Communications Lawyer
Publication of the Forum on Communications Law
American Bar Association
Volume 29, Number 4, June 2013
THE JOURNAL OF MEDIA, INFORMATION, AND COMMUNICATIONS LAW

Mobile Privacy Initiatives and Actions Cloud the Future, Creating a Patchwork Landscape of Policy and Regulatory Prospects

Mary Ellen Callahan, Michael T. Borgia, David M. Didion, and Sabrina N. Guenther

The past year has been both transformative and tumultuous for mobile privacy law. Multiple federal and state agencies have shown a serious interest in the field and have taken some aggressive steps to define what privacy rights consumers have when they use their mobile devices.

Each of these agencies is pursuing the same general goal—to bring some level of definition to the generally nebulous mobile privacy standards for transparency, information sharing, service provision, and data use. But each agency, naturally, has somewhat different regulatory priorities and different legal tools at its disposal. In the absence of a comprehensive nationwide framework, the agencies' efforts have taken a variety of binding and nonbinding forms: policy statements, self-regulatory agreements with mobile platform providers, and civil law enforcement actions and litigation. The result of having multiple independent government actors using varying strategies to regulate the same activities has been predictable: a confusing regime for companies to navigate, whether as communications providers or as content providers through mobile applications. Only the area of children's privacy potentially provides regulatory clarity on how to interact with consumers via mobile devices, but even those regulations have expanded greatly in the last year and may be subject to challenge in litigation.

Despite the sometimes chaotic nature of the mobile privacy landscape, several key trends have emerged from the past year's major mobile privacy initiatives. First, as in many other areas of consumer protection law, the foundational principle for mobile privacy is informed consumer choice through disclosure. In general, the recent mobile privacy initiatives have been intended not to prohibit particular collection methods or uses of consumer data, but rather to require companies to disclose their activities in explicit, consumer-friendly ways. The goal of these initiatives has been to give consumers the ability to make more informed choices when they decide whether to provide their personal data.

A second trend has been the expansion of the type of data that is considered "personally identifiable information." Both federal and state actors have worked to push the definition of personally identifiable information or individually identifiable information beyond the traditional categories such as name, e-mail and street address, and telephone number, to more advanced types of data like geolocation and IP address. Geolocation has received an especially large amount of attention because of both its significant implications for user privacy and its usefulness to companies who want to market local vendors and services to consumers.

A third major trend has been increased attention to third-party data collection and use. This partly is an offshoot of regulators' focus on consumer choice and disclosure, as third parties present a particular challenge for ensuring that consumers understand when and how their information is used. When consumers provide personally identifiable information to a mobile application branded by one company, they may be completely unaware that third parties also may be collecting and using those data. This trend also highlights an explicit recognition by regulators that the mobile ecosystem is both exceedingly complex and interrelated. App developers often borrow third-party code from advertising networks and other sources, code that the developer may not fully understand. Such code may collect user information and pass it directly onto third parties. The Federal Trade Commission (FTC) and other regulators have

expressed hopes that these developments can trickle down and eventually force each layer of the mobile ecosystem to become more aware and transparent with one another.

This article will first discuss the recent mobile privacy initiatives, and then provide an analysis for companies and industry on what is necessary to know about these recommendations.

Recent Major Mobile Privacy Initiatives *California Attorney General-CalOPPA*

Perhaps no one is more responsible for the past year's swell of activity on mobile privacy than California Attorney General Kalama Harris. Since entering into an agreement with major mobile app platform providers—such as Apple and Google—in February 2012,[1] Harris's office has led the way among both federal and state regulators in pushing for greater transparency and uniformity in how mobile app developers use consumers' personally identifiable information.

Harris has been able to leverage what no other state or federal regulator can—legislation that applies to all consumers (not just children, as with the federal law, COPPA) and addresses what kind of information companies must disclose about their collection and uses of consumers' personally identifiable information and the format in which companies must make those disclosures. The California Online Privacy Protection Act of 2003 (CalOPPA) requires an "operator of a commercial Web site or online service that collects personally identifiable information" to "conspicuously post" a privacy policy concerning its collection and use of personal data.[2] The privacy policy must disclose the categories of personally identifiable information collected by the site operator and by any third parties when the user visits the site.[3] Harris has taken the position that a company's mobile app is a "commercial Web site or online service" under CalOPPA, although that stance has not yet been decided by a court.

Although technically specific to California residents, in practice CalOPPA's reach is nationwide. The Act applies to any website or online service that collects the personal information of California consumers,[4] and therefore effectively governs every website (and, according to Harris, every mobile app) operating in the U.S. market. CalOPPA has allowed Harris to reach far beyond California to influence the national debate about mobile privacy norms.

