ALSTON&BIRD LLP

WWW.ALSTON.COM

Privacy & Security ADVISORY ■

**MAY 14, 2014**

# Special Assistant Attorney General Speaks on Privacy Issues at Alston & Bird's Los Angeles Office

**By: Dominique Shelton and Sheila Shah**

As part of the California Attorney General's ongoing effort to educate the business community regarding privacy issues, Jeffrey Rabkin, Special Assistant Attorney General for Law and Technology, briefed business professionals, privacy officers, in-house and outside counsel on May 13, 2014, in Alston & Bird's Los Angeles office. Mr. Rabkin, who serves as Special Assistant Attorney General to California Attorney General Kamala D. Harris and is the Attorney General's principal policy advisor on technology, discussed which privacy issues the California AG's office will focus on in the near future, the office's forthcoming report on best practices for privacy disclosures, the recent White House Report on Big Data, behavioral tracking, mobile apps and data breach issues. As a regulator, Mr. Rabkin has a great deal of experience with these issues as he oversees the office's policy and enforcement work on cybercrime, cybersecurity, privacy, intellectual property, technology-related antitrust issues and the development of the Department of Justice's digital forensics laboratories.

Although Mr. Rabkin's discussion touched on numerous issues pertinent to the digital privacy world, Alston & Bird gleaned some "best practices" components of the discussion that could be useful to players in the digital ecosystem in the areas of:

- Big Data
- Privacy Policies
- Data Breach
- Mobile Apps
- Medical Information
- Enforcement

## I. Big Data: The White House Report and the Growing Business Model

- **The White House Report:** Fresh on everyone's minds were the two White House reports on big data that were released on May 1, 2014: (1) Big Data: Seizing Opportunities, Preserving Values; and (2) Big Data and Privacy: A Technological Perspective. Both reports were thorough and should be consulted in detail. Based on the plain language of the reports, the discussion by Mr. Rabkin and other comments made during the briefing, we believe companies should pay close attention to the proposed evolution enunciated in the White House reports *away from* reliance solely on the regime of notice and consent towards a new—and potentially emerging—"use" regime that would place the onus on companies to comply with pre-determined user privacy preferences as articulated in pre-prepared profiles. In the Big Data and Privacy: A Technological Perspective report authored by the President's Counsel of Advisors on Science and Technology (at p. 39-40), there is discussion of how such pre-determined consumer privacy profiles could be created, incentivizing companies to build apps and technology that match such profiles. In this "use"-based paradigm, if it were to be adopted, the White House reports discuss there are certain data that companies would agree never to collect, others that could be collected and disclosed without consent based upon universal agreement, and the third category requiring consent would be based upon the consumer profiles discussed above. Big Data: Seizing Opportunities, Preserving Values (at p. 54-55).
- **The Evolution of Notice and Consent:** As discussed above, the briefing touched on the White House report's language as a harbinger that someday down the road, regulators may be moving away from the notice and consent regime (a system whereby consumers are provided with a description of privacy practices and consent to the privacy practice) to a regime where data use rather than data collection and retention will be the critical regulatory issue. As we mentioned in our previous client alert, while companies should keep this "evolution" in mind, companies should not yet jettison their notice and consent regimes. *See*, e.g., Alston & Bird's blog post The White House Releases Report on Big Data. As Mr. Rabkin mentioned, comprehensive privacy policies are still a critical component to compliance with existing law. Nevertheless, we should be on the lookout for a shift from placing the onus on the consumer (i.e., compelling consumers to read disclosures and provide consent) to placing the onus on providers (i.e., having the providers craft their services so that they are in accordance with a consumer's preferences for data use). Indeed, these new data use preference settings may be embarking into the technologies of the future.

