

A Bill to Require Internet Providers to Obtain “Opt-In” Consent to Use and Share Sensitive Consumer Information.

BE IT ENACTED BY THE CONGRESS HERE ASSEMBLED THAT:

SECTION 1. Internet Service Providers (ISPs) must obtain affirmative permission from consumers to use and share sensitive information.

SECTION 2. A. Sensitive information includes, but is not limited to: precise geo-location, health information, financial information, Social Security numbers, web-browsing history, application usage history, and the content of communication.

B. These regulations shall not impact privacy practices of websites or apps, like Twitter or Facebook, regulate other services of broadband providers, or address issues such as government surveillance, encryption, or law enforcement.

C. Customer consent shall be inferred when data is (1) used and shared to provide and market services and equipment typically marketed with broadband service subscribed to by the customer, (2) used to bill and collect for said service, and (3) used to protect the provider and its customers from fraudulent use of the provider’s network.

D. Use and sharing of non-sensitive information shall be subject to opt-out consent requirements.

SECTION 3. A. The Federal Trade Commission shall ensure that all data security requirements are met, while the National Institute of Standards and Technology will ensure that ISPs have reasonable measures in place to protect customer data from cyber-attacks.

B. ISPs shall be fined \$100 per violation not to exceed a total valuation of \$10 billion per fiscal year. Collected fines shall be earmarked for the Department of Homeland Security’s cyber-security initiatives.

SECTION 4. The data security requirements and notification of choice requirements will become effective within 90 days.

SECTION 5. All laws in conflict with this legislation are hereby declared null and void.

*Introduced by Rep. Alexandra B. Sencer, The Collegiate School (NY)
for the Harvard Debate Council Summer Workshops.*