SEC. 2. FINDINGS[1]

Congress finds the following:

(1) Privacy is an inalienable American right guaranteed by the Constitution of the United States, federal and state statutes, state constitutions, and the common law.

(2) Marketers and websites have deployed an elaborate system of digital surveillance that tracks, compiles, and analyzes consumer movements and activities on the Internet, from log-on to sign-off. Companies engaged in behavioral targeting routinely monitor individuals, the searches they make, the Web pages they visit, the content they view, their interactions on social networking sites, the content of their emails, the products and services they purchase, and their physical location.

(3) Offline marketers combine data such as age group, income level, real estate records, motor vehicle records, credit ratings, age and number of children in a household, and purchase histories to create detailed profiles of American, [Add something more about offline data practices/data brokers?]

(4) The problems of offline privacy are exacerbated by the greater speed and quantity of personal information exchange among businesses and other organizations today.

(5) Even when tracking of computers and Internet users does not collect overt identifiers, such as names and email addresses, the resulting information about users can still often be linked to identifiable individuals using IP addresses, cookies, and other techniques. Even without any collection of overt identifiers, an individual can be tracked from session to session, and the compiled information can be used to make decisions about the individual based on current and previous activities.

(6) Studies show that consumers are concerned about online privacy.

(A) A 2008 poll from the Consumer Reports National Research Center found: "72 percent are concerned that their online behaviors were being tracked and profiled by companies" and "93 percent of Americans think internet companies should always ask for permission before using personal information and 72 percent want the right to opt out when companies track their online behavior."[2]

(B) In 2009, the University of Southern California's Center for the Digital Future found in its eighth annual "Surveying the Digital Future" project that "almost

---

[1] The footnotes are so that staff can check the facts cited; they will not be part of the legislation.

[2] Consumers Union, "Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy," (September. 25, 2008, http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html.

all respondents continue to report some level of concern about the privacy of their personal information when or if they buy on the Internet."[3]

(7) Studies show that consumer want strong protections. A 2009 joint study by the University of Pennsylvania and the University of California-Berkeley found 69% of American adults feel there should be a law that gives people the right to know everything that a website knows about them and 92% agree there should be a law that requires "websites and advertising companies to delete all stored information about an individual, if requested to do so."[4]

(8) Consumers expect that the entities they transact with and the services they use will protect their privacy and will not sell or share their personal information without their express consent. Studies also show that there is confusion among consumers about companies' privacy policies and practices.

(A) The 2009 joint study by the University of Pennsylvania and the University of California-Berkeley found: "Americans mistakenly believe that current government laws restrict companies from selling wide-ranging data about them. When asked true-false questions about companies' rights to share and sell information about their activities online and off, respondents on average answer only 1.5 of 5 online laws and 1.7 of the 4 offline laws correctly because they falsely assume government regulations prohibit the sale of data."

(B) The 2008 Consumer Reports poll also found: "61% are confident that what they do online is private and not shared without their permission"; "57% incorrectly believe that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations"; and, "43% incorrectly believe a court order is required to monitor activities online."

(9) Commerce and technological innovation will suffer if businesses and other organizations, which depend on consumer trust, do not protect personal privacy. When users are kept informed about privacy policies and new services, companies can reduce the kind of customer surprise that leads to front-page horror stories, government investigations and fines, costly lawsuits, and loss of customers and business partners.[5]

---

[3] Center for the Digital Future, University of Southern California, "Surveying the Digital Future: Survey Highlights" (April 28, 2009), http://www.digitalcenter.org/pdf/2009_Digital_Future_Project_Release_Highlights.pdf.

[4] University of Pennsylvania and University of California at Berkeley, "Americans Reject Tailored Advertising and Three Activities that Enable It" (September 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[5] ACLU of Northern California, "Privacy and Free Speech: It's Good for Business" (February 2009), http://www.aclunc.org/docs/technology/privacy_and_free_speech_it%27s_good_for_business.pdf.

(10) Though the marketing industry has pointed to self-regulatory principles, released in July 2009 by the Interactive Advertising Bureau, as adequate consumer privacy protection, these industry-imposed self-regulatory principles do little to protect consumer privacy.[6] The effort is negated by the fact that there is no enforcement of these principles. Non-compliance merely results in "public reporting" of non-compliance. Companies ignoring the principles do not face meaningful consequences.

(11) Past industry attempts at privacy regulation have failed or been abandoned. Previous efforts that did nothing to protect consumer privacy include the Individual Reference Services Group, Privacy Leadership Initiative, Online Privacy Alliance, Better Business Bureau Online Privacy Seal, and the National Advertising Initiative from 2000.[7] FTC efforts to encourage self-regulation for privacy have done nothing to protect consumers.

