THE COMMONWEALTH OF MASSACHUSETTS
OFFICE OF THE ATTORNEY GENERAL
ONE ASHBURTON PLACE
BOSTON, MASSACHUSETTS 02108

MARTHA COAKLEY
ATTORNEY GENERAL

(617) 727-2200
www.ago.state.ma.us

February 18, 2011

The Honorable Donald S. Clark
Secretary, Federal Trade Commission
Room H-135 (Annex Q)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Preliminary Federal Trade Commission Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

Dear Secretary Clark:

On behalf of the Attorneys General of the States of Arizona, Illinois, Indiana, Iowa, Massachusetts, Montana, Nevada, New Mexico, New York, North Dakota, Rhode Island, Tennessee, Vermont, Virginia, and Washington ("the States"), we are writing to comment on the Preliminary Federal Trade Commission Staff Report, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (hereinafter the "Report"), from a consumer protection standpoint. We are the primary state officials who handle consumer complaints and enforce state laws designed to protect consumers from unfair and deceptive business practices.

The States support the protection of consumer privacy, and this letter focuses on three main questions raised by the FTC in the Report's Appendix A:

(1) Are there substantive protections, in addition to those set forth in Section V(B)(1) of the report, that companies should provide and how should the costs and benefits of such protections be balanced? (A-1);
(2) How should the scope of sensitive information and sensitive users be defined and what is the most effective means of achieving affirmative consent in these contexts? (A-3); and
(3) Should additional protections [of teenagers] be explored in the context of social media services? (A-4).

In addition, this letter addresses the States' position that any federal laws or regulations protecting consumer privacy that are adopted as a result of the Report should not preempt states from enforcing state laws and regulations.

1. *Are there substantive protections, in addition to those set forth in Section V(B)(1) of the report, that companies should provide and how should the costs and benefits of such protections be balanced?*

The States believe that the four substantive protections described in Section V(B)(1)[1] should be incorporated into companies' business practices in order to establish standard, comprehensive privacy protections for consumers. As the Report notes, several federal and state laws already require the basic safeguarding of personal information. Forty-six states, plus the District of Columbia, have adopted data security statutes and regulations. In addition, in order to safeguard consumers' information before a data breach occurs, several states have adopted laws requiring businesses to assess their data security policies and procedures and to review what type of personal information is in their possession, where the information is located, and how to safeguard this sensitive information. Additionally, a number of states have laws that detail how consumers' information is to be destroyed when no longer needed.

The Report highlights Massachusetts and California for codifying a set of "reasonable safeguards" that must be implemented for the protection of consumer data.

Massachusetts data security regulations, 201 CMR 17.00, enacted in March 2010, require that entities which own or license personal information about a resident of Massachusetts develop and implement a comprehensive written information security program that requires, among other provisions, that entities: (a) assess the reasonably foreseeable internal and external risks to the security of data containing personal information; (b) implement procedures for preventing terminated employees from accessing physical and electronic records containing personal information; and (c) take reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information. Massachusetts regulations also establish computer security system requirements for entities that own or license personal information about a resident of Massachusetts and electronically store or transmit this information. Covered entities are required, among other provisions, to the extent technically feasible, to: (a) control user IDs and other identifiers; (b) restrict access to company computer systems to active user accounts only; (c) control data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; (d) encrypt transmitted records and files containing personal information that will travel across public networks, and encrypt all data containing personal information to be transmitted wirelessly; and (e) encrypt all personal information stored on laptops or other portable devices. The Massachusetts data security regulations approach to information security takes into account the particular business's size, scope of business, amount of resources, and the need for security.

---

[1] Section V(B)(1) highlights four substantive protections companies should provide: (1) ensuring reasonable safeguards to protect information; (2) collecting only information needed to fulfill a specific, legitimate business need; (3) implementing reasonable and appropriate data retention periods; and (4) taking reasonable steps to ensure the accuracy of data collected.

California has also implemented multiple statutes intended to protect consumer privacy. For example, California Civil Code § 1798.81.5, is designed "to encourage businesses that own or license personal information about Californians to provide reasonable security for that information," and requires businesses that own or license personal information about a California resident to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." In addition, California law also requires that companies that collect personal information about consumers residing in California: (1) conspicuously post their privacy policies on their websites (California Business and Professions Code § 22575); (2) dispose of records containing personal information properly (California Civil Code § 1798.81); (3) notify consumers if a computer system has been breached and their personal information has been or is believed to have been acquired by an unauthorized person (California Civil Code § 1798.82); and (4) disclose their information-sharing practices to consumers upon request if they share the customers' personal information with third-parties that use the information for direct marketing purposes (California Civil Code § 1798.83).

To the extent the FTC is considering adopting data security policies and procedures to encourage more widespread adoption of substantive privacy protections, the States believe that the FTC, in contemplating exemptions, should err on the side of caution in exempting any entity from undertaking an assessment of the preventive steps necessary for protecting consumers' personal information. The States generally support an approach to information security that assesses: (1) the size of the business; (2) the scope of the business; (3) the resources of the business; and (4) the need for the security of the personal information in the possession of the business. By utilizing this approach, both consumer protection and business interests can be balanced.

