of the ad network's privacy practices on app software development kits (SDKs); and using enhanced notice measures and obtaining prior consent before accessing users' personal information. In addition, the report recommends that app developers generally avoid delivering out-of-app ads and transition from using permanent, device-specific identifiers to app-specific or temporary device identifiers.

For operating system developers and mobile operators, the report suggests a few ways in which mobile ecosystem players can collaborate to enhance consumer privacy. The report specifically recommends that operating system developers offer users global privacy settings and overrides, which could be accessed by apps. In addition, the report recommends that mobile carriers educate their customers on mobile privacy.

Industry Criticism

Although the report stated that the attorney general's office engaged a "broad spectrum of stakeholders" to arrive at the recommendations, a coalition of Internet and media advertising associations immediately sent a letter criticizing the attorney general's office for not adequately seeking the input of companies expected to implement the report's recommendations.[5] The letter asserted that the recommendations do not reflect the perspective or input of the broader industry, that they extend far beyond existing legal requirements, and that they are unworkable and may harm the economy.

Takeaways

Privacy protection has been a top priority for California Attorney General Harris. The *Privacy on the Go: Recommendations for the Mobile Ecosystem* report builds on her extensive efforts in the mobile privacy space over the past year. Although these guidelines do not carry the force of law, they offer mobile ecosystem players insight into the attorney general's view regarding best privacy practices for players in the mobile space. In light of the additional enforcement actions that can be expected from Attorney General Harris's Privacy Enforcement and Protection Unit, mobile ecosystem players would be wise to examine how their privacy practices measure against the privacy practice recommendations offered in the report.

[4] For more information about the Joint Statement of Principles of February 2012, please see http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf.

[5] *See* January 2013 Letter to Attorney General Harris, *available at*: http://the-dma.org/government/InternetTradeAssoicationLettertoCAAG.PDF.

Mobile Apps: Learning from the WhatsApp Dutch Privacy Investigation

Cédric Burton
Associate, Brussels
cburton@wsgr.com

Anna Pateraki
Associate, Brussels
apateraki@wsgr.com

On January 28, 2013, the Dutch Data Protection Authority[1] (Dutch DPA) published an opinion addressing its findings from the investigation into WhatsApp, Inc., a California-based company, and WhatsApp's processing of personal data in the context of the WhatsApp mobile application. The WhatsApp mobile application is an instant-messaging application with more than 400 million users worldwide that is used largely in the Netherlands.

The opinion follows a one-year joint investigation by the Office of the Privacy Commissioner of Canada and the Dutch DPA into the privacy practices of WhatsApp. The two regulators have issued separate reports relating to each country's data protection law

[1] "College bescherming persoonsgegeven" in Dutch.

Continued on page 6...

and will pursue any further action independently.[2] This article provides an analysis of the Dutch DPA opinion.

Learning from the Dutch DPA Opinion

In its opinion, the Dutch DPA describes in detail the facts, the investigation, and how the WhatsApp mobile application works. It also elaborates on the applicable legal framework and assesses whether WhatsApp's privacy practices are compliant with Dutch data protection law. In particular, the Dutch DPA discusses the issues of applicable law, jurisdiction, controllership and the obligation to appoint a representative in the Netherlands, legal grounds for the processing of personal data, proportionality, data-retention principles, and security requirements.

Below are some key findings and recommendations addressing a few select issues[3] that can generally be helpful for mobile app providers:

- Applicable law and obligation to appoint a representative: The Dutch DPA determined that the use of apps on Dutch users' smartphones is a means for processing personal data located in the Netherlands and that the display of app features in Dutch targets Dutch individuals. Therefore, the Dutch DPA noted, these two elements trigger the application of Dutch data protection law.[4] Following this interpretation, every global mobile app provider could potentially be subject to EU national data protection law for app services provided to individuals located in the EU.[5] Furthermore, the Dutch DPA identifies WhatsApp as the data controller for the processing of personal data and thus requires this entity to appoint a representative in the Netherlands, as is required for any data controller subject to Dutch law but not established in the Netherlands. This representative is responsible for compliance with Dutch data protection law.

- Access to mobile phone contacts only with consent: At the time of the investigation, once the users had given their consent to the use of their address books to identify other WhatsApp users from their contacts, the app was able to pull and store information from the mobile device's full address book, including telephone numbers for both WhatsApp users and non-users. The Dutch DPA determined that consent is the only appropriate legal basis for the collection of both users' and non-users' data, and that consent given by users to grant access to their address books does not extend to non-users' data contained in such address books, since users cannot grant unambiguous consent on behalf of non-users. Thus, accessing the users' full address books to collect and process non-users' data without their consent was considered to be illegal and excessive by the Dutch DPA. Furthermore, the fact that users were not given the ability to decide which contact details to share[6] contravenes the Dutch Data Protection Act.

- Best practices for the processing of non-users' data: One mitigating measure that had been implemented by WhatsApp for the collection of non-users' data was to de-identify this data and keep it in hashed format. By doing this, WhatsApp no longer considered this data to be "personal data." However, according to the Dutch DPA, the type of one-way hash used for non-users' data could allow for the re-identification of the data (e.g., by recalculating the hashed numbers of non-users and creating a look-up table) and was therefore not sufficient to reach the threshold for anonymization.[7]

  The Dutch DPA nevertheless acknowledges that obtaining non-users' consent may be impossible and thus recommends performing an initial "compare and forget" scan of mobile phone numbers contained in the users' address books. This method should be strictly limited to identification of the contacts who are already WhatsApp users or those who have provided their consent in the past to be identified in such searches. The contact details of non-users should be deleted immediately after this scan.