Harris has pushed for stronger consumer-centric mobile privacy rules—rules seeking to ensure that apps deliver pertinent information about how they use personal data when delivery is most convenient and useful to consumers. She has pursued that initiative using a variety of methods. Harris's first major step was to sign a "Joint Statement of Principles" with the seven major providers of mobile app platforms (i.e., mobile app stores and other centralized locations where users can search for and download mobile apps). The Joint Statement sets out standards for how apps offered on those platforms should disclose their collection and use of personal information to consumers. Six platform providers—Amazon, Apple, Google, Hewlett-Packard, Microsoft, and Research in Motion—signed the agreement in February 2012, and the seventh—Facebook—joined the agreement that June.

Under the Joint Statement, the platform providers agreed to supply optional data fields in which developers can post their mobile apps' privacy policies—or hyperlinks to those policies—when the developers submit a new or updated app for inclusion on the platform. When an app's developers elect to use those optional fields, the platform providers agree to provide consumers with access to the privacy policy or hyperlink from within the app platform—in other words, before the consumer downloads the app.

Although the Joint Statement is not binding law by its own terms, it illustrates how the attorney general would like to see mobile apps disclose their collection and use of personally identifiable information—specifically, by presenting consumers with a privacy policy before the app is downloaded, and thus *before* the app can begin collecting personal data. The Joint Statement may even provide insight into Harris's interpretation of what mobile app developers must do to comply with CalOPPA's requirement that they "conspicuously post" a privacy policy. The Act, which was written with more traditional web interfaces in mind, generally requires an "online service" to make its privacy policy accessible from a homepage or through "any other reasonably accessible means."[5] It may be Harris's position that this requirement, when applied to mobile apps, means that apps must post their policies before the app is downloaded, or at least must make it readily accessible before the consumer begins to use the app's core functions.

Following the Joint Statement, Harris shifted her attention to enforcement. In July 2012, she announced the creation of a Privacy Enforcement and Protection Unit charged with enforcing CalOPPA and other state and federal privacy laws. On October 30, 2012, the attorney general's office issued a press release announcing that it had begun to send letters to mobile app developers notifying them that their apps failed to conspicuously post a privacy policy in violation of CalOPPA. The press release stated that the attorney general's office was issuing noncompliance notices to the developers of as many as 100 apps, starting with the most popular. The letters gave the developers 30 days to modify their apps to comply with the law or face legal action.

The attorney general's office quickly followed through on its threat when it sued Delta Airlines for allegedly violating CalOPPA with its Fly Delta mobile app by failing to make its privacy policy readily accessible from anywhere in the app. Delta defended itself with the argument that CalOPPA was preempted by the federal Airline

Deregulation Act—an act that prohibits states from enacting or enforcing laws or regulations related to the price, route, or service of air carriers—as well as making a secondary argument that the term "online service" in CalOPPA can only mean technology that existed at the time the law was enacted.[6] On May 9, 2013, the trial court sided with Delta and dismissed the attorney general's suit without reaching the interpretation questions; instead the court issued a terse opinion that took Delta's draft motion in toto and therefore was most likely persuaded by Delta's primary preemption argument.[7] To date, the Delta suit remains the only action brought by Harris's office to enforce CalOPPA. But the attorney general is almost certainly not deterred. The Delta dismissal left California with no impediment to future suits, as long as they are not against airlines.

Harris's intention to push the mobile app industry toward a more consumer-centric approach to privacy is perhaps most apparent from the comprehensive mobile privacy recommendations her office released earlier this year. The recommendations, entitled *Privacy on the Go*, primarily target mobile app developers but also provide guidance for other relevant parties, including advertising networks and app platform providers.[8]

As with the Joint Statement, the attorney general's recommendations encourage app developers to make privacy policies accessible to consumers before the application is downloaded.[9] The recommendations go even further, however, by suggesting that developers supplement their general privacy policies with "just-in-time" special notices—notices that appear while the app is being used—to warn consumers about collection or use of personal data that is unexpected or especially sensitive, or that will be shared with third parties.[10] More generally. *Privacy on the Go* recommends that app developers limit collection, use, and retention of personal information to what is necessary for the app's core functions.[11] Among the more onerous recommendations, the California attorney general recommended that all personal information—including e-mail address, phone number, and the mobile device's MAC address (an ID number unique to each device)—be encrypted in transit and in storage.[12]

The FTC's Best Practices Recommendations and the HTC Consent Decree

In February 2013, the FTC offered up its own mobile privacy recommendations—*Mobile Privacy Disclosures: Building Trust Through Transparency*—which raised the stakes for platforms, app developers, third parties (such as ad networks and analytics companies), and app trade associations.[13]

These FTC mobile recommendations mostly focus on disclosure. They have a narrower scope and are not as prescriptive as the California attorney general's guidelines—for example, they have no encryption or deletion requirements. Although the recommendations extend beyond the current federal law, they may set a new baseline for potential exposure to enforcement actions—especially where they overlap with the California guidelines.