## II. Privacy Policies and Best Practices for Disclosures

- **There Will Be a New Guidance Emerging from the AG's Office Any Day Now Regarding "Do Not Track" and Best Practices for Privacy Policy Drafting in General:** Mr. Rabkin discussed the genesis of the AG office's forthcoming report on privacy disclosure, "Making Your Privacy Practices Public: Recommendations on Developing a Meaningful Privacy Policy." The "best practices" guide was largely in response to A.B. 370, the California law that amended California Business and Professions Code Section 22575 requiring companies to include in their privacy policies how they respond to "Do Not Track." From the discussion, Alston & Bird suggests this be strictly followed, despite potential controversies and unknowns when it comes to the technology of "Do Not Track." As was underscored during the discussion, A.B. 370 does not mandate any particular response to Do Not Track, only that companies include descriptions of their response in their privacy policies and behave in accordance with those descriptions.

- **The Importance of a Comprehensive but Readable Policy:** Although the discussion did include questions about the continuing importance of a comprehensive privacy policy and the difficulty in making it both comprehensive and comprehensible, Alston & Bird believes that the AG's office is still committed to the notion of a comprehensive privacy policy requirement. Beyond the fact that companies are required to have privacy policies per California law, the AG's office believes it to be important from a governance perspective. Despite the fact that there are debates over "privacy fatigue" and whether consumers actually spend time reading through privacy policies, these policies are useful to regulators and consumer watchdog groups that do look at these policies. Moreover, these policy requirements force companies to map out and think through their privacy practices. As such, it continues to be a best practice to ensure that companies have a comprehensive, current privacy policy that is in compliance with existing law. Moreover, under California's Online Privacy Protection Act, companies must post a privacy policy whenever collecting personal information from California residents.

## III. Data Breach

- **"Reasonable Security":** There has long been confusion surrounding what constitutes "reasonable security" in data breach actions. We interpreted Mr. Rabkin's comments on this issue to mean the following reasonable security standard is akin to the notion of negligence, both are highly nuanced, multifaceted concepts that cannot be reduced down to a single element. In determining what is "reasonable security," companies should think about how a judge or jury would react to certain practices. Was there adequate training of staff and employees? Was there a cogent plan to deal with a potential breach in place prior to the breach? How did the company react after the breach, i.e., what remediation measures were taken? Although companies should be sure to work with counsel who are current in what the FTC has deemed to be "reasonable security," the above items are also important to bear in mind.
- **Create an Incident Response Plan – Keeping in Mind That Upper Management Needs to Be Involved in Privacy and Data Security Issues:** Creating a data breach plan, monitoring data security and data mapping should not be limited to a company's IT departments. Rather, given the growing importance of data collection for businesses, upper management should be actively involved in crafting privacy and data security policies for their companies. Moreover, companies should think beyond "compliance" when it comes to privacy and data issues and think in terms of brand management, i.e., a company should think in terms of how it can brand its privacy policies, and in turn, incorporate its privacy policies into its brand.
- **Encryption and Privacy Trainings Are Important.** The discussion also covered technological and human relations steps that can be taken to address cybersecurity. Encryption emerged as an important factor.
- **California Resources on Cybersecurity and Data Breach:** The audience was provided copies of the CA AG's February 2014 report titled "Cybersecurity in the Golden State," as well as the AG's 2012 Data Breach report reflecting the reports to the CA AG of data breaches involving more than 500 California residents. These resources are also useful for companies attempting to develop protocols to satisfy "reasonable security" standards.

## IV. Mobile Apps

- **Mobile Apps Will Continue to Be a Priority Area for the AG's Office in the Near Future:** Last year, the CA AG issued guidance on mobile apps ("Privacy on the Go") and filed a lawsuit related to the same. We suggest companies revisit "Privacy on the Go," which outlines "best practices" for privacy disclosures in mobile apps. When asked about what the AG's office was planning on focusing on in the near future, Mr. Rabkin mentioned that the office would continue to focus on mobile apps.
- **Placement of Short-Form Notice:** Although the AG's office is hesitant to micromanage app developers and publishers, when it comes to the placement of short-form notice, also known as Just-in-Time notice, we think the AG's office supports flexibility in the placement of the short form or Just-in-Time notice. It appears that there is support for both pop-up notices before collection of financial and medical information and other forms of Just in Time. However, based on Mr. Rabkin's comments, it would also be wise to include short-form notice in the mobile app store so that a consumer is informed prior to their purchase of the app.

