The Consumer Data Protection Act of 2018 Discussion Draft - Senator Wyden

The explosive growth in the collection and sale of consumer information enabled by new technology poses unprecedented risks for Americans' privacy. The government has failed to respond to these new threats:

(1) Information about consumers' activities, including their location information and the websites they visit is tracked, sold and monetized without their knowledge by many entities;
(2) Corporations' lax cybersecurity and poor oversight of commercial data-sharing partnerships has resulted in major data breaches and the misuse of Americans' personal data;
(3) Consumers have no effective way to control companies' use and sharing of their data.

The Federal Trade Commission, the nation's main privacy and data security regulator, currently lacks the authority and resources to address and prevent threats to consumers' privacy.

(1) The FTC cannot fine first-time corporate offenders. Fines for subsequent violations of the law are tiny, and not a credible deterrent.
(2) The FTC does not have the power to punish companies unless they lie to consumers about how much they protect their privacy or the companies' harmful behavior costs consumers money.
(3) The FTC does not have the power to set minimum cybersecurity standards for products that process consumer data, nor does any federal regulator.
(4) The FTC does not have enough staff, especially skilled technology experts. Currently about 50 people at the FTC police the entire technology sector and credit agencies.

The **Consumer Data Protection Act** protects Americans' privacy, allows consumers to control the sale and sharing of their data, gives the FTC the authority to be an effective cop on the beat, and will spur a new market for privacy-protecting services. The bill empowers the FTC to:

(1) Establish minimum privacy and cybersecurity standards.
(2) Issue steep fines (up to 4% of annual revenue), on the first offense for companies and 10-20 year criminal penalties for senior executives.
(3) Create a national Do Not Track system that lets consumers stop third-party companies from tracking them on the web by sharing data, selling data, or targeting advertisements based on their personal information. It permits companies to charge consumers who want to use their products and services, but don't want their information monetized.
(4) Give consumers a way to review what personal information a company has about them, learn with whom it has been shared or sold, and to challenge inaccuracies in it.
(5) Hire 175 more staff to police the largely unregulated market for private data.
(6) Require companies to assess the algorithms that process consumer data to examine their impact on accuracy, fairness, bias, discrimination, privacy, and security.