以下の文中の書式
青色文字：見出し
斜体文字：定義用語

[STAFF DISCUSSION DRAFT]

MAY 3, 2010

To require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual.

A BILL

To require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as [To be provided].

SEC. 2. DEFINITIONS.

In this Act the following definitions apply:
(1) ADVERTISEMENT NETWORK. - The term ‘”advertisement network” means an entity that provides advertisements to participating websites on the basis of individuals’ activity across some or all of those websites.
(2) AGGREGATE INFORMATION. - The term “aggregate information” means data that relates to a group or category of services or individuals, from which all information identifying an individual has been removed.
(3) COMMISSION. - The term “Commission” means the Federal Trade Commission.
(4) COVERED ENTITY. - The term “covered entity” -
(A) means a person engaged in interstate commerce that collects data containing *covered information*; and

(B) does not include -

(i) a government agency; or

(ii) any person that collects *covered information* from fewer than 5,000 individuals in any 12-month period and does not collect *sensitive information*.

(5) COVERED INFORMATION. - The term “covered information” means, with respect to an individual, any of the following:

(A) The first name or initial and last name.

(B) A postal address.

(C) A telephone or fax number.

(D) An email address.

(E) Unique biometric data, including a fingerprint or retina scan.

(F) A Social Security number, tax identification number, passport number, driver’s license number, or any other government-issued identification number.

(G) A Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual’s financial account.

(H) Any unique persistent identifier, such as a customer number, unique pseudonym or user alias, Internet Protocol address, or other unique identifier, where such identifier is used to collect, store, or identify information about a specific individual or a computer, device, or
software application owned or used by a particular user or that is otherwise associated with a particular user.

(I) A *preference profile*.

(J) Any other information that is collected, stored, used, or disclosed in connection with any *covered information* described in subparagraphs (A) through (I).

(6) FIRST PARTY TRANSACTION. - The term “first party transaction” means an interaction between an entity that collects *covered information* when an individual visits that entity’s website or place of business and the individual from whom *covered information* is collected.

(7) OPERATIONAL PURPOSE. -

(A) IN GENERAL - The term “operational purpose” means a purpose reasonably necessary for the operation of the *covered entity*, including –

(i) providing, operating, or improving a product or service used, requested, or authorized by an individual;

(ii) detecting, preventing, or acting against actual or reasonably suspected threats to the *covered entity*’s product or service, including security attacks, unauthorized transactions, and fraud;

(iii) analyzing data related to use of the product or service for purposes of

optimizing or improving the *covered entity*'s products, services, or operations;

(iv) carrying out an employment relationship with an individual;

(v) disclosing *covered information* based on a good faith belief that such disclosure is necessary to comply with a Federal, State, or local law, rule, or other applicable legal requirement, including disclosures pursuant to a court order, subpoena, summons, or other properly executed compulsory process; and

(vi) disclosing *covered information* to a parent company of, controlled subsidiary of, or affiliate of the *covered entity*, or other *covered entity* under common control with the *covered entity* where the parent, subsidiary, affiliate, or other *covered entity* operates under a common or substantially similar set of internal policies and procedures as the *covered entity*, and the policies and procedures include adherence to the *covered entity*'s privacy policies as set forth in its privacy notice.

(B) EXCLUSION - Such term shall not include the use of *covered information* for marketing, advertising, or sales purposes, or any use of or disclosure of *covered information* to an *unaffiliated party* for such purposes.

(8) PREFERENCE PROFILE. - The term "preference profile" means a list of information, categories of information, or preferences associated with a specific individual or a computer or device owned or used by a particular user that is maintained by or relied upon by a *covered entity*.

(9) RENDER ANONYMOUS. - The term "render anonymous" means to remove or obscure *covered information* such that the remaining information does not identify, and there is no reasonable basis to believe that the information can be used to identify -

(A) the specific individual to whom such *covered information* relates; or

(B) a computer or device owned or used by a particular user.