Specifically, the FTC recommends the following privacy practices for app developers:

- **Notice via Privacy Policy**: App developers should have a privacy policy and make sure it is easily accessible through the app stores.[14]
- **Just-in-Time Notices and Consent for Sensitive Data Collection and Sharing**: App developers should provide "just-in-time" disclosures—warnings that appear while the consumer is using the app just before specific data are collected—and obtain affirmative express consent before collecting or sharing with third parties sensitive information such as financial, health, or children's data. The recommendations also specify that platform providers (for example, companies like Apple and Google that host app stores) should issue just-in-time disclosures (and seek user consent) when apps access "sensitive" content such as geolocation information, photos, contacts, calendar entries, or the recording of audio or video content.[15] Because app developer disclosures should not overlap with platform disclosures, this may require platform/developer coordination.
- **Sensitive Information**: The recommendations do not define terms, but it may be reasonable to assume that, for example. sensitive geolocation corresponds to the definition the FTC adopted in COPPA—namely, geolocation at the city and street level.
- **Understanding Third-Party Data Access and Code**: App developers need to improve coordination and communication with ad networks and other third parties, such as analytics companies, that provide services for apps so the app developers can provide accurate disclosures to consumers.[16] The FTC seems to be signaling here that it will hold app developers more accountable for integrating third-party code—which may facilitate advertising or analytics within an app—into their apps without first understanding what information the third party is collecting and how the information is being used.

The FTC also introduced the concept of a "do not track" for mobile devices, which is the first time it has suggested such a practice for mobile devices. To the extent that individual app developers use third-party ad serving or analytics, there may need to be structural changes to that process in the midterm future.

On the heels of these recommendations, the FTC released a consent decree in its first enforcement action against a mobile device manufacturer in early 2013. In its complaint against HTC America, Inc. (HTC), a manufacturer of Android mobile devices, the FTC charged HTC with three counts of unfair and deceptive business practices.[17] According to the FTC, HTC had

introduced several security lapses when it customized the Android software for its mobile devices. These lapses allowed third-party app developers to circumvent the devices' permissions-based security system and download information-gathering apps and other software without consumer consent. In its first count, the FTC charged that HTC's failure to implement reasonable security measures to protect sensitive information contained in and transmitted by its mobile devices, coupled with these security lapses, amounted to an unfair business practice. In its second and third counts, the FTC charged that HTC had engaged in deceptive business practices by misrepresenting its permissions-based security system and by misrepresenting the location information provided to HTC when consumers reported device errors. Notably, HTC's deceptive statements were in its owner's manual, not in a privacy policy; therefore, companies should evaluate any public statements to evaluate materiality and the potential for deception.

The terms of the February 22, 2013, consent decree with HTC emphasize implementing prevention measures and adequate information security protocols, rather than just remedying the specific software inadequacies alleged in the FTC's complaint. Under the decree, HTC must, among other remedies, implement a comprehensive written security program designed to address security risks related to HTC's new and existing covered devices,[18] and to protect the security, confidentiality, and integrity of covered information collected by HTC or input into, stored on, captured with, accessed, or transmitted through a covered device.

The consent decree defined the "covered information" that HTC agreed to protect far more broadly than traditional PII—first and last names, e-mail and street addresses, telephone numbers, or other contact information for specific individuals (notably, the FTC did not use the term "personally identifiable information" in this consent decree). The "covered information" includes persistent identifiers, such as a customer number held in a "cookie," static IP addresses or a mobile device's ID numbers, geolocation data, and a seemingly boundless catchall encompassing "any other communications or content that is input into, stored on, captured with, accessed or transmitted through a covered device, including but not limited to contacts, emails, text messages, photos, videos, and audio recordings."[19] The catchall provision could extend to almost all information on a particular mobile device.

However, the consent decree explicitly does not require HTC to identify and correct security vulnerabilities in third parties' software on covered devices to the extent the vulnerabilities are not the result of HTC's integration, modification, or customization of the third-party software.

