Is There a Privacy Policy for That App?

Tanya Forsheit*

I. Introduction

Many predictions for 2013's hot topics in privacy law revealed a common theme—mobile apps and California's Attorney General Kamala Harris.[1] Why? Ms. Harris made clear through numerous actions in 2012 and early 2013 that she takes mobile app privacy very seriously and will use her office to educate and enforce appropriate privacy practices in the mobile app world. Organizations across the country should take note because Ms. Harris interprets the California law she seeks to enforce as applying to any app that collects personally identifiable information from a California resident.

The following article explains what the California fuss is all about, and what it means for app developers, any organization that has an app, and other players in the app ecosystem.

---

* Tanya L. Forsheit is a Founding Partner of InfoLawGroup LLP and a former partner with Proskauer, where she was Co-Chair of that firm's Privacy and Data Security practice group. She is the immediate past President of the Women Lawyers Association of Los Angeles. In 2009, Ms. Forsheit was named one of the Los Angeles Daily Journal's Top 100 women litigators in California.

[1] *See*, *e.g*., Thomas O'Toole, *Cyberlaw Predictions: The Privacy Policy Debate in the United States*, BLOOMBERG BNA, Jan. 8, 2013, http://www.bna.com/cyberlaw-predictions-privacy-b17179871752/; Christopher Wolf & Jules Polonetsky, *Happy New Year from the Future of Privacy Forum!*, FUTURE OF PRIVACY FORUM, Jan. 2, 2013, http://www.futureofprivacy.org/2013/01/02/happy-new-year-201/ (lists the top ten "ins" and "outs" for 2013 with California AG Kamala Harris listed as number two on the "in" list).

II. CALIFORNIA'S ATTORNEY GENERAL AND MOBILE APP PRIVACY

What exactly did Ms. Harris do with respect to apps in 2012 to receive so much attention and concern?

First, in February 2012, the Attorney General announced an agreement with Amazon, Apple, Google, Hewlett-Packard, Microsoft, and Research In Motion, the leading operators of mobile application platforms, pursuant to which those platforms committed to "privacy principles designed to bring the industry in line with a California law requiring mobile apps that collect personal information to have a privacy policy."[2] Facebook later signed on to the agreement. The agreement stated that, where required by law, an app that collects personal data from a user must conspicuously post a privacy policy or other statement describing the app's privacy practices that provides clear and complete information regarding how personal data is collected, used, and shared. The app platforms also agreed that they would include in the application submission process for new or updated apps either an optional data field for a hyperlink to, or for the text of, the app's privacy policy or a statement describing the app's privacy practices. For developers who chose to submit such a hyperlink or text,

[2] Press Release, State of California Department of Justice Office of the Attorney General, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications (Feb. 22, 2012), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy.

the app platforms agreed to enable access for users to the hyperlink or text from the app store.[3]

Over the summer, Ms. Harris also formed a new Privacy Enforcement and Protection Unit in her office to oversee privacy issues and prosecute companies that violate California's many privacy laws.[4]

In October, out of the blue, Ms. Harris used Twitter to note that United Airlines' new mobile app did not include a privacy policy: "Fabulous app, @United Airlines, but where is your app's #privacy policy?"[5] Subsequently, on October 30, 2012, the Attorney General reportedly sent notices to as many as 100 apps, including United, Delta, and OpenTable, instructing them to conspicuously post privacy policies pursuant to California's Online Privacy Protection Act (Business & Professions Code sections 22575-22579) ("CalOPPA") within their apps within thirty (30) days. The notices (a) required that these policies inform users of what personally identifiable information about them is being collected and what will be done with that information, and (b) made clear that, if the companies failed to comply with this directive, the Attorney General might take legal action under CalOPPA.

---

[3] *See* Joint Statement of Principles, State of California Department of Justice Office of the Attorney General, (Feb. 22, 2012), *available at* http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf?.