(10) SENSITIVE INFORMATION. - The term "sensitive information" means any information that is associated with *covered information* of an individual and relates to that individual's -

(A) medical records, including medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;

(B) race or ethnicity;

(C) religious beliefs;

(D) sexual orientation;

(E) financial records and other financial information associated with a financial account, including balances and other financial information; or

(F) precise geolocation information.

(11) SERVICE PROVIDER. - The term "service provider" means an entity that collects, maintains, processes, stores, or otherwise handles *covered information* on behalf of

a *covered entity*, including, for the purposes of serving as a data processing center, providing customer support, serving advertisements to the website of the *covered entity*, maintaining the *covered entity*'s records, or performing other administrative support functions for the *covered entity*.

(12) TRANSACTIONAL PURPOSE. - The term "transactional purpose" means a purpose necessary for effecting, administering, or enforcing a transaction between a *covered entity* and an individual.

(13) UNAFFILIATED PARTY. - The term "unaffiliated party" means any entity that is not related by common ownership or affiliated by corporate control with a *covered entity*.

SEC. 3. NOTICE AND CONSENT REQUIREMENTS FOR THE COLLECTION, USE, AND DISCLOSURE OF *COVERED INFORMATION*.

(a) NOTICE AND CONSENT PRIOR TO COLLECTION AND USE OF *COVERED INFORMATION*. -

(1) IN GENERAL. - A *covered entity* shall not collect, use, or disclose *covered information* from or about an individual for any purpose unless such *covered entity* -

(A) makes available to such individual the privacy notice described in paragraph (2) prior to the collection of any *covered information*; and

(B) obtains the consent of the individual to such collection as set forth in paragraph (3).

(2) NOTICE REQUIREMENTS. -

(A) NATURE OF NOTICE. -

(i) COLLECTION OF INFORMATION THROUGH THE INTERNET - If the covered entity collects *covered information* through the Internet, the privacy notice required by this section shall be.

(I) posted clearly and conspicuously on the website of such *covered entity* through which the *covered information* is collected; and

(II) accessible through a direct link from the Internet homepage of the *covered entity*.

(ii) MANUAL COLLECTION OF INFORMATION BY MEANS OTHER THAN THROUGH THE INTERNET. - If the *covered entity* collects *covered information* by any means that does not utilize the Internet, the privacy notice required by this section shall be made available to an individual in writing before the *covered entity* collects any *covered information* from that individual.

(B) REQUIRED INFORMATION. - The privacy notice required under paragraph (1) shall include the following information:

(i) The identity of the *covered entity* collecting the *covered information*.

(ii) A description of any *covered information* collected by the *covered entity*.

(iii) How the *covered entity* collects *covered information*.

(iv) The specific purposes for which the *covered entity* collects and uses *covered information*.

(v) How the *covered entity* stores *covered information*.

(vi) How the *covered entity* may merge, link, or combine *covered information* collected about the individual with other information about the individual that the *covered entity* may acquire from *unaffiliated parties*.

(vii) How long the *covered entity* retains *covered information* in identifiable form.

(viii) How the *covered entity* disposes of or *renders anonymous covered information* after the expiration of the retention period.

(ix) The purposes for which *covered information* may be disclosed, and the categories of *unaffiliated parties* who may receive such information for each such purpose.

(x) The choice and means the *covered entity* offers individuals to limit or prohibit the collection and disclosure of *covered information*, in accordance with this section.

(xi) The means by and the extent to which individuals may obtain access to *covered information* that has been collected by the *covered entity* in accordance with this section.

(xii) A means by which an individual may contact the *covered entity* with any inquiries or complaints regarding the *covered entity's* handling of *covered information*.

(xiii) The process by which the *covered entity* notifies individuals of material changes to its privacy notice in accordance with paragraph (4).

(xiv) A hyperlink to or a listing of the *Commission's* online consumer complaint form or the toll-free telephone number for the *Commission's* Consumer Response Center.

(xv) The effective date of the privacy notice.