NTIA Multistakeholder Process for Mobile App Transparency

A final voice in this ongoing state and federal cacophony emerged in June 2012, when the National Telecommunications and Information Administration of the Department of Commerce (NTIA) announced that, as part of its support for the White House-endorsed *Consumer Bill of Rights*,[20] it would begin hosting a multistakeholder process designed to develop a code of conduct for how companies providing mobile apps can effectively communicate how those apps handle personal data. Although the agency is overseeing this process, players and stakeholders from across the industry actually are drafting the code. The process has focused on crafting a voluntary code that provides guidelines for a "short-form" notice that app developers eventually can implement. The draft code is still in flux as of May 2013, but the reasoning behind the initiative is to provide greater transparency for consumers so that they can make better privacy-driven choices when they download mobile apps. Despite its malleability, the draft code has always focused on disclosure, on requiring the developers who sign on to identify whether their app collects certain sensitive personally identifiable information and whether it shares personally identifiable information with certain types of outside entities. As of May 2013, the categories of sensitive information have been stable for some time, and include biometrics, browser history or phone/text history, contacts, financial information, health information, location, and user files.

Legislators also have taken notice. In May 2013. Representative Hank Johnson introduced a bill—the Application Privacy, Protection, and Security Act of 2013—where NTIA's code, whenever it is completed, can potentially serve as a safe harbor.[21] The FTC, too, has informally suggested— through staff members at several NTIA meetings—that it may view a strong code of conduct as a de facto safe harbor from certain (but not all) Section 5 claims. Many stakeholders have some hope that the code eventually will provide a floor for app privacy disclosures and will contribute to consumer protection and education. But, despite its avowed voluntary nature, legislators and regulators have kept a close eye on the proceedings and, if they ever give birth to a strong consensus-christened code, that code easily could play a role in other regimes.

COPPA

The past year also carried an avalanche of FTC activity in children's privacy, culminating with the Commission releasing the first significant changes to its Children's Online Privacy Protection Act (COPPA) Rule in 12 years, changes that closely followed an unprecedented pair of privacy reports on mobile apps for kids. COPPA and its implementing Rule protect the personal information of children under the age of 13 by requiring parental consent and other precautions from operators of Internet sites or apps who target children—or who have actual

knowledge that they are collecting information from children. Originally implemented in 2000, the FTC initiated updated rulemaking proceedings in 2010, reasoning that significant updates to the COPPA Rule may be necessary in light of the recent rapid technological changes online.

Shortly before releasing its updated COPPA Rule, the FTC twice surveyed available apps aimed at kids. The Commission hoped to assess what information developers provide to parents about their privacy practices or about the apps' interactive features. The FTC's February 2012 report found that the mobile apps surveyed made little or no information available to parents about their privacy practices and interactive features prior to download.[22] The FTC's follow-up report in December 2012 (shortly before the release of the final revised Rule) found little change and criticized children's app developers for their failure to meaningfully improve privacy practices.[23]

On December 19, 2012, the FTC released its updated COPPA Rule, amending the definitions of "operator," "personal information," and "website or online service directed to children" and updating the requirements for notice, parental consent, confidentiality and security, and the safe harbor provisions.[24]

Some of the most significant changes included clarifying the definition of a covered "operator"—expanding it to include those sites or apps that incorporate third-party online services (such as plug-ins or advertising networks) that in turn collect personal information directly from users—and explicitly sparing app stores themselves from coverage.[25] The new Rule also expanded and clarified the types of "personal information" that trigger the parental consent and heightened protection requirements (for use other than delivering the service) to include (1) geolocation information at the city and street level; (2) persistent identifiers such as IP addresses, MAC addresses, device identifiers, and cookies; and (3) online contact information such as an instant messaging user identifier, a VoIP identifier, or a video chat user identifier. Finally, the new Rule added new parental consent mechanisms—including electronic scans, video verification, government-issued identification, and credit card information or online payment systems used in a monetary transaction—and retained the "email plus" consent method, which allows an operator to satisfy the parental consent requirement through e-mail with some additional step, but only when collecting personal information exclusively for internal use.

These changes will become effective July 1, 2013, provided the Rule is not challenged in court and its implementation stayed.

In the meantime, the FTC repeatedly has signaled its intentions to pursue mobile device COPPA violations, and it sounded the opening charge in February 2013 with the release of its Path Consent Decree.[26] Path, Inc.—a social networking app that allows users to create and share online journals—agreed to the decree's terms after the FTC alleged that Path's practices violated Section 5 of the FTC Act by engaging in deceptive trade practices,[27] and that it violated COPPA and Section 5 by collecting children's information without notice and without verifiable parental consent. The FTC invoked COPPA's statutory damages to impose an $800,000 civil penalty on Path, and implied that the combination of children and deception made the alleged violations particularly troubling. Indeed, considering that the FTC pledged in its December 2012 app privacy report to launch "multiple nonpublic investigations" into COPPA compliance, more such decrees could appear before the updated Rule is slated to become effective.