[4] Press Release, State of California Department of Justice Office of the Attorney General, Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit (July 19, 2012), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection.

[5] Tweet from Kamala Harris, Attorney General of California, https://twitter.com/KamalaHarris/status/256778084219502592 (Oct. 12, 2012, 08:27 AM).

True to her word, Ms. Harris brought her first lawsuit with respect to a company's failure to include a privacy policy in its mobile app in December 2012.[6] The suit against Delta Air Lines alleges a violation of CalOPPA. The complaint alleges that the "Fly Delta" app collects at least fourteen (14) categories of personal information including geo-location data, a user's full name, address, and credit card number and expiration date. Further, the complaint alleges that Delta's failure to have a privacy policy that informs users what information is collected and how it is used constitutes an "unlawful, unfair, or fraudulent" business act or practice under California law.[7] The complaint seeks an injunction and $2,500 in damages for each violation of CalOPPA, which the Attorney General contends applies to each download of a noncompliant app. The complaint includes allegations that, although Delta has a privacy policy on its website, it does not mention the "Fly Delta" app at all and does not include information about what information is collected in the app specifically (as opposed to on the website) and how it is used.

Shortly thereafter, in the first weeks of 2013, the Attorney General released a set of recommendations directed at a number of different mobile app industry players (including app developers, app platform providers, mobile ad

---

[6] Press Release, State of California Department of Justice Office of the Attorney General, Attorney General Kamala D. Harris Files Suit Against Delta Airlines for Failure to Comply with California Privacy Law (Dec. 6, 2012), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-suit-against-delta-airlines-failure.

[7] California v. Delta Air Lines, Inc., No. CGC-12-526741, ¶¶ 4, 13, 29-30 (Cal. Super. Ct. filed Dec. 6, 2012) (Complaint for Civil Penalties, Permanent Injunction and Other Equitable Relief for Violations of Business and Professions Code Section 17200 (Unfair Competition Law)).

networks, operating system providers, and mobile carriers) titled "Privacy on the Go," seeking to "educate the industry and promote privacy best practices."[8]

Thus, the stage is set for a potential showdown regarding the purported applicability to mobile apps of California law governing website privacy.

But first, how did we get here? A little history on mobile apps themselves is in order.

III. The Emergence of Apps

What exactly is an "app"? PC Magazine provides what may be the most practical definition for purposes of this article:

> The term has been shorthand for "application" in the IT community for a long time. However, it became popular with the consumer for mobile applications in smartphones and tablets after Apple debuted the iPhone 3G in 2008. It is just as correct to say "iPhone application" as it is "desktop computer app;" although app is shorter, and computer people love to abbreviate."[9]

When exactly did the term "app" become part of our everyday vocabulary? Less than five years ago. The Apple App Store for iOS launched on

---

[8] Kamala D. Harris, Attorney General, California Department of Justice, Privacy on the Go: Recommendations for the Mobile Ecosystem 1 (Cal. Dept. Justice 2013), *available at* http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf [hereinafter Privacy on the Go]. Immediately on the heels of the issuance of the new California recommendations, the Federal Trade Commission also issued a new staff report, "Mobile Privacy Disclosures: Building Trust Through Transparency," reiterating the FTC's previous mobile and online privacy related efforts and distilling its latest recommendations for clearly and transparently informing users about mobile data practices. FTC Staff Report, Mobile Privacy Disclosures: Building Trust Through Transparency (Fed. Trade Comm'n 2013) *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

[9] PC Mag.com, App Definition from PC Magazine Encyclopedia, http://www.pcmag.com/encyclopedia_term/0,1237,t=app&i=37865,00.asp (last visited Jan. 21, 2013).