- Retention period for inactive accounts: WhatsApp was storing the personal data of inactive accounts for one year after the accounts were last used.[8] However, the Dutch DPA felt that the retention period for inactive accounts should be shorter than one year after the last use. The regulator recommended sending reminders to users of inactive accounts and, in the case of inactivity, the users' accounts should be automatically cancelled and all their data erased.

- Pop-up notification for status submissions: Although not strictly required by Dutch law, the Dutch DPA recommended that users be warned via a pop-up message that their status will be globally viewable by WhatsApp users every time they change it. In the interim, WhatsApp has amended its privacy policy

---

[2] *See* Dutch report, available at http://www.dutchdpa.nl/downloads_overig/rap_2013-whatsapp-dutchdpa-final-findings-en.pdf (English translation); *See* Canadian report, available at http://www.priv.gc.ca/cf-dc/2013/2013_001_0115_e.asp.

[3] It is important to note the good collaboration of WhatsApp with the regulators and, in particular, that WhatsApp has taken steps to mitigate some privacy and security issues that regulators had identified (e.g., measures to enhance its encryption and authentication processes) and has committed to continue improving its data protection practices.

[4] *See* Dutch report pp. 19, 20.

[5] Under current draft EU data protection legislation, which is likely to become law in a few years, EU data protection law will apply to all non-EU-based companies offering services remotely to EU citizens. For more information, please visit www.wsgr.com/eudataregulation.

[6] This is no longer true for iPhone users with iOS6 software who can manually select the contacts they would like to add.

[7] *See* Dutch report, p. 30.

[8] This retention period could be increased to two years if the user installed the app and only tried it out once but did not actively cancel the account. *See* Dutch Report, p. 33.

Continued on page 7...

to provide more transparency about the different levels of status visibility and urges users not to submit status updates that they do not wish to share globally.

- Security requirements: WhatsApp was using the hashed Wi-Fi MAC address on iPhones and the hashed IMEI device number on other smartphones for generating individuals' passwords. These practices have been considered by the Dutch DPA to be insufficient under Dutch law, since they could be easily reproduced and used to hack into the user database. WhatsApp subsequently issued a new version of its app to modify the way it generates users' passwords.[9]

Conclusions and Trends

The WhatsApp case is one of the first investigations involving mobile apps in Europe and cooperation among DPAs in different regions of the globe. The joint investigation of the Canadian and Dutch authorities forced WhatsApp to modify its privacy practices to take into account both Dutch and Canadian data protection law.[10] Mobile applications are definitely on the EU DPA's agenda and an Article 29 Working Party opinion is expected very soon on this topic.[11] The WhatsApp case provides a number of interesting recommendations and gives an indication of what to expect regarding the forthcoming Article 29 Working Party opinion. In particular, it underscores a trend of broad interpretation of EU law requirements and their extension to non-EU mobile app companies. Following the Article 29 Working Party opinion, every mobile app provider offering app services to EU individuals should conduct a risk analysis to assess whether EU law applies to its business and, when it does, review its practices in light of EU data protection law.

[9] However, the security of inactive accounts (e.g., when the application has not been updated by the users) should still be improved to ensure that expired versions of inactive users' WhatsApp messages could not be intercepted and read.

[10] In response to the investigation by the Dutch and the Canadian regulators, WhatsApp modified a number of its practices and also has announced that it will prioritize the following points in its future implementation plan: (i) security of inactive accounts; (ii) retention periods and relevant notice (the privacy policy is expected to be updated in the coming months); and (iii) pop-up notification about the visibility of status messages when users update such messages.

[11] *See* Article 29 Working Party agenda, http://ec.europa.eu/justice/data-protection/article-29/press-material/agenda/files/public_agenda_20130226-27_en.pdf.

Caution! Social Media Can Get You Into Trouble

Colleen Bal
Partner, San Francisco
cbal@wsgr.com

Scott Andrews
Associate, San Francisco
sandrews@wsgr.com

Online social media platforms such as LinkedIn, Facebook, and Twitter offer tremendous potential benefits to lawyers, particularly for factual investigations, marketing, and public relations efforts. But the world of social media presents traps for the unwary, including in ways that may seem surprising when compared with traditional forms of communication. In this article, we describe several ways a lawyer can unwittingly get into trouble using social media.

"Friending" a Judge

It is hardly unusual for practicing attorneys to know judges personally and, indeed, attorneys are actively encouraged to meet and mingle with judges at bar association and other professional functions. But can lawyers and judges ever be "friends"?

"Friending" in the social media context generally refers to the act of giving another person access to one's private information on a particular social media platform. As observed by the Eastern District of Pennsylvania, Facebook friendships are commonplace and "may be as fleeting as the flick of a delete button."[1]

Yet in a recent decision, the Florida District Court of Appeal ruled that a judge must be disqualified for having a Facebook friendship with a prosecutor appearing before the judge, on the grounds that the Facebook relationship "would create in a reasonably prudent person a well-founded fear of not receiving a fair and impartial trial."[2] That decision relied heavily on a Florida Judicial Ethics Advisory Committee Opinion stating that a Facebook friendship between a judge and an attorney would convey the impression that the attorney was in a special position to influence the judge, resulting in the judge violating Florida Code of Judicial Conduct Canon 2(B) (similar to American Bar Association Model Code of Judicial Conduct Rule 2.4(c)). A later ethics opinion from the same panel found that the perception of improper influence would not be dispelled even if the judge accepted as Facebook friends all attorneys who request that status and posted a disclaimer on the Facebook profile page stating that "friend" means only "acquaintance," not "friend" in the traditional sense.[3] Oklahoma has adopted the reasoning of both Florida judicial ethics opinions.[4]

[1] *Quigley Corp. v. Karkus*, No. 09-1725, 2009 U.S. Dist. LEXIS 41296, at *16, n.3 (E.D. Pa. May 19, 2009).