Analysis

Mobile Transparency Is the First, and Sometimes Last, Priority

The overarching theme in the disparate privacy regimes has been the same as in other areas of consumer protection; disclosure and transparency. The administration's *Consumer Bill of Rights*, for example, identified seven principles, and highlighted transparency as a cornerstone element.

The FTC repeatedly has signaled its intentions to pursue mobile device COPPA violations.

Transparency has been arecurring theme among regulators: how best to describe what activities are taking place on the device, including data collection, use, and sharing; secondary use of information; and data retention. The California attorney general joined the swell of mobile privacy transparency advocates when she released recommendations for mobile app developers and other mobile players early in 2013. While some recommendations—for example, those dealing with data protection—are substantive, the bulk of California's suggestions deal with disclosures, a trend that unsurprisingly dovetails with CalOPPA's own bent towards increasing consumer transparency simply by requiring privacy policies. The FTC also recently entered the transparency debate with its best practice recommendations and its series of consent decrees that focused on deception. Finally, NTIA has brought together stakeholders from throughout the mobile ecosystem in a process that explicitly hopes to find consensus on what mobile apps should disclose about how they use consumer information.

Many transparency guidelines take a consumer-focused approach by recommending that apps prioritize disclosing data uses that a typical consumer would find surprising or troubling.

The FTC defined precise geolocation in its amended COPPA Rule as geolocation at the city and street level.

California suggests disclosures when apps do surprising or unexpected things with consumer data, [28] and the FTC similarly has suggested disclosing practices that violate consumer expectations, in addition to practices dealing with specific "sensitive" information.[29] These types of recommendations ask developers to disclose when their practices meet (or fail to meet) certain consumer-protective functional standards or guidelines, rather than asking the developers to identify specific categories of information they collect or entities with which they share such information. But these same regulators also are willing to request disclosure for the specific data they find most important, such as those elements in the expanding definitions discussed below. Similarly, NTIA's process has long focused on a category-centric approach for disclosure—requesting disclosure of data practices that fall into specified buckets—rather than a functional one. COPPA, too, relies heavily on categories when setting requirements for children's personal information. As regulators shift away from guidelines and closer to regulations or laws, they may well create more of a categorical approach to transparency more akin to these latter two processes, perhaps in part out of practical concerns for how members of the mobile ecosystem will operationalize the requirements as well as concerns about how to judge compliance. The details of these categories may shape not only transparency, but also more substantive requirements for data protection, so the continued evolution of the definition of personally identifiable or individually identifiable protected information becomes ever more important.

Expanding the Definition of Protected Information for Mobile Devices

Personally identifiable information traditionally protected under the law includes first and last names, e-mail and street addresses, telephone numbers, or other contact information for specific individuals. But, in their recent mobile privacy initiatives, the FTC and other regulators have expanded the definition of sensitive or protected information beyond these traditional categories.

For example, all of the FTC's recent reports, guidelines, and enforcement actions have defined sensitive or covered information to include geolocation. The California mobile privacy best practices guidelines also included geolocation as sensitive. The FTC succinctly expressed its concern about the role of such information in its recent report on mobile payment systems:

> In the mobile context, unique features of a mobile phone, such as the ability to store and transmit precise geolocation information, facilitate unprecedented levels of data collection. This only heightens the need for companies to implement reasonable data collection and security practices.[30]

Although not all of the reports and enforcement actions have specified the level of geolocation they found sensitive, the FTC defined precise geolocation in its amended COPPA Rule as geolocation at the city and street level.[31] This expansion arguably is the most significant for mobile application companies, which often use geolocation information to market their products more effectively or to allow third-party advertising services to do the same. The FTC and the California attorney general also have expanded sensitive information to include persistent identifiers, such as IP addresses, and consumers' user names for applications, social media sites, and instant messengers. The California attorney general recommended encryption for transmission of all such information.[32]

In its consent decree with HTC, however, the FTC introduced the broadest category of sensitive information yet. The decree defined "Covered Information" to include, among other things, a catchall category: "any other communications or content that is input into, stored on, captured with, accessed or transmitted through a covered device, including but not limited to contacts, emails, text messages, photos, videos, and audio recordings." The FTC's complaint against HTC also suggests that the FTC may seek protections for information such as users' and their contacts' phone numbers; the size, number, and content of text messages; GPS-based location information; digits dialed by the user; the users' web-browsing and media-viewing history; International Mobile Equipment Identity or Mobile Equipment Identifier; registered account user names and passwords; and the names of applications on the user's device.[33] Thus, the FTC potentially has begun to carve out a much broader definition of protected information at risk in the mobile industry.

