

Privacy and Information Security Alert

California Attorney General Announces Principles of Mobile Privacy;
Mobile Platform Developers are Onboard

JENNIFER STANLEY AND DAVID MARTY

Fenwick
FENWICK & WEST LLP

On Wednesday, February 22, 2012, California's Attorney General, along with the six leading mobile application platform developers, released a "Joint Statement of Principles" pertaining to privacy in the mobile space. The Joint Statement, adopted by Amazon, Apple, Google, Hewlett-Packard, Microsoft, and RIM, espoused four core principles of mobile privacy. While the Joint Statement does not take the form of a binding agreement and purports to impose no obligations on the platform developers beyond those already imposed by law, it is anticipated that these privacy principles will soon be adopted in full, amongst the six major platforms and beyond:

1. Where required by applicable law, mobile applications that collect personal data from their users must conspicuously post a privacy policy or some statement describing the privacy practices of the application. The policy or statement must provide clear and complete information regarding how the application and the application developer handle the personal data collected.
2. Mobile platform developers will implement an optional data field that will allow application developers, in submitting their applications, to provide a privacy policy or statement regarding the privacy practices of the application. Where developers provide such information in the submission process, the platform developers will then provide consumers with access to each policy or statement through the platform's online application store or marketplace.
3. Platform developers will each implement a method for application users to report to the platform developers any non-compliance by apps with their stated privacy policies, terms of service, or other applicable laws.
4. Platform developers will each implement a process for responding to reported instances of application developers' non-compliance with privacy policies and/or applicable law.

The platform developers additionally agreed in the Joint Statement to continue to work the Attorney General toward developing best practices for protecting consumer privacy in the mobile application space and beyond. The group will convene again with the Attorney General within six months to continue their evaluation and assess progress in the industry.

The Attorney General's Joint Statement, while optimistic in tone, sends a message to the mobile application and mobile device industries that the Attorney General's office is engaged with consumer privacy issues and expects companies to comply with California privacy law. The California Online Privacy Protection Act requires an operator of

a commercial website or online service that collects personally identifiable information of Californians to conspicuously post a privacy policy describing (1) the personal information it gathers, (2) how the information may be shared, (3) available processes by which users can review and modify their stored information, and (4) the process by which the operator notifies consumers of material changes to its privacy policy. See Cal. Bus. & Corp. Code § 22575 *et seq.* According to some reports, 95% of application developers do not have privacy policies, even though many applications collect information about their users that could be construed as personal information. Application developers should review their information collection practices and consider whether they are disclosing those practices in their privacy policies.

Within hours of the release of the California Attorney General's Joint Statement, the White House outlined its proposed "Consumer Privacy Bill of Rights" in a new report entitled "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy." Amongst the many topics covered by the White House's lengthy report is consumer privacy in the mobile space.

For the full text of the White House's Consumer Privacy Report, see [here](#). For the full text of the California Attorney General's Joint Statement of Principles, see [here](#). For more information or guidance regarding either of these recent developments, please contact David Marty or Jennifer Stanley.

Authors

Jennifer Stanley is a partner in the Intellectual Property Group at Fenwick & West LLP. Her practice concentrates on structuring, drafting and negotiating complex commercial transactions relating to intellectual property. Ms. Stanley is also a member of the firm's transactional privacy and data security practice, assisting clients to confront and manage the international risks associated with handling consumer and employee information. She can be reached at jstanley@fenwick.com or 415.875.2429.

David Marty is an associate in the Litigation Group at Fenwick & West LLP. Mr. Marty is also a member of the firm's Privacy and Information Security Group. His practice focuses on data privacy and copyright issues. Before attending law school, Mr. Marty worked as a Senior Technical Project Manager at a New York-based software startup. He can be reached at dmarty@fenwick.com or 650.335.7288.

©2012 Fenwick & West LLP. All rights reserved.

THE VIEWS EXPRESSED IN THIS PUBLICATION ARE SOLELY THOSE OF THE AUTHOR, AND DO NOT NECESSARILY REFLECT THE VIEWS OF FENWICK & WEST LLP OR ITS CLIENTS. THE CONTENT OF THE PUBLICATION ("CONTENT") IS NOT OFFERED AS LEGAL SHOULD NOT BE REGARDED AS ADVERTISING, SOLICITATION, LEGAL ADVICE OR ANY OTHER ADVICE ON ANY PARTICULAR MATTER. THE PUBLICATION OF ANY CONTENT IS NOT INTENDED TO CREATE AND DOES NOT CONSTITUTE AN ATTORNEY-CLIENT RELATIONSHIP BETWEEN YOU AND FENWICK & WEST LLP. YOU SHOULD NOT ACT OR REFRAIN FROM ACTING ON THE BASIS OF ANY CONTENT INCLUDED IN THE PUBLICATION WITHOUT SEEKING THE APPROPRIATE LEGAL OR PROFESSIONAL ADVICE ON THE PARTICULAR FACTS AND CIRCUMSTANCES AT ISSUE.