[2] *Domville v. State*, 103 So.3d 184, 186 (Fla. Dist. Ct. App. 2012).

[3] Florida Judicial Ethics Advisory Committee Opinion No. 2010-06 (Mar. 2010).

[4] *See* Okla. Judicial Ethics Advisory Panel, Judicial Ethics Opinion 2011-3 (July 6, 2011).

Continued on page 8...

In contrast, a Kentucky ethics opinion allows Facebook friendships between judges and the lawyers who might appear before them. The Ethics Committee of the Kentucky Judiciary has stated that "designation of a 'friend' on a social networking site does not, in and of itself, indicate the degree or intensity of a judge's relationship with the person who is the 'friend.' The committee conceives such terms as 'friend,' 'fan' and 'follower' to be terms of art used by the site, not the ordinary sense of those words [sic]."[5]

New York and California permit judges to become "friends" with attorneys who may appear before them in court, but advocate caution to prevent the appearance of impropriety.[6] Among factors to take into account are how personal the site appears to be, how many "friends" the judge has, whether the judge accepts many or only a few people into his or her social network, and whether the specific attorney "friend" appears before the judge regularly.[7] Under these guidelines, a judge should not "friend" an attorney who might appear before the judge if the judge's social media site is used purely for personal purposes, such as posting family pictures, because that "friendship" connotes a close personal relationship between the judge and attorney.[8] The California ethics committee also advises that a judge should not become the Facebook friend of a lawyer currently appearing before him or her and should "unfriend" a currently appearing lawyer who was already an online friend.[9]

Communications with Parties and Witnesses

Social media offers terrific tools for gathering facts about witnesses, jurors, and opposing parties, but the use of social media can blur the line between private research and improper communication.

It is unsurprising that lawyers and their agents are prohibited from sending friend requests that contain false information to try to gain access to the private, social media information of a witness or party. For instance, the New York Bar Association advises against attorneys creating a phony Facebook profile that makes the attorney appear to have some affinity (such as shared hobbies or backgrounds) with parties or witnesses, to try to encourage their acceptance of a friend request. Similarly prohibited would be having an investigator email a YouTube account holder, "falsely touting a recent digital posting of potential interest as a hook to ask to subscribe to the account holder's 'channel' and view all of her digital postings." Such deceptive behavior would violate New York Rules of Professional Conduct 4.1 (lawyer cannot use another person to take acts that lawyer is barred from taking) and 8.4(c) (barring attorney "conduct involving dishonesty, fraud, deceit or misrepresentation").

But a lawyer also can get into trouble using only a true identity. The San Diego County Bar Association's Legal Ethics Committee has opined that a lawyer cannot send a friend request using his or her true name to an opposing party without stating the purpose for the request.[10] Failure to disclose the purpose would exploit the other party's lack of understanding of the adversarial relationship between the requesting attorney and the party.[11] In that context, the lawyer might violate anti-deception rules such as California Business & Professions Code Section 6068(d) and ABA Model Rules 4.1(a) and 8.4(c).[12]

Truthful friend requests to a represented party also may violate rules forbidding lawyers from communicating about the subject of a representation without the consent of the party's counsel. Even if the friend request made no reference to the underlying dispute, the San Diego Ethics Committee has opined that the request would be "about the subject of the representation" because its purpose would be to obtain information for use in the representation.[13]

There are, however, conflicting views as to whether a lawyer must reveal the purpose of a friend request to a witness. The Philadelphia Bar Association Professional Guidance Committee has opined that a lawyer should not employ a third person to send a request to a witness that does not reveal the purpose of the request.[14] Such a request "omits a highly material fact, namely, that the third party who asks to be allowed access to the witness's pages is doing so only because he or she is intent on obtaining information and sharing it with a lawyer for use in a lawsuit to impeach the testimony of the witness."[15] In contrast, the New York City Bar concluded that "an attorney or her agent may use her real name and profile to send a 'friend request' to obtain information from an unrepresented person's social networking website without also disclosing the reasons for making the request."[16] New York University Law School ethics professor Stephen Gillers agrees with this opinion: "This is no different than if a lawyer or investigator learns that a witness typically hangs out at a bar on Saturday nights, and the investigator sidles up to the witness and starts a conversation. If the investigator doesn't misrepresent himself or his purpose, then it's OK."

---

[5] Formal Judicial Ethics Opinion JE-119 (Jan. 20, 2010), *Kentucky Bench & Bar* (Mar. 2010).

[6] *See* N.Y. Advisory Committee on Judicial Ethics, Op. 08-176; Cal. Judges Ass'n Judicial Ethics Comm., Op. 66.

[7] Cal. Judges Ass'n Judicial Ethics Comm., Op. 66 at 8.

[8] *Id.* at 9.

[9] *Id.* at 10–11.

[10] San Diego County Bar Ass'n, Legal Ethics Op. 2011-2.

[11] *Id.*

[12] *Id.*

[13] *See* San Diego County Bar Ass'n, Legal Ethics Op. 2011-2; *accord* Oregon State Bar Formal Opinion No. 2005-164 at 453–54.

[14] The Philadelphia Bar Ass'n Professional Guidance Comm., Opinion 2009-02 (March 2009).

[15] *Id.* at 3.

[16] N.Y. City Bar Ass'n Formal Opinion 2010-2: Obtaining Evidence From Social Networking Websites.

Continued on page 9...