On top of this "regulatory" creep of legislating standards by consent order, future studies and research may lead to unexpected new categories of sensitive information, or to a new urgency over the risk posed by certain types of information. For example, a recent study showed that knowing four spatio-temporal points—that is, knowing where an individual generally was located at four random points in time, specified to the hour—was enough to uniquely identify 95 percent of people from a database containing fairly coarsegrained traces of past geolocation data from over 1.5 million individuals.[34] Studies like this eventually could encourage regulators to look beyond merely "precise" geolocation for their privacy concerns. Other studies might conceivably lead regulators to focus on a new type of sensitive information, or on a sensitive *combination* of otherwise innocent data. The FTC's growing concern over device IDs was born in part from studies and surveys that purported to show such IDs could be (or become) a privacy risk. History easily could repeat itself as new studies find new potential data nexuses that might identify individuals or devices.

The recent enforcement actions above demonstrate a clear trend of expanding the types of information potentially subject to protection. The increased scope of potentially protected or sensitive information, coupled with arguably inconsistent "recommendations" from regulators, increases the scope and breadth of potential enforcement actions as companies continue to access, collect,

and use these data. Therefore, companies should consider whether collecting and using the types of information included in the expanded definitions above are necessary to their business models. If so, they should affirm that their mobile privacy practices comply with each regulator's recommendations.

The Risks of Third-Party Involvement

As recognized during the FTC's December 2012 online privacy workshop, companies increasingly are relying on consumer information gathered by third parties for targeted advertising. Third parties often gather consumer information by redirecting consumers to intermediary sites that record the links clicked, by setting cookies, and by other plug-ins and widgets. In addition, companies frequently incorporate third-party code necessary to gather this information or to facilitate advertising or analytics within their own apps, devices, or other products. Consumers, however, remain largely unaware of these practices and of companies' technological capabilities in general.

Amid these industry conditions, the FTC has indicated a growing concern about incorporating thirdparty code and allowing third-party access to sensitive information. Each of its recent reports and enforcement actions in some way addressed this issue. For example, in its February 1, 2013, best practices recommendations for mobile privacy, the FTC urged app developers to provide just-intime disclosures to—and obtain affirmative consent from—consumers before collecting or sharing with third parties the consumers' sensitive information.[35] In addition, the FTC said platform providers should provide just-in-time disclosures to—and obtain consent from—consumers when apps access sensitive mobile content.[36] In order for these consumer disclosures to be accurate, app developers will need to improve coordination and communication with ad networks and other third parties. These recommendations signal that the FTC may hold app developers more accountable when those developers integrate third-party code with little understanding of what information the third party is collecting and how the third party is using that information.

The FTC's complaint against and consent decree with HTC further demonstrate that allowing third parties to access sensitive information without consumer consent can result in an enforcement action. The FTC's allegations against HTC emphasized how HTC had exposed its consumers to unauthorized *third-party* access in its attempt to customize its Android devices.[37] According to the FTC, this exposure to third-party data collection and HTC's failure to monitor and control for such unauthorized access amounted,to an unfair business practice subject to FTC enforcement.[38] Importantly, however, the FTC stopped short of requiring HTC to identify and correct security vulnerabilities in third parties' software to the extent the vulnerabilities were not caused by HTC's integration, modification, or customization of the third-party software. Thus, the consent decree shows both the potential breadth of and limits to companies' responsibility for third-party actions. Based on these developments, consumer-facing companies should anticipate increasing accountability for third parties' data collection and sharing activities. Companies should consider the benefits and risks associated with third-party involvement in their products. If a company chooses to incorporate third-party code or services, it not only should understand the code and the third parties' activities, it also should consider notifying or obtaining consumer consent for those activities. Moreover, the company should work with the third party to ensure its privacy policies and disclosures are accurate and complete.

The Continued Role of the States

The continued lack of a comprehensive federal legal regime for mobile privacy will allow California to maintain a lead role in shaping laws and industry norms. California may continue to take an aggressive approach to mobile privacy without worrying that its laws will be preempted by federal rules.[39] However, while no federal legislation currently is on the horizon, an especially aggressive approach by California's legislature and its attorney general could prompt a congressional response. The federal Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, more popularly known as the CAN-SPAM Act, provides a useful illustration. The Act was passed by Congress after the California legislature enacted an "opt in" regime for e-mail marketing. CAN-SPAM generally preempts state laws governing the use of e-mail to send commercial messages.[40]

Consumer-facing companies should anticipate increasing accountability for third parties' data collection and sharing activities.

Depending on how aggressive, or contradictory, state legislative regimes become, the attractiveness of enacting a federal mobile privacy regime that preempts state law may increase.