July 10, 2008, and the Android Market, now known as Google Play, launched in October of that same year. BlackBerry's App World went live in April 2009.[10]

Apps are now omnipresent. According to recent news reports, 1.76 billion apps were downloaded by iOS and Android users from December 25 through December 31, 2012, alone. The weekly average before the holidays, between December 4 and December 17, was 1.07 billion. The research firm Flurry Analytics has estimated that more than 1 billion apps will be downloaded on a weekly basis in 2013 until some point in the fourth quarter, when it predicts iOS and Android app downloads will combine to hit 2 billion downloads each week.[11]

Although the new mobile app economy is exploding, and mobile apps are collecting more and more personal information from users, many apps have not been developed with privacy in mind and most have lacked privacy notices or other disclosures regarding data collection, uses, and sharing. As noted by Ms. Harris in her January 2013 mobile app guidelines, "[r]ecent studies have found that many mobile apps did not provide users with privacy policy statements at all."[12]

---

[10] Wikipedia.org, App Store (iOS), http://en.wikipedia.org/wiki/App_Store_(iOS)#History (last visited Jan. 21, 2013); Wikipedia.org, BlackBerry App World, http://en.wikipedia.org/wiki/BlackBerry_App_World, (last visited Jan. 21, 2013); Wikipedia.org, Google Play, http://en.wikipedia.org/wiki/Google_Play (last visited Jan. 21, 2013); *see* Posting of Victor, ShoutEm CEO, to ShoutEm Blog, Infographic—The History of Mobile App Stores, http://blog.shoutem.com/2012/02/07/infographic-the-history-of-mobile-app-stores/ (Feb. 7, 2012).

[11] Don Reisinger, *Record iOS, Android App Downloads Tallied in Last Week of 2012*, CNET NEWS, Jan. 2, 2013, http://news.cnet.com/8301-1035_3-57561604-94/record-ios-android-app-downloads-tallied-in-last-week-of-2012/.

[12] PRIVACY ON THE GO, *supra* note 8, 3 n.5 (citing *Your Apps Are Watching You*, WALL ST. J. (Dec. 17, 2010); FED. TRADE COMM'N, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE

With mobile apps now pervasive, and the California Attorney General making mobile app privacy an education and enforcement priority, the obvious question is—what law purports to require that an app have a privacy policy? Kamala Harris points to CalOPPA. The remainder of this article explores CalOPPA's requirements for privacy policies, as well as other sources of law and best practices that should be considered in crafting privacy policies for websites and mobile apps alike.

IV. PRIVACY POLICIES: LAW AND BEST PRACTICES

A. *CALIFORNIA'S WIDE-REACHING LAW REQUIRING PRIVACY POLICIES*

CalOPPA became operative on July 1, 2004, more than eight and a half years ago. It requires that any "operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service" conspicuously post its privacy policy.[13] The following discusses CalOPPA's specific requirements, starting with the scope of coverage.

1. *Who and What Are Covered*

Under CalOPPA, the term "operator" means any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in

---

DISAPPOINTING (Feb. 2012); FED. TRADE COMM'N, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE (Dec. 2012); FUTURE OF PRIVACY FORUM, FPF MOBILE APPS STUDY (June 2012)).

[13] CAL. BUS. & PROF. CODE § 22575.

California who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes.[14] It does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner's behalf or by processing information on behalf of the owner.[15]

CalOPPA effectively operates as a federal law because it purports to apply to any site or service that collects certain kinds of information about individual consumers residing in California, regardless of where the site is located. Consumers are not limited to actual customers. They include any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes.[16]

As discussed above, Ms. Harris has made clear that she very much considers apps to be an "online service," as used in CalOPPA, i.e., "any service available over the Internet or that connects to the Internet."

2. *How the Policy Must Be Posted*

Once an organization has determined that it is covered by CalOPPA, it must then decide how to post its privacy policy on its website and/or app. CalOPPA requires that privacy policies be posted in one of the following ways:

---

[14] CAL. BUS. & PROF. CODE § 22577(c).
[15] *Id*.
[16] CAL. BUS. & PROF. CODE § 22577(d).