## V. Compliance with California's Medical Information Act Is Important for Developers of Mobile Apps, Software and Hardware (e.g., Clouds)

- **California Medical Information Act (CMIA) Compliance May Present Thorny Issues in the Near Future:** A major takeaway from Tuesday's briefing was that companies, particularly companies that are involved with health or fitness data, should pay particular attention to California's Confidentiality of Medical Information Act (CMIA). Effective January 1, 2014, the newly amended Section 56.06(b) makes software, hardware and mobile app developers "providers of health care," imposing disclosure authorization and security requirements on them. Civil Code Section 56.06(b) states that: "Any business that offers *software or hardware to consumers, including a mobile application . . . that is designed to maintain medical information*, as defined in subdivision (g) of Section 56.06, in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual, shall be deemed to be a provider of health care subject to the requirements of this part. However, nothing in this section shall be construed to make a business specified in this subdivision a provider of health care for purposes of *any law other than this part*, including laws that specifically incorporate by reference the definitions of this part." See, Cal. Civ. Code § 56.06(b) (emphasis added).

  The CMIA defines "medical information" broadly to mean any information "in the possession of or derived from a provider of health care . . . regarding a patient's medical history, mental or physical condition, or treatment." If one were to insert "mobile app provider" where "provider of health care" appears in the above definitions, then fitness apps could arguably fall within the CMIA to the extent they generate and/or possess information regarding the user's physical condition. For instance, apps that monitor one's heart rate could be generating "medical information," thus triggering the confidentiality requirements of the CMIA.

  The Bill Analysis for AB 658 (the bill that was ultimately signed into law on September 9, 2013) and other legislative history makes clear that opponents such as the Chamber of Commerce and other industry representatives, were concerned the bill might be misconstrued to apply to fitness data like heart rate or steps taken, tracked by a smartphone, and potentially sent to a user's Personal Health Record [PHR]. In response, the analysis maintains that "the intent of the CMIA was to protect medical information that originated with medical professionals, insurers, administrators, or other contractors who held a person's medical information." The bill was later further

amended to include language that the definition of "provider of health care" that includes mobile apps and software and hardware was not meant to change "any law other than this part." And therein lies the problem.

This language designed to limit the application of CMIA to mobile apps appears to be a result of a scrivener's error. As written, Section 56.06(b) purports to apply to the entirety of the CMIA, given that it is applicable for purposes of "this part," rather than only this "section" or this "subdivision," which would cabin its applicability to Section 56.06 or Section 56.06(b), for instance. Under this plain language reading, wherever the term of art "provider of health care" appears within the CMIA, a mobile app provider is also implicated.

This creates a potential for widespread applicability of the CMIA nondisclosure requirements, given that the existing definitions of "medical information" and "patient" in Section 56.05 both incorporate the term of art "provider of health care," that now has a new definition, per the amendment.

Individual plaintiffs can seek statutory damages of $1,000 with no actual proof of damages. (Civil Code Section 56.36(b).) More importantly, companies that negligently or wilfully violate the CMIA may face administrative fines and/or civil penalties if their conduct is pursued by a regulator such as the CA AG's office. Civil Code Section 56.36(c) imposes an administrative remedy or civil penalty of up to $2,500 for negligent disclosure and $25,000 for "knowingly and willfully" obtaining, disclosing or using medical information in violation of the CMIA. These penalties shoot to $250,000 per violation plus disgorgement of profits if a violator knowingly or willfully obtains or uses information for "purposes of financial gain."

The takeaway here is to know this amendment is out there and make sure that if medical information is collected through your app, valid authorization is obtained under Civil Code Section 56.11.

## VI. Enforcement

- Based on the discussion, no predictions regarding enforcement can be made at this juncture. That said, from the discussion, we would expect the AG's office to work to avoid litigation where possible and handle privacy issues with phone calls and discussions. That being said, it would not surprise us if some enforcement actions are filed in 2014.