On the other hand, the lack of a federal regime may limit the role of other states' attorneys general in shaping mobile privacy rules because there is no federal foundation on which states can build. Other regimes allow states to piggyback off existing federal laws. For example, under the Consumer Financial Protection Act of 2010 (part of the Dodd-Frank Wall Street Reform and Consumer Protection Act), states may bring actions to enforce regulations promulgated by the federal Consumer Financial Protection Bureau.[41] Additionally, many states provide that their own consumer protection laws should be interpreted in light of what has been found to violate the Federal Trade Commission Act. Some federal privacy laws, such as COPPA and CAN-SPAM, directly grant enforcement authority to state attorneys general. Although state laws could be used to mirror the FTC's enforcement strategy, they would not allow state attorneys general to follow California's enforcement actions, including suits

against companies that fail to post readily accessible privacy policies, except under an "unfair or deceptive trade practices" theory. Federal-state coordinated legislative regimes grant state attorneys general considerable enforcement authority even where state laws or regulations are lacking. At this point, however, most state attorneys general are limited to using either their own unfair and deceptive practices legislation or specific statutes such as COPPA.

Communications companies and mobile app providers face a great deal of uncertainty when navigating the chaos of the mobile privacy landscape.

Navigating Uncertain Regulatory Environment

Communications companies and mobile app providers face a great deal of uncertainty when navigating the chaos of the mobile privacy landscape. The ever-changing nature of the law and the technology itself make it impossible for companies to fully map out the best route forward. But regardless of where mobile privacy law moves, two strategies are advised: ensure that your company's privacy practices comport with standard industry practices and actively monitor new developments at both the federal and state levels.

Companies must pay particular attention to where they stand with regard to the three emerging themes of mobile privacy identified. After all, these themes have emerged because regulators have been especially committed to them. First, companies must ensure that they are fully disclosing their privacy practices to consumers in consumerfriendly ways. Detailed privacy policies must be accessible from mobile apps, ideally before an app is downloaded.

Second, companies should give careful consideration to their use of geolocation technology, as this is certain to remain an area of serious interest for regulators. In every recent policy discussion and regulatory initiative, geolocation—city and street—has been considered sensitive information, and regulators are encouraging noncarriers in the mobile ecosystem to use geolocation only with affirmative consent. Companies should consider seriously whether real-time geolocation is integral to their business models; if so, building in affirmative consumer consent is a very good idea.

Third, companies must be intimately aware of how their apps are using third-party code and plug-ins. Both the California attorney general and the FTC want those relationships clearly disclosed, and might possibly seek to limit third-party data collection and use in the future. Although much of the attention thus far has been on ensuring that those relationships are disclosed, companies should expect to see the "next generation" of enforcement actions focusing on deceptive activities—in other words, examining whether the apps actually are doing what they say and living up to the disclosed promises.

The mobile landscape for privacy is undulating, with no sign of slowing down. Companies must pay attention. They need to be aware of the regulatory guidance and their own mobile activities to avoid a civil law enforcement investigation or a noncompliance litigation.

Mary Ellen Callahan is a partner and chair and founder of the privacy and information governance practice at Jenner & Block LLP and was the chief privacy officer of the U.S. Department of Homeland Security from 2009-12. She can be reached at mecallahan@jenner.com

Michael Borgia and David Didion are associates in the Washington, DC office of Jenner & Block. They can be reached, respectively, at mborgia@jenner.com and ddidion@jenner.com.

Sabrina Guenther is an associate in the Chicago office of Jenner & Block. She can be reached at sguenther@jenner.com

Endnotes

1. Press Release, Office of the Att'y Gen., Cal. Dep't of Justice, *Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications* (Feb. 22, 2012), *available at* https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-securesglobal- agreement-strengthen-privacy.

2. CAL. BUS. & PROF. CODE § 22575(a) (West 2008).

3. *Id.* t (b)(1).

4. *Id.* at (a).

5. *Id.* §22577(b)(lH5).

6. Dem. to Compl. at 2, *People v. Delta Air Lines Inc.*, No. CGC 12-526741 (Cal. Super. Ct. Feb. 11,2013).

7. Order Sustaining Def. Delta Airlines, Inc.'s Dem. to Compl., *People v. Delta Air Lines Inc.*, No. CGC 12-526741 (Cal. Super. Ct. May 9, 2013), *available at* http://webaccess.sftc.org/minds_asp_pdf/ mainpage.asp?Web_Server=webaccess. sftc.org&MINDS_Server=ntimagex&Category=C&DocID=04049258.

