Information Transparency and Personal Data Control Act

Consumer Data Privacy Today

Data privacy is a 21st Century issue of civil rights, civil liberties, and human rights and the U.S. has no policy to protect our most sensitive personal information. 70 percent of Americans believe that their personal data is less secure now than it was five years ago. Over a five-year period, 45 percent of Americans have had their personal information compromised in a data breach with limited to no accountability for those responsible.

Domestic Concern

In the absence of a federal policy, states are developing their own privacy laws, including California with the passage of its privacy legislation in 2018 and other states are following suite. A patchwork of state standards will only lead to confusion for consumers and small businesses.

International Problem

If we do not have a clear domestic policy, we will not be able to shape standards abroad, and risk letting others drive global policy. The EU has not been shy about their desire to have General Data Protection Regulation (GDPR) set the global standard for data protection.

That is why we need a national consumer data privacy standard, which ensures your most sensitive information is kept safe and that everyone is playing by the same rules.

What Will the Information Transparency and Personal Data Control Act Do?

Congresswoman Suzan DelBene (WA-01) introduced the Information Transparency and Personal Data Control Act. The legislation ensures our most sensitive personal information, including financial, health, genetic, biometric, geolocation, sexual orientation, citizenship and immigration status, Social Security Numbers, religious beliefs, and information pertaining to children under 13 years of age is kept safe. Key elements of the bill include:

Plain English: Requires companies to provide their privacy policies in "plain English."

Opt-in: Allows users to "opt-in" before companies can use their most sensitive private information in ways they might not expect.

Disclosure: Increases transparency by requiring companies to disclose if and with whom personal information will be shared and the purpose of sharing the information.

Preemption: Creates a unified national standard and avoids a patchwork of different privacy policies by preempting conflicting state laws.

Enforcement: Gives the Federal Trade Commission (FTC) strong rulemaking authority to keep up with evolving digital trends and the ability to fine bad actors on the first offense. Empowers state attorneys general to also pursue violations if the FTC chooses not to act.

Audits: Establishes strong "privacy hygiene" by requiring companies to submit privacy audits every 2 years from a neutral third party.