https://arstechnica.com/tech-policy/2019/11/new-bill-would-create-digital-privacy-agency-to-enforce-privacy-rights/

(United States – 116th Congress 1st Session)
New bill would create Digital Privacy Agency to enforce privacy rights

The bill proposes sweeping reforms to privacy rights and enforcement.

KATE COX - 11/5/2019, 5:07 PM

Chairwoman Anna Eshoo, D-Calif., conducts a House Energy and Commerce Subcommittee on Health markup on Thursday, July 11, 2019. | Photo by Tom Williams – CQ Roll Call – Getty Images

https://arstechnica.com/tech-policy/2019/11/new-bill-would-create-digital-privacy-agency-to-enforce-privacy-rights/

Congress is taking yet another stab at addressing the near-complete lack of federal laws covering the absolutely massive trove of data that companies now collect on every one of us, which forms the backbone of basically the entire big tech era.

Representatives Anna Eshoo and Zoe Lofgren, both Democrats from California, introduced the Online Privacy Act today. The act would create a new federal agency, the Digital Privacy Agency, to enforce privacy rights. The act would also authorize the agency to hire up to 1,600 employees.

"Every American is vulnerable to privacy violations with few tools to defend themselves. Too often, our private information online is stolen, abused, used for profit, or grossly mishandled," Eshoo said in a statement. "Our legislation ensures that every American has control over their own data, companies are held accountable, and the government provides tough but fair oversight."

"Our country urgently needs a legal framework to protect consumers from the ever-growing data-collection and data-sharing industries that make billions annually off Americans' personal information," Rep. Lofgren added. "Privacy for online consumers has been nonexistent—and we need to give users control of their personal data by making legitimate changes to business practices."

The Online Privacy Act

The provisions in the bill (PDF - Online Privacy Act) would apply to "any entity (including nonprofits and common carriers) that intentionally collects, processes, or maintains personal information AND transmits personal information over an electronic network."

Under the terms of the OPA, individuals would have the right to obtain, correct, and delete data collected about them by covered entities, as well as to request "a human review" of automated decisions. Users would also have to opt-in to having their personal data used for training machine learning algorithms. They would be able to choose for how long companies retain their data.

The bill distinguishes between aggregated data and personal, identifiable data that is tied to an individual, and it places strong limitations on use of the latter. As outlined in a one-page fact sheet, the OPA would:

https://arstechnica.com/tech-policy/2019/11/new-bill-would-create-digital-privacy-agency-to-enforce-privacy-rights/

- articulate the need for and minimize the user data [covered entities] 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

The Privacy Mess

Privacy law in the United States today is a patchwork of regulation, and the end result is basically a hot mess that leaves agencies with limited authority to investigate and penalize even egregious abuses of personal data.

The federal statutes that exist each cover a specific, limited kind of data and enumerate a specific, limited kind of entity that's obligated to protect that data. So for example, while your doctor's office can't sell information about your diagnoses to a third party, no such limitation applies to apps or wearable devices that collect the same kinds of data.

A handful of states have additional laws on the books. Illinois, for example, adopted a prescient law back in 2008 that regulates the collection and use of individuals' biometric data. Facebook since 2015 has been embroiled in a class-action lawsuit in that state over its use of facial recognition.

The biggest player at the state level is California, which in 2018 adopted a sweeping privacy law that would give individuals more control over how their personal data is collected, used, and sold. That law has survived several attempts by opponents to weaken its key provisions, and it goes into effect on January 1.

https://arstechnica.com/tech-policy/2019/11/new-bill-would-create-digital-privacy-agency-to-enforce-privacy-rights/

Representatives Eshoo and Lofgren are far from the first to propose new federal legislation to address the morass. In fact, they're not even the first this year. Sen. Ron Wyden (D-Ore.) last month introduced the Mind Your Own Business Act, which not only seeks to introduce new standards for user privacy and how data is handled, but would also impose criminal penalties, including jail time, on the leadership of companies that fail to comply.

Sen. Marco Rubio (R-Fla.) also introduced a privacy-related bill earlier this year. His American Data Dissemination Act would create a process and timeline for the Federal Trade Commission to establish privacy rules, rather than actually establishing new rules. It would also prohibit any state from enforcing its own law related to the same kinds of data as the federal law, something many big tech companies strongly support.

KATE COX Kate covers tech policy issues, including privacy, antitrust, and other shenanigans, from Washington, DC.
EMAIL kate.cox@arstechnica.com