Caution! Social Media . . . *(continued from page 8)*

Researching Jurors

Lawyers typically are barred from communicating with jurors during jury selection and trial, except during court proceedings and as otherwise allowed by the judge. It is therefore impermissible for a lawyer to communicate with venire persons or impaneled jury members in the following ways: sending a "friend request," attempting to connect via LinkedIn, signing up for an RSS feed for a juror's blog, or "following" a juror's Twitter account.[17] That much may be obvious. But there are less obvious ways of using social media sites that may result in inadvertent improper communication. For instance, if a juror becomes aware that an attorney is trying to see the juror's profiles, the "contact may well consist of an impermissible communication . . . ."[18] Twitter account holders can see who is "following" them on Twitter and, depending on the account settings, may receive a communication with the identity of each new "follower." Similarly, LinkedIn provides a function that allows a user to see the identities of a subset of other users who recently viewed the user's profile. A lawyer therefore must know whether his or her actions in trying to learn about the juror will cause the juror to become aware of the attempt, in order to determine whether that attempt is permissible.[19]

Spoliation of Social Media Evidence

Spoliation of social-media-based evidence also raises particular concerns. As an initial matter, it is often unclear whether a corporate party has a duty to preserve evidence that an employee, contractor, or other person maintains through a social media account. The line between corporate social media accounts and personal accounts seems increasingly blurred. In the recent case of *PhoneDog v. Kravitz*,[20] the company claimed to own the Twitter account maintained by an employee, but the employee claimed that the company had given him control when he left the company's employ. In some industries, employees routinely maintain their own professionally oriented social media accounts through which they promote the work they are doing for their employers. In these situations, disputes may arise as to whether the corporate entity has any obligation to preserve the social media data for use in anticipated or pending litigation.

Frequent updating of social media data may render it even more ephemeral than electronically stored information generally. If such data is being replaced frequently, counsel should tailor litigation hold policies accordingly. On the other hand, it is not always clear whether the deletion of social media data causes the data to become permanently unavailable. The persistence of deleted data depends heavily on the particular preservation policies of the social media platform at issue. In *Lester v. Allied Concrete Co.*,[21] a plaintiff intentionally deleted photographs on his Facebook profile that were damaging to his litigation position, only to have them recovered by the defense using a forensic expert. Similarly, in *Romano v. Steelcase Inc.*,[22] the court ordered the plaintiff to give the defendant access to "all deleted pages" from the plaintiff's Facebook and MySpace pages.

Conclusion

In summary, social media presents new opportunities for attorneys, but also new challenges. To keep out of trouble, lawyers should try to stay abreast of the (potentially conflicting) applications of legal and ethical rules to social media communications in relevant jurisdictions. This will require an understanding of how social media platforms work. Being aware of when a click will send an impermissible communication might be key to preventing a case-altering mistake.

---

[17] *See* N.Y. County Lawyer's Ass'n, Committee on Professional Ethics, Formal Opinion No.: 743 (May 18, 2011).

[18] *Id.*

[19] N.Y.C. Bar Formal Opinion 2012-2.

[20] *PhoneDog v. Kravitz*, No. C 11–03474 MEJ, 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011).

[21] *Lester v. Allied Concrete Co.*, Case No. CL.08-150, slip. op. at 4 (Va. Cir. Ct. Sept. 1, 2011).

[22] *Romano v. Steelcase Inc.*, 30 Misc. 3d 426, 435, 907 N.Y.S.2d 650, 657 (N.Y. Sup. Ct. 2010).

Into the Breach: The Executive Order on Cybersecurity

Don Vieira
Partner, Washington, D.C.
dvieira@wsgr.com

Brock Dahl
Associate, Palo Alto
bdahl@wsgr.com

President Barack Obama released an executive order aimed at "Improving Critical Infrastructure Cybersecurity" on the eve of his State of the Union address on February 12, 2013.[1] The order is not in and of itself a definitive pronouncement on all the details of the nation's new cybersecurity architecture. Rather, it sets in motion a variety of processes that will lead to significant changes in the way the government deals with cybersecurity. The order also lays out a number of actions the White House is directing executive agencies to take in order to accelerate these changes. A table of those actions is included at the end of this article, and key elements of the order are described briefly below.

Defining "critical infrastructure" broadly, the new order includes several directives to executive agencies, including: (1) requiring the establishment of a process for defining entities that will qualify as "critical infrastructure"; (2) requiring the establishment of procedures for the dissemination of cyber threat information to identified targets, including the dissemination of classified information to entities deemed to be "critical infrastructure" as well as to commercial cybersecurity service providers; (3) requiring the establishment of a "baseline framework" for dealing with cyber threats to critical infrastructure; (4) laying a foundation for future cyber regulations; (5) mandating a privacy and civil liberties assessment of the required actions to be conducted by the senior privacy officials at each relevant agency and coordinated by the Department of Homeland Security's (DHS's) chief privacy and civil liberties officers; and (6) mandating potential revisions to government acquisition and contract administration procedures to incorporate certain security standards.

Identifying At-Risk Critical Infrastructure

The order defines critical infrastructure as:

> systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[2]

The order then mandates that the Secretary of the DHS identify the critical infrastructure "where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[3] This will be done in part through a consultative process with other agencies and with the private sector. The order requires the Secretary to confidentially notify entities that are designated as part of the "critical infrastructure" and permits those entities to request reconsideration of the designation.[4] Significantly, the order specifically excludes "commercial information technology products" and "consumer information technology services" from being designated as critical infrastructure.[5]

Information Sharing Between the Government and the Private Sector

The order envisions that by early summer 2013, certain government agencies will produce procedures for providing unclassified reports about cyber threats "that identify a specific targeted entity" to such targeted entities.[6] The information-sharing proposal also contemplates expanding the Enhanced Cybersecurity Services program, an existing information-sharing program between the government and certain private sector entities.[7] The expansion is intended to open the program to all critical infrastructure sectors.[8] To facilitate the receipt of classified reports by certain entities that are part of the nation's critical infrastructure, the order also mandates that the Secretary of DHS expedite the provision of security clearances for certain eligible employees of those entities.[9] In expediting clearances, the order requires that priority be given to employees of entities designated as constituting the greatest risk under Section 9 of the order.