(1) Web page on which the actual privacy policy is posted if the Web page is the homepage or first significant page after entering the Web site.
(2) An icon that hyperlinks to a Web page on which the actual privacy policy is posted, if the icon is located on the homepage or the first significant page after entering the Web site, and if the icon contains the word "privacy." The icon shall also use a color that contrasts with the background color of the Web page or is otherwise distinguishable.
(3) A text link that hyperlinks to a Web page on which the actual privacy policy is posted, if the text link is located on the homepage or first significant page after entering the Web site, and if the text link does one of the following:
(A) includes the word "privacy,"
(B) is written in capital letters equal to or greater in size than the surrounding text,
(C) is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.
(4) Any other functional hyperlink that is so displayed that a reasonable person would notice it.
(5) In the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the online service.[17]

3. *What Content the Policy Must Include*

CalOPPA includes specific requirements for privacy policy content. First, the privacy policy must:

> (1) Identify the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.[18]

---

[17] CAL. BUS. & PROF. CODE § 22577(b).
[18] CAL. BUS. & PROF. CODE § 22575(b)(1).

Personally identifiable information is broadly defined for this purpose, not like the narrow definition used by most breach notification statutes. It means:

> [A]ny individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:
>
> (1) A first and last name.
>
> (2) A home or other physical address, including street name and name of a city or town.
>
> (3) An e-mail address.
>
> (4) A telephone number.
>
> (5) A social security number.
>
> (6) Any other identifier that permits the physical or online contacting of a specific individual.
>
> (7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described [above].[19]

The privacy policy must also include the following:

> (2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process.
>
> (3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy for that Web site or online service.
>
> (4) Identify its effective date.[20]

4. *Violation*

CalOPPA provides that an operator shall be in violation of the law only if the operator fails to post its policy within thirty days after being notified of

---

[19] CAL. BUS. & PROF. CODE § 22577(a).

[20] CAL. BUS. & PROF. CODE § 22575(b)(2)-(4).

noncompliance.[21] An operator is in violation if it fails to comply with the requirements described above or with the provisions of its posted privacy policy either knowingly and willfully or negligently and materially.[22]

B. *OTHER CONSIDERATIONS*

While CalOPPA provides specific guidance as to essentials that should be included in privacy policies and how such policies must be presented, it is only a starting place. Practitioners should consider other sources of law and best practices in preparing privacy policies. Poorly crafted privacy policies are not without consequence. As just one example, in this country since 1998, the FTC has taken the position that use or disclosure of personal information in a manner contrary to an organization's posted privacy policy is a deceptive practice under Section 5 of the *FTC Act*.[23] The FTC has brought dozens of cases against organizations under its Section 5 power related to privacy and data security issues, including a number related to privacy promises.[24]

Following is a non-exhaustive discussion of certain other elements that should be considered in preparing privacy policies, for websites and mobile apps alike.

---

[21] CAL. BUS. & PROF. CODE § 22575(a).
[22] CAL. BUS. & PROF. CODE §§ 22575, 22576.
[23] FTC Act, 15 U.S.C. § 45; *see* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 102 (Int'l Ass'n of Privacy Professionals 2011).
[24] *See*, *e.g.*, Myspace LLC, 2012 WL 4101790 (F.T.C. Aug. 30, 2012); Facebook, Inc., 2012 WL 3518628 (F.T.C. July 27, 2012); U.S. v. Google, 2012 WL 5833994 (N.D. Cal. Nov. 16, 2012); Sears Holdings Mgmt. Corp., 2009 WL 2979770 (F.T.C. Aug. 31, 2009); Gateway Learning Corp., 138 F.T.C. 443 (Sept. 10, 2004).