(3) OPT-OUT CONSENT REQUIREMENTS. -

(A) OPT-OUT NATURE OF CONSENT. - A *covered entity* shall be considered to have the consent of an individual for the collection and use of *covered information* relating to that individual if -

(i) the *covered entity* has provided to the individual a clear statement containing the information required under paragraph (2)(B) and informing the individual that he or she has the right to decline consent to such

collection and use; and

(ii) the individual either affirmatively grants consent for such collection and use or does not decline consent at the time such statement is presented to the individual. If an individual declines consent at any time subsequent to the initial collection of *covered information*, the *covered entity* may not collect *covered information* from the individual or use *covered information* previously collected.

(B) ADDITIONAL OPTIONS AVAILABLE. - A *covered entity* may comply with this subsection by enabling an individual to decline consent for the collection and use only of particular *covered information*, provided the individual has been given the opportunity to decline consent for the collection and use of all *covered information*.

(4) NOTICE AND CONSENT TO MATERIAL CHANGE IN PRIVACY POLICIES. - A *covered entity* shall provide the privacy notice required by paragraph (2) and obtain the express affirmative consent of the individual prior to –

(A) making a material change in privacy practices governing previously collected *covered information* from that individual; or

(B) disclosing *covered information* for a purpose not previously disclosed to the individual and which the individual, acting reasonably under the circumstances, would not expect based on the *covered entity*'s prior privacy notice.

(5) EXEMPTION FOR A *TRANSACTIONAL PURPOSE* OR AN *OPERATIONAL PURPOSE*. -

(A) EXEMPTION FROM NOTICE REQUIREMENTS. - The notice requirements in this sub-section shall not apply to *covered information* that –

(i) is collected by any means that does not utilize the Internet, as described in paragraph (2)(A)(ii); and

(ii)

(I) is collected for a *transactional purpose* or an *operational purpose*; or

(II) consists solely of information described in subparagraphs (A) through (D) of section 2(5) and is part of a *first party transaction*.

(B) EXEMPTION FROM CONSENT REQUIREMENTS. - The consent requirements of this subsection shall not apply to the collection, use, or disclosure of *covered information* for a *transactional purpose* or an *operational purpose*, but shall apply to the collection by a *covered entity* of *covered information* for marketing, advertising, or selling, or any use of or disclosure of *covered information* to an *unaffiliated party* for such purposes.

(b) EXPRESS CONSENT REQUIRED FOR DISCLOSURE OF *COVERED INFORMATION* TO *UNAFFILIATED*

PARTIES. –

(1) IN GENERAL. - A *covered entity* may not sell, share, or otherwise disclose *covered information* to an *unaffiliated party* without first obtaining the express affirmative consent of the individual to whom the *covered information* relates.

(2) WITHDRAWAL OF CONSENT. - A *covered entity* that has obtained express affirmative consent from an individual must provide the individual with the opportunity, without charge, to withdraw such consent at any time thereafter.

(3) EXEMPTION FOR CERTAIN INFORMATION SHARING WITH *SERVICE PROVIDERS*. - The consent requirements of this subsection shall not apply to the disclosure of *covered information* by a *covered entity* to a *service provider* for purposes of executing a *first party transaction* if –

(A) the *covered entity* has obtained consent for the collection of *covered information* pursuant to subsection (a); and

(B) the *service provider* agrees to use such *covered information* solely for the purpose of providing an agreed-upon service to a *covered entity* and not to disclose the *covered information* to any other person.

(c) EXPRESS CONSENT FOR COLLECTION OR DISCLOSURE OF *SENSITIVE INFORMATION*. - A *covered entity* shall not collect or disclose *sensitive information* from or about an individual for any purpose unless such *covered entity* –

(1) makes available to such individual the privacy notice described in subsection (a)(2) prior to the collection of any *sensitive information*; and

(2) obtains the express affirmative consent of the individual to whom the *sensitive information* relates prior to collecting or disclosing such *sensitive information*.