In addition, the order mandates that the Secretary of DHS expand the use of existing programs to "bring private sector subject-matter experts into Federal service on a temporary basis."[10] The order envisions utilizing these experts to advise the government on the types of information most useful to critical infrastructure entities in addressing cyber risks.[11]

---

[1] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. (Subsequent references to the executive order in these footnotes will read as "order.")
[2] Order, Sec. 2.
[3] Order, Sec. 9(a).
[4] Order, Sec. 9(c).
[5] Order, Sec. 9(a).
[6] Order, Sec. 4(a)-(b).
[7] Order, Sec. 4(c); http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf.
[8] Order, Sec. 4(c); http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0.
[9] Order, Sec. 4(c)-(d).
[10] Order, Sec. 4(e).
[11] *Id.*

Continued on page 11...

Cybersecurity Framework

Another key element of the order is Section 7, which proposes the development of a "cybersecurity framework." According to the White House, the framework will consist of "cybersecurity practices to reduce cyber risks to critical infrastructure."[12] The order delegates the development of the framework to the National Institute of Standards and Technology.[13] It notes that the objective of the standards will be to "align policy, business, and technological approaches to address cyber risks."[14]

Section 7 of the order is likely to be the focus of further discussions. First, the order directs the Secretary of DHS to establish a voluntary program to support and incentivize the adoption of these standards and provides her with significant discretion.[15] Second, the order signals that agencies may utilize the framework to seek additional authority to implement its provisions.[16] Where agency authorities are not adequate to establish such requirements, the agencies are ordered to propose "prioritized, risk-based, efficient, and coordinated actions" to address cyber risks.[17]

The order anticipates that a preliminary version of this framework could be completed by the fall of 2013 and finalized by February 2014.[18]

The order envisions several opportunities for the private sector to influence the process. It orders the Secretary of DHS to establish a formal consultative process so that several constituencies, including critical infrastructure owners and operators, can make recommendations on necessary enhancements to cybersecurity infrastructure.[19]

Finally, in establishing the cybersecurity framework, the order envisions the implementation of a review-and-comment process, perhaps akin to those typically used by rule-making agencies.[20]

Potential Future Regulations

Importantly, the White House has noted that the order could lead to the establishment of new regulations for companies operating key infrastructure.[21] Michael Daniel, a Special Assistant to the President and Cybersecurity Coordinator at the White House, has noted that the order directs certain regulatory agencies to review and align their regulations and requirements with the new cybersecurity framework.[22] Describing this regulatory option as a backstop, Daniel has noted that if companies are "not participating in the voluntary programs for whatever reason . . . those regulators could take action to try to bring their requirements and regulations up to the level of the framework."[23]

Privacy and Civil Liberties

The order also contains a section on privacy and civil liberties.[24] Primarily, the section focuses on mandating a role for certain privacy officials and compliance with "Fair Information Practice Principles."[25] According to the White House, the agencies involved in developing and implementing the actions called for in the order "will conduct regular assessments of privacy and civil liberties impacts of their activities and such assessments will be made public."[26]

Acquisition and Contract Administration

One long-standing government concern has been the security of items in the government supply chain and whether products incorporated into government systems are vulnerable to cyberespionage, sabotage, or other criminal hacking. In a step towards addressing this concern, the order requires recommendations for incorporating security standards into acquisition planning and contract administration.[27] Given the sizeable role of federal government acquisitions in the marketplace, potential changes could have a significant impact on the way that the private sector incorporates cybersecurity into its products and services.

Conclusion

In releasing this order, the Obama administration has initiated a process for the establishment of initially voluntary standards that the White House notes could eventually result in new regulations. Much work remains, however, in identifying the institutions that are understood to fall under the critical infrastructure rubric, developing the standards to which they will be subject, and creating the mechanisms for facilitating information flow between the government and the private sector. The devil, as they say, is in the details—and the details are yet to come.

---

[12] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0.

[13] Order, Sec. 7(a).

[14] *Id.*

[15] Order, Sec. 8.

[16] Order, Sec. 10(a).

[17] Order, Sec. 10(b).

[18] Order, Sec. 7(e).

[19] Order, Sec. 6.

[20] Order, Sec. 7(d).

[21] Jennifer Martinez, "Obama cybersecurity chief warns further regulations may be required," *Hillicon Valley* (February 27, 2013), *available at*: http://thehill.com/blogs/hillicon-valley/technology/285133-cybersecurity-chief-further-regulations-may-be-required.

[22] *Id.*

[23] *Id.*

[24] Order, Sec. 5.

[25] Order, Sec. 5(a).

[26] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0.

[27] Order, Sec. 8(e).

Continued on page 12...