## Conclusion

Ultimately, the California AG's office looks forward to a collaborative relationship with the private sector, and is interested in maintaining a productive dialogue between private and public actors regarding privacy issues in the digital space. The office also looks forward to educating privacy professionals in the future regarding its policies, guidance and enforcement priorities.

The evening opened with remarks from Thomas Wingard, Partner-in-Charge of Alston & Bird's Los Angeles office. Wingard pointed to the May 13 editions of the ***Wall Street Journal, Los Angeles Times*** and ***Financial Times***—all filled with discussions of privacy. He noted that as a corporate lawyer, he has seen an uptick in privacy issues in business. As Wingard noted, privacy is "top of mind" for all of us in the business and legal community these days.

The discussion was held in a question-and-answer format, with questions being posed by Alston & Bird Partner Dominique Shelton, a member of the firm's Litigation & Trial Practice and Privacy & Data Security Groups. Ms. Shelton opened the program with the disclaimer that the program was solely for educational purposes. Shelton also emphasized, "The program's content was not an official statement from the California Attorney General's office or from Mr. Rabkin personally, nor is the content binding on the office."

If you would like to receive future *Privacy & Security Advisories* electronically, please forward your contact information to **privacy.post@alston.com**. Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

## Members of Alston & Bird's Privacy & Security Group

### Atlanta


Angela T. Burnette
angie.burnette@alston.com
404.881.7665

Kristine McAlister Brown
kristy.brown@alston.com
404.881.7584

Megan K. Callahan
megan.callahan@alston.com
404.881.4283

Lisa H. Cassilly
lisa.cassilly@alston.com
404.881.7945

Maki DePalo
maki.depalo@alston.com
404.881.4280

Clare H. Draper, IV
clare.draper@alston.com
404.881.7191

Peter K. Floyd
peter.floyd@alston.com
404.881.4510

James A. Harvey
jim.harvey@alston.com
404.881.7328

John R. Hickman
john.hickman@alston.com
404.881.7885

William H. Jordan
bill.jordan@alston.com
404.881.7850
202.239.3494

David C. Keating
david.keating@alston.com
404.881.7355

W. Scott Kitchens
scott.kitchens@alston.com
404.881.4955

Dawnmarie R. Matlock
dawnmarie.matlock@alston.com
404.881.4253

Kacy McCaffrey
kacy.mccaffrey@alston.com
404.881.4824

Todd S. McClelland
todd.mcclelland@alston.com
404.881.4789

Zachary Neal
zach.neal@alston.com
404.881.4968

Bruce Sarkisian
bruce.sarkisian@alston.com
404.881.4935

Katherine M. Wallace
katherine.wallace@alston.com
404.881.4706

Michael R. Young
michael.young@alston.com
404.881.4288


### Los Angeles


Kim Kisabeth Chemerinsky
kim.chemerinsky@alston.com
213.576.1079

Jonathan Gordon
jonathan.gordon@alston.com
213.576.1165

Katherine E. Hertel
kate.hertel@alston.com
213.576.2600

Sheila A. Shah
213.576.2510
sheila.shah@alston.com

Dominique R. Shelton
dominique.shelton@alston.com
213.576.1170

Nicholas Stamos
nick.stamos@alston.com
213.576.2515


### Washington, D.C.


Edward Britan
edward.britan@alston.com
202.239.3364

Louis S. Dennig, IV
lou.dennig@alston.com
202.239.3215

Paul G. Martino
paul.martino@alston.com
202.239.3439

Kimberly K. Peretti
kimberly.peretti@alston.com
202.239.3720

Eric A. Shimp
eric.shimp@alston.com
202.239.3409

Paula M. Stannard
paula.stannard@alston.com
202.239.3626

Jeffrey R. Sural
jeff.sural@alston.com
202.239.3811


ALSTON&BIRD LLP

WWW.ALSTON.COM




ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213-576-1100
NEW YORK: 90 Park Avenue ■ 12th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, California, USA, 94303-2282 ■ 650-838-2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.756.3300 ■ Fax: 202.756.3333