The Information Transparency & Personal Data Control Act

Rep. Suzan DelBene (D-WA)

Specifically, this legislation would accomplish the following:

1. Gives Consumers Control Over Their Data:
    a. Directs the Federal Trade Commission (FTC) to put forward regulations no more than 90 days after enactment, that require platforms to put in place opt-in protocols along with plain English privacy policy descriptions.
    b. An opt-in model will allow consumers to pick and choose who has access to their information and who doesn't.

2. Stronger Enforcement for Bad Actors:
    a. Makes the FTC the primary enforcer of consumer privacy. If the FTC does not act within 60 days of being notified of a violation, the enforcement authority opens to include state attorneys' general. This creates a safety net protecting consumers' data.
    b. Allows the FTC to fine companies who are in violation of federal privacy regulations on their first offense. Currently, companies can only be fined for their second violation of an FTC enforced rule.
    c. Provides FTC with additional resources to better protect consumer privacy. This bill will provide the FTC with 50 additional full-time personnel, 15 of which must be technical experts, and an additional $35 million in monetary resources.
    d. Requires companies to obtain privacy audits by a neutral third party and submit those results to the FTC every two years. This will ensure that businesses who collect, store, or share consumers' data are continuously keeping privacy top of mind.

3. Defining Data that is Worth Protecting
    a. This bill defines Sensitive Personal Information. Sensitive Personal Information encompasses genetic data, financial account information, geolocations, and information about religious beliefs and sexual orientation, and more.
4. Creates a National Standard:
    a. One federal standard will empower consumers to understand their rights in plain English and avoid confusion no matter where in the country they live.
    b. Empowers U.S. companies, large and small, to compete on a global stage by requiring them to abide by one clear standard instead of varying state-by-state data requirements.
    c. A national privacy standard will make conducting business in the U.S. less burdensome for startups.