(12) Existing law is inadequate to protect personal privacy because consumers are in a poor position to know who has access to or uses their personal information. Often consumers are not asked for their consent at all, are not asked for consent in a meaningful way, and have no effective knowledge about or control over the collection, maintenance, use, or disclosure of their information. Much information processing is undertakes by third parties that are wholly unknown to consumers.

(A) In 2010, it was revealed that several social-networking sites – including Facebook, MySpace, LiveJournal, Hi5, and Digg – sent to advertisers information such as site users' names or ID numbers tied to personal profiles without the users' knowledge or consent. To be clear: Users' names or ID numbers were embedded in the referring URLs to advertisers. A sample referring URL: http://www.facebook.com/profile.php?id=123456789&ref=name. Often, social-networking sites' user names are individuals' real names. For example, Facebook requires consumers to use their real names and personal data when creating a profile on the sites. Through this surreptitious process, advertisers learned if a specific person (and his or her age or other characteristics depicted on their profile page) clicked on a specific ad. This was not an unknown technical flaw.

(1) The privacy problem connected with sending referrer URLs had been identified as early as 1996 in a paper co-written by Tim Berners-Lee, the computer scientist who invented the Internet. "Because the source of a link may be private information or may reveal an otherwise private

---

[6] Interactive Advertising Bureau, "Self-Regulatory Principles for Online Behavioral Advertising" (July 2009), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf

[7] World Privacy Forum, "The NAI: Failing at Consumer Protection and at Self-Regulation" (2007), http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

information source, it is strongly recommended that the user be able to select whether or not the Referer field is sent."[8]

(2) A 2009 research paper detailed the privacy problem and explained that the "referer field" identification data could be combined with tracking cookie data to create a detailed history of the consumer's Web use. "First, since tracking cookies have been gathered for several years from *non*-[Online Social Networking (OSN)] sites as well, it is now possible for third-party aggregators to associate identity with those *past* accesses. Second, since users on OSNs will continue to visit OSN and non-OSN sites, such actions in the *future* are also liable to be linked with their OSN identity."[9] The end result is: Americans had no control over the social-networking sites' practice of sending personally identifiable user data without individuals' knowledge or consent.[10]

(B) In 2009, it was revealed that a company selling parental-control software (which parents install so that it reads private chats conducted through Yahoo, AOL and other Instant Messaging services) to gather the IM data to send back to the company. The company then offered the children's data for sale to businesses that market to children. The company argued parents could opt-out of this tracking and selling of their children's personal data, but the opt-out could only be found on the company's Web site; it was not included in the software given to the parents. Many were enraged to learn that this company surreptitiously tracked and sold their children's private data without their parents' knowing consent.

(13) Americans increasingly rely on the Internet for many aspects of their day-to-day lives, including banking, communicating with friends and family, and purchasing basis goods and services. Business, nonprofit organizations and religious and political groups also conduct their work over the Internet. Transactional records documenting these activities and associations are generated and collected by websites and other service providers. This transactional data reveals a great deal about Americans' personal beliefs as well as their private, religious and organizational lives.

(14) Some of their online activities involve sensitive matters such as health and finances. In these contexts, tracking people's every move online, including routine

---

[8] Tim Berners-Lee, Roy Fielding and Henrik Frystyk, "Hypertext Transfer Protocol — HTTP/1.0" (May 1996), http://www.rfc-editor.org/rfc/rfc1945.txt.

[9] Balachander Krishnamurthy and Craig E. Wills, "On the Leakage of Personally Identifiable Information Via Online Social Networks" (August 2009), http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf.

[10] Wall Street Journal, "Facebook, MySpace Confront Privacy Loophole" (May 21, 2010), http://online.wsj.com/article/SB10001424052748704513104575256701215465596.html.

use of search engines, is not simply a matter of convenience or relevance. It presents serious risks to consumers' privacy, security and dignity.

(15) Consumers' online and mobile interactions are compiled, analyzed, and combined with information from offline sources to create detailed profiles. In the United States, a consumer research firm (with information on 115 million American households) and a digital-marketing firm (with data on more than 150 million Internet users) planned in 2010 to merge online and offline data in order to create more detailed profiles of consumers for targeted behavioral advertising. The personal details gathered and tracked include consumer's age, sex, ethnicity, marital status and profession.[11]

[11] Wall Street Journal, "Exploring Ways to Build a Better Consumer Profile" (March 15, 2010), http://online.wsj.com/article/SB10001424052748703447104575117972284656374.html. Also occurring in the UK: Financial Times, "Yahoo and Nectar team up on adverts" (February 12, 2010), http://www.ft.com/cms/s/0/b0530e62-1775-11df-87f6-00144feab49a.html.