1. *Automated Collection of Data via Cookies, Web Beacons, and Tracking Technologies*

It is highly recommended that policies include a description of the kinds of information that are automatically collected using various technologies such as cookies and web beacons, particularly those that track user surfing behavior, even if those kinds of information, such as IP address, are not commonly thought of in this country as "personally identifiable." The EU Privacy and Electronic Communications Directive (the "ePrivacy Directive") requires web sites to obtain opt-in consent from consumers prior to setting cookies, and has been adopted by the United Kingdom and a handful of other EU member countries. Some jurisdictions, like the UK, have imposed requirements for cookie opt-in compliance that go far beyond anything required in this country to date.

Behavioral advertising, or tracking user behavior across websites, has also caught the attention of regulators here in the United States and abroad, and requires more explicit consent than contextual advertising. The privacy implications of such technologies and activity are beyond the scope of this article, but the FTC has issued numerous reports exploring those issues,[25] and they are fertile ground for litigation and potential legislation.

[25] *See*, *e.g.* FTC REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (Fed. Trade Comm'n 2012), *available at* http://ftc.gov/os/2012/03/ 120326privacyreport.pdf; FTC STAFF REPORT, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (Fed. Trade Comm'n 2009), *available at* http://www.ftc.gov/os/2009/02/ P085400behavadreport.pdf.

2. *Children*

Organizations must consider whether they directly target children or knowingly collect personal information from children under the age of thirteen. On December 10, 2012, the FTC released a follow-up to its February 2012 report on mobile apps for kids and found that, for the most part, privacy and other material disclosures are still not being made available to parents prior to app download or at all.[26] The follow-up report also found that where there are privacy disclosures, the disclosures sometimes contradict the actual practices of the app.

Also in December 2012, the FTC announced that it had finalized amendments to the Children's Online Privacy Protection Act ("COPPA") Rule, originally enacted in 2000.[27] The original Rule required that websites: (1) obtain parental consent before collecting children's personal information; (2) keep children's personal information secure; and (3) not condition continued use of a website upon children entering more personal information than is necessary to reasonably access the website's services, in addition to other restrictions and requirements.[28] The changes to the Rule were in response to the pace of change of technology on websites and other services, particularly mobile apps, and mean changes for privacy policies of all types, including those for apps.

---

[26] FTC STAFF REPORT, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE 4 (Fed. Trade Comm'n 2012), *available at* http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf.

[27] Press Release, Federal Trade Commission, FTC Strengthens Kids' Privacy, Gives Parents Greater Control over Their Information By Amending Children's Online Privacy Protection Rule (Dec. 19, 2012), *available at* http://www.ftc.gov/opa/2012/12/coppa.shtm.

[28] 16 C.F.R. pt. 312.

In the original COPPA Rule, "personal information" included a child's name, physical address, and certain online contact information (e.g., an email address), which would, together, permit a party to contact a child, whether in person, by telephone, or online.[29] Acknowledging that there are now several ways that sites track users over time and across websites, the FTC amended the definition of "personal information" to now require parental consent when collecting "persistent identifiers" that are not only connected to a child's personally identifiable information, but also to the device from which the child may access the website or mobile app, including unique device identifiers, IP addresses, and any plug-in or cookie that can be tracked across websites.

Also significant—while the original Rule defined an "operator" as a first party website that directly targets children or knowingly collects personal information from children, the new Rule expands the definition to include certain service providers, including third party ad networks, which operate on such websites and knowingly collect information from users of those websites. Operators are now directly liable for the actions of any third party service providers that collect information from children on their sites.

There is much more to the new COPPA Rule—app developers and other organizations should become familiar with those provisions and take heed in formulating information collection, use, and sharing practices.

---

[29] 16 C.F.R. § 312.2.

3. *Third Party Content and Links*

Especially in this day and age of social networking, it is increasingly important for apps and websites to make clear whose privacy practices they do not control—those of third parties whose content or sites might be linked to an app or website. It is important to make clear that such third party sites and apps are beyond the scope of a given privacy policy, and to encourage users to review and understand the privacy policies of those third parties.