(d) EXPRESS CONSENT FOR COLLECTION OR DISCLOSURE OF ALL OR SUBSTANTIALLY ALL OF AN INDIVIDUAL'S ONLINE ACTIVITY. - A *covered entity* shall not collect or disclose *covered information* about all or substantially all of an individual's online activity, including across websites, for any purpose unless such *covered entity* -

(1) makes available to such individual the privacy notice described in subsection (a)(2) prior to the collection of the *covered information* about all or substantially all of the individual's online activity; and

(2) obtains the express affirmative consent of the individual to whom the *covered information* relates prior to collecting or disclosing such *covered information*.

(e) EXCEPTION FOR INDIVIDUAL MANAGED *PREFERENCE PROFILES*. - Notwithstanding subsection (b), a *covered entity* may collect, use, and disclose *covered information* if –

(1) the *covered entity* provides individuals with the ability to opt out of the collection, use, and disclosure of *covered information* by the *covered entity* using a readily accessible opt-out mechanism whereby, the opt-out choice of the individual is preserved and protected from incidental or accidental deletion, including by

-

(A) website interactions on the *covered entity*'s website or a website where the *preference profile* is being used;

(B) a toll-free phone number; or

(C) letter to an address provided by the *covered entity*;

(2) the *covered entity* deletes or *renders anonymous* any *covered information* not later than 18 months after the date the *covered information* is first collected;

(3) the *covered entity* includes the placement of a symbol or seal in a prominent location on the website of the *covered entity* and on or near any advertisements delivered by the *covered entity* based on the *preference profile* of an individual that enables an individual to connect to additional information that –

(A) describes the practices used by the *covered entity* or by an *advertisement network* in which the *covered entity* participates to create a *preference profile* and that led to the delivery of the advertisement using an individual's *preference profile*, including the information, categories of information, or list of preferences associated with the individual that may have led to the delivery of the advertisement to that individual; and

(B) allows individuals to review and modify, or completely opt out of having, a *preference profile* created and maintained by a *covered entity* or by an *advertisement network* in which the *covered entity* participates; and

(4) an *advertisement network* to which a *covered entity* discloses *covered information* under this subsection does not disclose such *covered information* to any other entity without the express affirmative consent of the individual to whom the *covered information* relates.

SEC. 4. ACCURACY AND SECURITY OF *COVERED INFORMATION* AND CONSUMER EDUCATION CAMPAIGN.

(a) ACCURACY. - Each *covered entity* shall establish reasonable procedures to assure the accuracy of the *covered information* it collects.

(b) SECURITY OF *COVERED INFORMATION*. -

(1) IN GENERAL. - A *covered entity* or *service provider* that collects *covered information* about an individual for any purpose must establish, implement, and maintain appropriate administrative, technical, and physical safeguards that the *Commission* determines are necessary to –

(A) ensure the security, integrity, and confidentiality of such information;

(B) protect against anticipated threats or hazards to the security or integrity of such information;

(C) protect against unauthorized access to and loss, misuse, alteration, or

destruction of, such information; and

(D) in the event of a security breach, determine the scope of the breach, make every reasonable attempt to prevent further unauthorized access to the affected *covered information*, and restore reasonable integrity to the affected *covered information*.

(2) FACTORS FOR APPROPRIATE SAFEGUARDS. - In developing standards to carry out this section, the *Commission* shall consider the size and complexity of a *covered entity*, the nature and scope of the activities of a *covered entity*, the sensitivity of the *covered information*, the current state of the art in administrative, technical, and physical safeguards for protecting information, and the cost of implementing such safeguards.

(c) CONSUMER EDUCATION. - The *Commission* shall conduct a consumer education campaign to educate the public regarding opt-out and opt-in consent rights afforded by this Act.

SEC. 5. USE OF *AGGREGATE* OR ANONYMOUS INFORMATION.

Nothing in this Act shall prohibit a *covered entity* from collecting or disclosing *aggregate information* or *covered information* that has been *rendered anonymous*.

SEC. 6. USE OF LOCATION-BASED INFORMATION.

