COMPREHENSIVE FEDERAL PRIVACY LEGISLATION

Limiting Unfair Data Practices

CENTER FOR DEMOCRACY & TECHNOLOGY

How many devices, apps, and digital services have you used today? Do you know what data you've shared with whom, and how it will be used a year from now? We've seamlessly integrated technology into every facet of our lives while tasking everyday users with navigating every pop-up, privacy policy, and setting. This is fundamentally unfair and unworkable. It's time to decide to put in place some purpose limitations and prohibitions on secondary collection and use that exist outside of our broken "notice and consent" model.

Location data provides a good example. It reveals everywhere we work, play, and pray. It is collected by our devices, our ISPs, and many of the apps and websites we use. While location data can enable useful services like maps, weather, and localized news, it is often sold or repurposed for other things, like marketing and even surveillance. Individuals want to protect their location but have few effective ways to maintain any control over it. The New York Times, for example, reported how apps that request permission to use location data to provide local news or weather buried details about how that information could be shared and repurposed by many other companies.

This challenge applies to other types of data like biometrics, health information, email contacts, private messages, photos, and more:

- Bloomberg reported that some menstruation tracking apps, which prompt users to enter all kinds of health information, sell that data to advertisers or use it to market fertilization services. Ironically, users reported feeling like the apps were more discreet than tracking menstruation in a notebook. Unlike healthcare providers, these apps are not required to follow HIPAA privacy and security rules.

- A Privacy International study found that some Android apps automatically sent personal information to Facebook, even when users were logged out of Facebook or did not have Facebook accounts. The KAYAK app, for example, shared detailed flight search information.

CDT's proposed privacy legislation would prohibit unnecessary processing or repurposing of the following types of information:

- Precise geolocation information
- Biometric identification
- Health information
- Probabilistic cross-device tracking
- Children's information, particularly for ad targeting
- Audio and visual recordings
- Contents of and parties to communications (who you're communicating with and what you're saying).

>_ CDT'S PRIVACY LEGISLATION

For more info on CDT's efforts to create comprehensive federal privacy legislation, visit http://bit.ly/CDTfedpriv or contact Michelle Richardson at mrichardson@cdt.org.