2. *How should the scope of sensitive information and sensitive users be defined and what is the most effective means of achieving affirmative consent in these contexts?*

Although there are variations in state law definitions of personal information, traditionally personal information includes a consumer's name, in combination with social security number, driver's license or other state identification number, or financial account number, including credit and debit card numbers. The States encourage the FTC to also consider including consumers' medical information and health insurance information to be sensitive information warranting privacy protection. As health information is increasingly maintained electronically and transmitted over the Internet, the concern for patient privacy and data security also increases, and additional protections must be implemented. Indeed, recognizing the sensitive nature of this information, several states have included medical information and health insurance information within the definition of "personal information" in their data security breach statutes and other statutes ensuring the proper safeguarding and disposal of personal information. See e.g., Cal. Civ. Code § 1798.80(e) (including medical information and health information in the

definition of "personal information" for purposes of California's disposal law, Cal. Civ. Code § 1798.81); Cal. Civ. Code § 1798.81.5(d)(1)(D) and (d)(2) (defining "personal information" for purposes of California's safeguards law to include medical information); Cal. Civ. Code § 1798.82(e)(4) and (5), and (f)(2) and (3) (defining "personal information" for purposes of California's data security breach law to include medical information and health insurance information); Cal. Civ. Code § 1798.83(e)(7)(P) and (Q) (defining "personal information" for purposes of California's direct marketing disclosure law to include medical condition and drugs, therapies, or medical products or equipment used); Texas Business and Commerce Code § 521 (including medical information and health information in the definition of "sensitive personal information" in Identity Theft Enforcement and Protection Act).

The States also strongly encourage the FTC to explore further whether location-based data, which is capable of tracking a person's movements, should be considered sensitive information. Location-based social networking is becoming increasingly popular. At a minimum, the States believe that there should be strong mechanisms requiring consumer consent before companies may share location-based data with third-parties, and a concerted effort, both on the state and federal level, to educate consumers about the risks and benefits of location-based services. Additionally, the FTC should explore whether there is any legitimate purpose for "location-based data" to ever be stored or retained by those who gather it. Consumer education is vital so that individuals using mobile devices can make informed choices about how to control their information, such as by adjusting the privacy settings on their mobile devices, and thus, can make conscious decisions about what type of information to share and what type of information should remain private.

3. *Should additional protections [of teenagers] be explored in the context of social media services?*

The States appreciate and echo the FTC's concern that young users, especially teenagers, are "heavy users of digital technology and new media applications" but "teens may not be fully aware of the consequences of what they do." (Report at page 16). Protection of children and teenagers on social networking sites has consistently been a priority for the States. The States support the implementation of additional online safety tools that: (1) protect minors from inappropriate contact on social networking sites; (2) protect minors from inappropriate content on social networking sites; and (3) provide safety tools for all social networking site users.

The States have long-recognized the need to protect the privacy of minors on social networking sites. In January 2008, MySpace and 49 State Attorneys General entered into a 'Joint Statement on Key Principles of Social Networking Sites Safety,' in order to better protect children on MySpace. The same 49 State Attorneys General entered into a similar agreement with Facebook in May 2008. Pursuant to its agreements with MySpace and Facebook, these social networking sites agreed to better protect children and teenagers on their websites by implementing policies such as: (1)

establishing "age locking" so that users cannot change their ages above and below the 18-year-old threshold; (2) allowing users to restrict "friend requests" to only those persons who know the user's last name or e-mail address, and making this functionality mandatory for users under 16-years-old; (3) allowing users under 18-years-old to block users who are over 18-years-old from contacting them or viewing their profiles; (4) assigning private profiles to users under 16 years of age; (5) prohibiting users over 18 years of age from browsing for users under 18-years-old; (6) instituting registries for parents that will allow them to register their children's e-mail addresses if they do not want their children to be using social networking sites; and (7) setting restrictions on the display of offline contact information, such as telephone number and address, in underage profiles and removing postings of such information in public forums upon request.

In addition, all users of social media sites should have extensive privacy controls to enable them to choose who can see their profile.

4. *Preemption*

The States urge the FTC to support the preservation of States' rights in any consumer privacy framework endorsed by the FTC to ensure the States are not preempted from protecting consumers in their jurisdictions, under both state and federal law, and to ensure that state regulation is not undermined. The States encourage a "dual sovereignty model," whereby both state and federal authorities would have the right to bring an action under federal law, and where state enforcement authority is explicitly granted under federal law. By allowing both state and federal entities to retain jurisdiction, the greatest protection will be provided to consumers and the State Attorneys General can continue their important role in bringing enforcement actions that protect their constituents.

We thank the FTC for considering our comments and hope they assist you in our mutual endeavor of protecting consumers.

Sincerely yours,

Martha Coakley
Attorney General of Massachusetts

Tom Horne
Attorney General of Arizona

Lisa Madigan
Attorney General of Illinois

Greg Zoeller
Attorney General of Indiana

Tom Miller
Attorney General of Iowa

Steve Bullock
Attorney General of Montana

Catherine Cortez Masto
Attorney General of Nevada

Gary K. King
Attorney General of New Mexico

Eric T. Schneiderman
Attorney General of New York

Wayne Stenehjem
Attorney General of North Dakota

Peter F. Kilmartin
Attorney General of Rhode Island

Robert E. Cooper, Jr.
Attorney General of Tennessee

William G. Sorrell
Attorney General of Vermont

Kenneth T. Cuccinelli, II
Attorney General of Virginia

Rob McKenna
Attorney General of Washington