(a) IN GENERAL. - Except as provided in section 222(d) of the Communications Act of 1934 (47 U.S.C. 222(d)), any provider of a product or service that uses location-based information shall not disclose such location-based information concerning the user of such product or service without that user's express opt-in consent. A user's express opt-in consent to an application provider that relies on a platform offered by a commercial mobile *service provider* shall satisfy the requirements of this subsection.

(b) AMENDMENT. - Section 222(h) of the Communications Act of 1934 (47 U.S.C. 222(h)) is amended by adding at the end the following: "(8) CALL LOCATION INFORMATION - The term 'call location information' means any location-based information."

SEC. 7. FEDERAL COMMUNICATIONS COMMISSION REPORT.

Not later than 1 year after the date of enactment of this Act, the Federal Communications Commission shall transmit a report to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate describing -

(1) all provisions of United States communications law, including provisions in the Communications Act of 1934, that address subscriber privacy; and
(2) how those provisions may be harmonized with the provisions of this Act to create a consistent regulatory regime for *covered entities* and individuals.

SEC. 8. ENFORCEMENT.

(a) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION. -
(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES. - A violation of this Act shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.
(2) POWERS OF *COMMISSION*. - The *Commission* shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any person who violates such regulations shall be subject to the penalties and entitled to the privileges and immunities provided in that Act. Notwithstanding any provision of the Federal Trade Commission Act or any other provision of law and solely for purposes of this Act, common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and any amendment thereto shall be subject to the jurisdiction of the *Commission*.
(3) RULEMAKING AUTHORITY AND LIMITATION. - The *Commission* may, in accordance with section 553 of title 5, United States Code, issue such regulations it determines to be necessary to carry out this Act. In promulgating rules under this Act, the *Commission* shall not require the deployment or use of any specific products or technologies, including any specific computer software or hardware.
(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL. -
(1) CIVIL ACTION. - In any case in which the attorney general of a State, or agency of a State having consumer protection responsibilities, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any person who violates this Act, the attorney general or such agency of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to –
(A) enjoin further violation of such section by the defendant;
(B) compel compliance with such section;
(C) obtain damage, restitution, or other compensation on behalf of residents

of the State; or

(D) obtain such other relief as the court may consider appropriate.

(2) INTERVENTION BY THE FTC. -

(A) NOTICE AND INTERVENTION. - The State shall provide prior written notice of any action under paragraph (1) to the *Commission* and provide the *Commission* with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The *Commission* shall have the right -

(i) to intervene in the action;

(ii) upon so intervening, to be heard on all matters arising therein; and

(iii) to file petitions for appeal.

(B) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING. - If the *Commission* has instituted a civil action for violation of this Act, no State attorney general or agency of a State may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the *Commission* for any violation of this Act alleged in the complaint.

(3) CONSTRUCTION. - For purposes of bringing any civil action under paragraph (1), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to -

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

SEC. 9. NO PRIVATE RIGHT OF ACTION.

This Act may not be considered or construed to provide any private right of action. No private civil action relating to any act or practice governed under this Act may be commenced or maintained in any State court or under State law (including a pendent State claim to an action under Federal law).

SEC. 10. PREEMPTION.

This Act supersedes any provision of a statute, regulation, or rule of a State or political subdivision of a State, that includes requirements for the collection, use, or disclosure of *covered information*.

SEC. 11. EFFECT ON OTHER LAWS.

(a) APPLICATION OF OTHER FEDERAL PRIVACY LAWS. - Except as provided expressly in this Act, this Act shall have no effect on activities covered by the following:

(1) Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

(2) The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(3) The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191).

(4) Part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.).

(5) The Communications Act of 1934 (47 U.S.C. 151 et seq.).

(6) The Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.).

(7) The CAN-SPAM Act of 2003 (15 U.S.C. 7701 et seq.).

(b) *COMMISSION* AUTHORITY. - Nothing contained in this Act shall be construed to limit authority provided to the *Commission* under any other law.

SEC. 12. EFFECTIVE DATE.

Unless otherwise specified, this Act shall apply to the collection, use, or disclosure of, and other actions with respect to, *covered information* that occurs on or after the date that is one year after the date of enactment of this Act.