8. OFFICE OF THE ATT'Y GEN., CAL. DEP'T OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (Jan. 2013), http://oag. ca.gov/sites/all/files/pdfs/privacy/ privacy _on_the_go. pdf.

9. *Id.* at 2, 9.

10. *Id.* at 5.

11. *Id.* at 2, 9.

12. *Id.* at 15.

13. FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (Feb. 2013), http://www.ftc.gov/os/2013/02/130201 mob ileprivacyreport.pdf.

14. *Id.* at ii.

15. *Id.* ati-ii.

16. *Id.* at ii-iii.

17. Complaint, *In re HTC Am.*, Docket No. C-122 3049 (Feb. 22, 2013), *available at* http://ftc.gov/os/ caselist/1223049/130222htcempt.pdf.

18. The consent decree defined "covered device" to include "any desktop computer, laptop computer, tablet, handheld or mobile device, telephone, or other electronic product or device developed by respondent or any corporation, subsidiary, division, or affiliate owned or controlled by respondent that has a platform on which to download. install, or run any software program, code, script, or other content and to play any digital audio, visual, or audiovisual content." Agreement Containing Consent Order, In re HTC Am., File No. 122 3049 (Feb. 22, 2013), *available at* http://ftc.gov/os/ caselist/1223049/130222hteorder.pdf.

19. *Id.*

20. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (Feb. 2012), http://www.whitehouse.gov/sites/default/ files/privacy-final.pdf. The Consumer Bill of Rights includes Individual Control, Transparency, Respect for Context, Security, Access and Accuracy, Focused Collection, and Accountability.

21. H.R. 1913. 113th Cong. §5(2013), http.7/beta.congress.gov/113/bills/hrl913/ BILLS-113hrl913ih.pdf.

22. FED. TRADE COMM'N, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING (Feb. 2012), http://www.ftc.gov/os/2012/02/120216mobile„ apps_kids.pdf. *See also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (Mar. 2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

23. FED. TRADE COMM'N, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE (Dec. 2012), http://www.ftc. gov/os/2012/12/1212 lOmobilekidsapp report.pdf.

24. Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972 (Jan. 17, 2013) (amending 16 C.F.R. pt. 312).

25. *Id.* at 3977.

26. Consent Decree and Final Order, *United States v. Path, Inc.,* Case 3:13-cv- 00448-RS (Feb. 8, 2013), *available at* http://www.fte.g0v/0s/caselist/l 223158/130 201pathincdo.pdf.

27. Under 15 U.S.C. § 45, "unfair or deceptive acts or practices" are illegal. The FTC uses its Section 5 authority to bring privacy enforcement actions against companies, either in conjunction with statutory violations (such as COPPA) or for stand-alone enforcement actions or consent decrees.

28. PRIVACY ON THE GO , *supra* note 8, at 5.

29. MOBILE PRIVACY DISCLOSURES, *supra* note 13, at 15-16, 19.

30. FED. TRADE COMM'N, PAPER, PLASTIC . . . OR MOBILE? AN FTC WORKSHOP ON MOBILE PAYMENTS (Mar. 2013), http://www.ftc.gov/os/2013/03/130306mobilereport.pdf.

31. Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 4009 (Jan. 17, 2013) (amending 16 C.F.R. pt. 312).

32. PRIVACY ON THE GO , *supra* note 8, at 10, 15.

33. Complaint, *supra* note 17, at 3-4.

34. *See* Yves-Alexandre de Montjoye, Cesar A. Hidalgo, Michel Verleysen & Vincent D. Blondel, *Unique in the Crowd: The Privacy Bounds of Human Mobility,* SCI. REP. (Mar. 25, 2013), *available at* http://www.nature.com/srep/2013/130325/ srep01376/full/srep01376.html.

35. MOBILE PRIVACY DISCLOSURES, *supra* note 13, at 23.

36. *Id.* at 15-16.

37. Complaint, *supra* note 17, at 1-A.

38. *Id.* at 7.

39. Even very recently, California legislators have continued to take a bold approach to privacy and consumer data rights. For example, in February 2013, California Assembly Member Lowenthal introduced the Right to Know Act of 2013, which, if enacted, would provide a consumer with an EU-like right to demand all of that consumer's "personal information" (defined to closely resemble the HTC "covered information" definition) retained or disclosed by any given business that has a relationship with that consumer. *See* Right to Know Act of 2013, Cal. Assembly Bill No. 1291 (Feb. 22, 2013). Although the Right to Know Act was withdrawn from legislative consideration in May 2013, such aggressive bills, if they become enacted, could find themselves quickly attracting federal interest.

40. 15 U.S.C. § 7707(b)(1) (2012).

41. 12 U.S.C. § 5552(a).