Actions Mandated by the President's Executive Order

Action	**Responsible Parties**	**Section**	**Period** (from 2/12/13, unless otherwise noted)
Issue instructions to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity.	Each of the Attorney General (AG), the Secretary of the Department of Homeland Security (DHS), and the Director of National Intelligence (DNI)	4(a)	120 days
Establish a process that rapidly disseminates reports produced pursuant to 4(a) to targeted entities. The process must also address the dissemination of classified reports to critical infrastructure entities authorized to receive them.	AG in coordination with DNI	4(b)	None given
Establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors.	DHS in collaboration with the Secretary of Defense (DOD)	4(c)	120 days
Submit a report assessing the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in the executive order and making recommendations to DHS on ways to minimize or mitigate such risks. The report will incorporate similar analyses from other relevant agencies.	Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the DHS, in consultation with the Privacy and Civil Liberties Oversight Board and in coordination with the Office of Management and Budget (OMB); in addition, senior agency privacy and civil liberties officials for other agencies engaged in activities under the order will provide information to DHS officials	5(b)-(c)	1 year; annual review
Submit a preliminary draft of the cybersecurity framework.	DNI	7(e)	240 days
Submit a final version of the cybersecurity framework.	DNI in coordination with DHS	7(e)	1 year
Submit annual reports to the President on the extent to which owners and operators notified under Section 9 are participating in the voluntary program to comply with the framework.	Sector-specific agencies (as defined in Presidential Planning Directive-21) through DHS	8(c)	Annually
Create a set of incentives designed to promote voluntary participation in a program aimed at supporting adoption of the framework.	DHS in coordination with unnamed parties	8(d)	None given
Submit recommendation to the President that shall include analysis of the benefits and relative effectiveness of incentives to voluntarily comply with the program referenced above, noting whether the incentives require legislation or can be provided under existing law and authorities.	DHS and the Secretaries of Treasury and Commerce, separately to the President through the Assistant to the President for Homeland Security and Counterterrorism (AHSC) and the Assistant to the President for Economic Affairs (AEA)	8(d)	120 days
Submit recommendations to the President on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration, including what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.	DOD and Administrator of General Services in consultation with DHS and the Federal Acquisition Regulatory Council, to the President through the AHSC and AEA	8(e)	120 days
Identify critical infrastructure, using a risk-based approach, where a cybersecurity incident could reasonably result in catastrophic effects and develop a process for "other stakeholders" to provide input.	DHS, using the consultative process established in Section 6 and drawing on the expertise of sector-specific agencies, to the President through the AHSC and AEA	9(a)-(b); 6	150 days; annual updates thereafter
Confidentially notify owners and operators of critical infrastructure designated under Section 9(a) and establish a process for them to request reconsideration.	DHS in coordination with sector-specific agencies	9(c)	None given
Submit a report to the President stating whether or not the agency has clear authorities (and what they are) to establish requirements based upon the cybersecurity framework to sufficiently address current and projected cyber risks and any additional authority required.	Agencies with responsibility for regulating the security of critical infrastructure, consulting with DHS, OMB, and the National Security Staff, to the President through AHSC, AEA, and Director of OMB	10(a)	90 days after publication of the preliminary framework
Propose prioritized, risk-based, efficient, and coordinated actions to mitigate cyber risk if current regulatory requirements are insufficient.	Agencies with responsibility for regulating the security of critical infrastructure	10(b)	90 days after publication of the final framework
Submit a report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements.	Agencies with responsibility for regulating the security of critical infrastructure in consultation with owners and operators of critical infrastructure	10(c)	2 years after publication of final framework

California Supreme Court Holds Song-Beverly Act Inapplicable to Online Businesses Selling Downloadable Products

Matthew Staples
Associate, Seattle
mstaples@wsgr.com

On February 4, 2013, in *Apple Inc. v. Superior Court of Los Angeles County (Krescent)*,[1] the California Supreme Court held that the Song-Beverly Credit Card Act of 1971,[2] which restricts businesses from collecting personal information in connection with credit card transactions, does not apply to online transactions involving electronically downloadable products.

This article gives a brief overview of the privacy-related provisions of the act and makes note of recent litigation preceding the *Apple* case. It then summarizes the *Apple* decision and provides key takeaways for businesses.

Overview of the Song-Beverly Act's Privacy-Related Provisions

The act places restrictions on businesses requesting or recording certain personal information in connection with credit card transactions. Specifically, in most situations, it prohibits any person, firm, partnership, association, or corporation[3] that accepts credit cards from:

- requesting, or requiring as a condition to accepting the credit card as payment, the cardholder to write any personal identification information upon the credit card transaction form or otherwise;
- requesting, or requiring as a condition to accepting the credit card as payment, the cardholder to provide personal identification information that the business accepting the credit card writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise; and
- using, in any credit card transaction, a credit card form that contains preprinted spaces specifically designated for filling in any personal identification information of the cardholder.[4]

The act defines "personal identification information" as "information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number."[5]

The act's prohibitions on collecting personal information do not apply in some circumstances, including:

- where the credit card is being used as a deposit to secure payment in the event of default, loss, damage, or similar occurrence;
- cash advance transactions;
- where the business is contractually obligated to provide personal identification information in order to complete the credit card transaction;
- where the business accepts a credit card in a sales transaction at a gas station pump or automated cashier and collects personal information solely for the prevention of fraud, theft, or identity theft;
- where the business is obligated to collect and record the personal information by federal or state law or regulation; or
- where collecting the personal information is required for a special purpose incidental but related to the credit card transaction, such as to convey information relating to the shipping, delivery, servicing, or installation of the purchased merchandise, or for special orders.[6]

The act also specifies that it does not prohibit a business from requiring a cardholder to provide reasonable forms of positive identification, such as a driver's license or state ID card (or, if neither is available, another form of photo identification), so long as none of the information on such identification is written or recorded.[7] It provides that if a customer does not make a credit card available upon request to verify the number, the business may record the customer's driver's license or ID card number.[8]

The act contains a private right of action and provides for civil penalties of $250 for an initial violation and $1,000 for each subsequent violation.[9]

