The Mind Your Own Business Act of 2019

The explosive growth in the collection and sale of consumer information enabled by new technology poses unprecedented risks for Americans' privacy and U.S. national security. These threats include:

(1) Corporations' lax cybersecurity and poor oversight of commercial data-sharing partnerships has led to major data breaches and the misuse of Americans' personal data;

(2) Information about consumers, including their location information and the websites they visit is tracked, sold and monetized without their knowledge;

(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. The fines the FTC can impose for subsequent violations of the law are far too small to meaningfully deter misdeeds.

(2) The FTC does not have the power to set minimum cybersecurity standards for products that process consumer data, nor does any federal regulator.

(3) 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.

(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 **Mind Your Own Business Act of 2019** would protect Americans' privacy, allows consumers to control the sale and sharing of their data, give the FTC the authority to be an effective cop on the beat, and 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 who knowingly lie to the FTC.

(3) Create a national Do Not Track system that lets consumers stop companies from tracking them on the web, selling or sharing their data, or targeting advertisements based on their personal information. Companies that wish to condition products and services on the sale or sharing of consumer data must offer another, similar privacy-friendly version of their product, for which they can charge a reasonable fee. This fee will be waived for low-income consumers who are eligible for the FCC's Lifeline program.

(4) Give consumers a way to review the 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.