4. *California Shine the Light Disclosures*

Until the emergence of direct authority on the question whether California's online privacy laws do or should apply to mobile apps, practitioners would also be well advised to address compliance with California's Shine the Light law, Civil Code section 1798.83 ("Shine the Light"), in their mobile app privacy policies.

Shine the Light allows California residents to request information from businesses about their third-party information-sharing practices. A business must make certain disclosures to customers upon request if the business "has an established business relationship with a customer and has within the immediately preceding calendar year disclosed personal information [of that customer] for the third parties' direct marketing purposes."[30] The business must designate an email address, postal address, toll-free phone number, or toll-free fax number to which

[30] CAL. CIV. CODE § 1798.83(a).

customers should send Shine the Light requests. The business has thirty (30) days to timely respond to a Shine the Light request sent to the designated contact point.

Once a business designates one or more Shine the Light contact points, the business must disseminate the contact point(s) in at least one of the following three ways: (1) by training all employees who regularly have contact with customers to provide the contact point information on request; (2) by adding a section to the company website describing customers' Shine the Light rights and providing the contact point information; and/or (3) by making the contact point information readily available at every location within California where the business and its agents regularly have contact with customers.[31] If a business chooses the second option, the company's homepage must contain a link entitled "Your California Privacy Rights," linking either to a section discussing its Shine the Light compliance or containing the company's overall privacy policy. The page must call attention to the link by making the text larger than the surrounding text, making the text distinct in color or typeface, or setting it off with a symbol. The first page after that link must describe customers' Shine the Light rights and provide the company's contact point information.[32]

In lieu of responding to Shine the Light requests, a company can choose to comply with Shine the Light by adopting and disclosing to the public in its privacy policy either a policy of not disclosing personal information of customers

[31] CAL. CIV. CODE § 1798.83(b).
[32] CAL. CIV. CODE § 1798.83(b)(1)(B).

to third parties for the third parties' direct marketing purposes unless the customer first affirmatively agrees to that disclosure, or one of not disclosing the personal information of customers to third parties for the third parties' direct marketing purposes if the customer has exercised an option that prevents that information from being disclosed to third parties for those purposes.[33] As long as the business maintains and discloses the policies, the business may comply with Shine the Light by notifying the customer of his or her right to prevent disclosure of personal information and providing the customer with a cost-free means to exercise that right.

V. The App Dilemma and What's to Come

As evidenced by some of the developments described above, regulators have progressively imposed more and more requirements for detailed disclosures in the text of privacy policies. At the same time, consumer advocates have grown understandably weary with privacy policies written by lawyers for lawyers that no ordinary consumer can understand, even if he or she is inclined to read it. The explosion of mobile devices has exacerbated this problem by reducing the size of the screen on which the user can view and digest such policies and disclosures. Attempting to apply existing website privacy policy requirements to mobile-optimized sites is itself problematic. Taking the next step to apps, designed for a

[33] Cal. Civ. Code § 1798.83(c)(2).

variety of technology-specific platforms, adds a whole new level of complexity where simplicity should be the goal.

A number of private organizations have begun to devise more simplified templates and structures for privacy policies that are focused on the mobile app world, and even the FTC is examining a "nutrition label" approach to simplified disclosure in privacy policies.[34] But, it remains to be seen whether, and how, a short "nutrition label" type notice can describe all of its various complex data collection, tracking, and sharing mechanisms of a mobile app in plain user-friendly language.

It is unclear how organizations will reconcile the complex and detailed regulatory requirements for privacy policies with the desire for simplicity and user-friendly disclosures. In the meantime, all organizations developing or using apps of any kind must take into consideration the new legal landscape described above. Mobile apps are, and will continue to be, under scrutiny. The question is no longer "Is there an app for that?" but "Is there a privacy policy for that app?"

---

[34] Allison Grande, *FTC Working On "Nutrition Label" For Data Collection*, LAW360, Oct. 23, 2012, http://www.law360.com/articles/388954/ftc-working-on-nutrition-label-for-data-collection.