The act has served as the basis for several recent class action litigation matters. In February 2011, the California Supreme Court held in *Pineda v. Williams-Sonoma Stores, Inc.* that a ZIP code, on its own, constituted "personal identifying information" under the act.[10] It also stated expressly that its decision applied retroactively.[11] Following this decision, approximately 150 suits reportedly were filed

[1] Case No. S199384 (Cal. Sup. Ct. Feb. 4, 2013), *available at* http://www.courts.ca.gov/opinions/documents/S199384.PDF ("slip opinion").
[2] Cal. Civ. Code § 1747 *et seq.*
[3] For simplicity, these are referred to as "businesses" in this article.
[4] Cal. Civ. Code § 1747.08(a).
[5] Cal. Civ. Code § 1747.08(b).
[6] Cal. Civ. Code § 1747.08(c).
[7] Cal. Civ. Code § 1747.08(d).
[8] *Id.*
[9] Cal. Civ. Code § 1747.08(e), (g).
[10] 51 Cal.4th 524, 534 (2011 WL 446921) (Cal. Sup. Ct. 2011).
[11] *Id.* at 536.

Continued on page 14...

against brick-and-mortar businesses alleging violations of the act relating to the collection of personal information in connection with credit card transactions.[12]

Apple Decision

Shortly after the California Supreme Court's decision in *Pineda*, David Krescent filed a putative class action against Apple alleging that the company had collected a street address and a telephone number as a condition to accepting credit cards for the purchase of media downloads from Apple's iTunes online store. Krescent further alleged that Apple recorded each customer's personal information, was not contractually or legally obligated to collect telephone numbers or addresses to complete credit card transactions, and did not require telephone numbers or addresses for any special purpose incidental but related to credit card transactions, such as shipping or delivery.[13]

Apple filed a demurrer, arguing that the act does not apply to online transactions and that deciding otherwise would undermine the prevention of identity theft and fraud. The trial court overruled the demurrer. Apple filed a petition for writ of mandate seeking review of the trial court's order, which the California Court of Appeals denied. The California Supreme Court granted Apple's petition for review.[14]

The court, finding the text of the statute not dispositive, examined the act's statutory scheme as a whole to determine whether it applies to a transaction that, according to the court, the California legislature had not envisioned.

Quoting *Pineda*, where the court previously had examined the act's legislative history, the court noted that the act's "overriding purpose was to 'protect the personal privacy of consumers who pay for transactions with credit cards,'"[15] and that the California legislature had "sought to address the misuse of personal identification information for [among other things] marketing purposes, and found that there would be no legitimate need to obtain such information from credit card customers if it was not necessary to the completion of the credit card transaction."[16]

The court stated, however, that while California's legislature had enacted the act to protect consumer privacy, it did not do so without regard to exposing consumers and businesses to undue risk of fraud. The court pointed to (i) the California legislature having prohibited the collection of personal identification information by brick-and-mortar businesses only after carefully considering—and rejecting—the possibility that doing so could serve a legitimate purpose such as fraud prevention; and (ii) the act permitting businesses to visually inspect—and, in limited circumstances, record—photo identification in order to combat fraud and identity theft.[17] The court noted that the safeguards against fraud permitted by the act are not available to online businesses selling electronically downloadable products. Unlike brick-and-mortar businesses, online businesses cannot visually inspect the credit card, the signature on the back of the card, or the customer's photo identification.[18]

Accordingly, "[b]ecause the statutory scheme provides no means for online businesses selling electronically downloadable products to protect against credit card fraud," the court concluded that the California legislature could not have intended the act to apply to that category of transactions. The court therefore held that the act does not restrict businesses selling electronically downloadable products online from collecting addresses, telephone numbers, or other information that is not required for completion of the credit card transaction.

Implications

The *Apple* decision undoubtedly is a relief for online businesses, but the scope of the decision is relatively narrow. The court limited its holding by stating that it did not apply to online transactions that do not involve electronically downloadable products or to any other transactions that do not involve in-person, face-to-face interaction between the customer and the business.[19] Further, the court explicitly declined to express a view as to whether the act governs mail order and telephone order transactions.[20] The decision therefore does not provide businesses with clear guidance regarding whether, for example, online transactions involving no delivery of a downloadable good, or in-store purchases at self-service purchase stations, are covered.

The court also invited California's legislature to revisit the issue of consumer privacy and fraud prevention in online credit card transactions.[21] The legislature may clarify the act to provide that it applies in the context of online sales of downloadable electronic goods.

Additionally, businesses should remain aware that various other laws may apply to their collection, use, and disclosure of personal information from consumers. The California Supreme Court, responding to concerns of dissenting justices regarding the protection of consumer privacy, cited two examples—the California Online Privacy Protection Act of

[12] Slip opinion at *20.
[13] Slip opinion at *3.
[14] Slip opinion at *4.
[15] Slip opinion at *9-10 (quoting *Pineda*, 51 Cal.4th at 534).
[16] Slip opinion at *10 (quoting *Asbsher v. AutoZone, Inc.*, 164 Cal.App.4th 332, 345 (2008)).
[17] Slip opinion at *11-12.
[18] Slip opinion at *12.
[19] Slip opinion at *16.
[20] *Id.*
[21] Slip opinion at *25.

Continued on page 15...

California Supreme Court Holds . . . *(continued from page 14)*

2003[22] and the federal Telephone Consumer Protection Act[23]—of state and federal legal regimes protecting the privacy of consumers who submit personal information online.[24] A number of other state and federal laws also impose requirements on online businesses collecting personal information from consumers, as well as on the use and disclosure of such information.

