# **Summary of H.R. 4978, the *Online Privacy Act***

Congresswomen Anna Eshoo and Zoe Lofgren

The ubiquity of the internet has led to educational, social, and entrepreneurial opportunities. But it has also created a new scale of privacy issues that outmatch existing laws. Cambridge Analytica and the Equifax data breach are but two symptoms of a much larger problem.

Other countries and many states have taken important steps, but Congress must act. Reps. Anna Eshoo and Zoe Lofgren, who represent Silicon Valley, have introduced comprehensive privacy legislation that protects individuals, encourages innovation, and restores trust in technology companies.

## **Key Provisions**

- **Digital Privacy Agency (DPA).** The bill creates a new federal agency to enforce users' privacy rights and ensure companies follow the law. While unique for the U.S., this would be not the only privacy agency in existence. Every E.U. country has a privacy agency, and a California ballot initiative is proposing a new state agency. The DPA would be an independent agency with funding for up to 1,600 employees.
- **User Rights.** The bill gives users the right to:
  - access, correct, delete, and transfer data about them;
  - request a human review of impactful automated decisions;
  - opt-in consent for using data for machine learning / A.I. algorithms;
  - be informed if a covered entity has collected your information; and
  - choose for how long their data can be kept.
- **Company Obligations.** Companies must:
  - articulate the need for and minimize the user data they collect, process, disclose, and maintain;
  - minimize employee and contractor access to user data;
  - not disclose or sell personal information without explicit consent;
  - not use third-party data to reidentify individuals;
  - not use private communications, (e.g., emails and web traffic) for ads or other invasive purposes;
  - not process data in a way that violates civil rights, e.g., employment discrimination;
  - only process genetic information in limited circumstances;
  - use objectively understandable privacy policies and consent processes, and may not use 'dark patterns' to obtain consent;
  - employ reasonable cybersecurity policies to protect user data; and
  - notify the agency and users of breaches and data sharing abuses, e.g., Cambridge Analytica.
- **Enforcement**
  - The DPA can issue regulations to implement this bill and issue fines for violations.
  - The max money damage is the same as the FTC Act's max ($42,530 per incident).
  - State attorneys general may also bring civil actions for violations of this bill.
  - Individuals may sue for declaratory or injunctive relief; individuals (not acting collectively) may sue for damages.
  - Harmed individuals and States may appoint nonprofits to bring collective, private civil actions for damages on behalf of users.
- **Protections for Journalists.** Expressly allows journalists to use or disclose personal information for investigative journalism no differently than they do today. This applies so long as there are safeguards against using the information for non-journalistic purposes.
- **Additional Provisions.** The bill criminalizes doxxing; limits companies from using data to build behavioral profiles without consent; exempts small businesses from the most onerous requirements; prohibits the sale of government records with personal data without consent, and creates an Open Source Machine Learning Training Data Grant Program.