The court's holding also is unlikely to impact ongoing class action lawsuits in which brick-and-mortar businesses are alleged to have violated the Song-Beverly Act by collecting ZIP codes in connection with in-person credit card transactions.

Despite these caveats, however, the *Apple* decision is welcome news for at least one category of online merchants. The decision also indicates that the court may be willing to interpret the act in a manner favorable to defendants, particularly with respect to modern technology that was not contemplated at the time the act was enacted.

[22] Codified at Cal. Bus. & Prof. Code §§ 22575-22579, this statute requires operators of commercial websites to conspicuously post on their websites, and operators of commercial online services to make reasonably accessible, a privacy policy that informs consumers about the categories of personal information collected by the operators and the categories of third parties with which the data is shared. It also contains specified content requirements for such privacy policy.

[23] Codified at 47 U.S.C. § 227 and with implementing Federal Communications Commission regulations at 47 CFR § 64.1200, this statute places restrictions on the use of telephone solicitations, as well as on the use of artificial or prerecorded voice messages, automatic dialing systems, text messaging, and fax messaging.

[24] Slip opinion at *21-24.

Tenth Circuit Finds no ECPA Violation for ISP Using Third Parties to Implement Online Behavioral Advertising

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

The Electronic Communications Privacy Act of 1986 (ECPA), which prohibits the unauthorized interception of electronic communications, has garnered attention as politicians have discussed whether and how to update the aging law for the Internet age. In the meantime, courts are applying the ECPA to situations that were not contemplated by those who drafted the legislation. In *Kirch v. Embarq Management Co.*,[1] the Tenth Circuit applied the ECPA to the practice of online behavioral advertising. The court concluded that an Internet service provider (ISP) does not violate the ECPA when it allows a third party to install a device that collects electronic communications for advertising purposes.

Background

Embarq, an ISP, allegedly authorized an online advertising company, NebuAd, Inc., to collect and use data passing through its network for the purpose of directing online behavioral advertising to Embarq's customers' web browsers. To facilitate this advertising, NebuAd installed hardware on Embarq's network, which allegedly sent some of the data offsite to NebuAd. The plaintiffs sued Embarq and others, alleging that this data collection and use was an illegal interception in violation of the ECPA.[2]

The Electronic Communications Privacy Act of 1986

The ECPA prohibits the interception of "electronic communications,"[3] which include Internet traffic. The ECPA provides for both criminal and civil liability for violators. The prohibition does not apply when the communications are acquired in the ordinary course of business by the provider of the electronic communications service.[4]

The Tenth Circuit's Decision

The Tenth Circuit reviewed two potential theories of liability for Embarq:

1) Direct liability for intercepting communications

2) Indirect liability as an aider and abettor of NebuAd's allegedly unlawful interception

First, the Tenth Circuit observed that under the ECPA, Embarq, as an ISP, is allowed to access the electronic communications of its customers in the ordinary course of its business. The court found that NebuAd's

[1] *Kirch et al. v. Embarq Management Co. et al.*, No. 11-3275 (10th Cir. 2012).

[2] For jurisdictional reasons, the plaintiffs separately sued NebuAd, Inc. in the Northern District of California, alleging several of the same claims as against Embarq. Before the court reviewed the ECPA claims, the parties settled. NebuAd agreed to pay $1.7 million to Internet privacy-related nonprofits and $720,000 to the plaintiffs in fees.

[3] 18 U.S.C. §§ 2511 (4), 2520.

[4] 18 U.S.C. § 2510(5)(a)(ii).

Continued on page 16...

hardware connected to Embarq's network did not provide Embarq with access to any additional electronic communications about Embarq's customers. The only data that Embarq could access was the same data it could access in its role as an ISP. Even if Embarq had control or possession of NebuAd's hardware connected to its network, the court held that the plaintiffs failed to prove that Embarq had obtained access to more communications than it already had. For this reason, the Tenth Circuit concluded that Embarq's access was within the ordinary course of its core business as an ISP.

Second, the Tenth Circuit quickly disposed of the aiding and abetting theory, as it interpreted the ECPA to impose liability only on those who are engaged directly in the violation. In other words, only the entity that intercepted the communication potentially violated the ECPA. Therefore, Embarq could not be liable for any unlawful interceptions by NebuAd.

Implications

The ECPA applies to any company that provides communications services to people, not just Internet service providers. For example, any company that provides network and Internet functionality to employees likely provides a communications service covered by the ECPA. Violations of the ECPA are serious, as criminal penalties are possible. Therefore, companies should thoughtfully assess the implications of any business practices that involve collecting and using data passing through their networks.

Companies may take advantage of certain exceptions to the ECPA to avoid direct liability. As we saw in *Embarq*, communications service providers are given some latitude for their collection and use of the communications data as long as they are accessing such data in their capacity as service providers in their ordinary course of business. In addition, communications service providers may obtain consent from their users to collect and use the data passing through the service for specified purposes. Companies should perform a review of their practices to ensure that they have obtained proper consent or that their actions fall within the ordinary-course-of-business exception before they collect or use data passing over their network.

Under the Tenth Circuit's ruling, communications service providers may not face potential indirect liability from the actions of third parties, even when such companies authorize third parties to collect and use data in a way that potentially violates the ECPA. However, close examination of the law and the company's particular business practices is warranted to assess whether the company's actions could be seen as taking part in the interception. If a court determines that a company participates in the interception, then it faces potential direct liability under the ECPA.

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

650 Page Mill Road, Palo Alto, California 94304-1050 | Phone 650-493-9300 | Fax 650-493-6811 | www.wsgr.com

Austin Beijing Brussels Georgetown, DE Hong Kong New York Palo Alto San Diego San Francisco Seattle Shanghai Washington, DC