Online Consumer Privacy and a Way Forward

As social media companies and search engines have ushered in an age of digital engagement, more and more personal data has been collected by internet edge providers. While the use of personal data enlivens the consumer internet experience and facilitates a broad range of internet functionality with applications such as real-time directions, it has also sparked concerns about privacy and just what the government should do to prevent abuses.

In today's internet ecosystem, internet service providers (ISPs), search engines, and social media platforms have different capabilities, with some being able to amass more sensitive information about individual users than others. Today, ISPs have less power to "look into" their users' private information than many edge companies.

The most commercially valuable personal information is harvested from social networks and internet searches as edge companies combine data they've gathered to form insights into a wide range of consumer behaviors across multiple devices and platforms.

Social media and other edge companies have access to a treasure trove of sensitive personal information. By contrast, encryption, virtual private networks, and other technological barriers, coupled with consumers' dependence on Wi-Fi hotspots and their desire to use multiple devices and different service providers, block ISPs from seeing all but a fraction of an individual's activity on any single device.[1]

At the same time, companies like Google, Facebook, Amazon, and Microsoft collect reams of high-quality data that when combined with machine learning techniques allow them to produce an intimate depiction of those using their services. In the cases of Google and Facebook this adds up information on billions of users, and with eight of the top 10 most popular mobile apps in the U.S. owned by those two companies, they touch nearly everyone who uses the internet – even when they aren't using those services.[2]

As lawmakers rewrite our nation's privacy rules, welding them into one nationwide law, they need to keep in mind the data collection capabilities of the different parts of the internet ecosystem. The new privacy law should protect individuals from abuses, but it must also rationalize and unify a splintered legal regime that sows confusion and is becoming less and less workable.

A new federal law needs to consider who really amasses our personal data and how they use it, and it should put enforcement power in the hands of Federal Trade Commission – the government's privacy expert. That way we can enjoy the full range of internet functionality without concern that our personal data is being abused.

Online Consumer Privacy and a Way Forward

As a starting point, the Business Roundtable has recently proposed a Privacy Framework that could serve as an outline for new federal legislation.

Any congressional legislation on privacy should:

- Provide one set of rules on privacy that applies to all companies in the internet ecosystem
- Apply no matter where a consumer is on the internet
- Apply no matter how a consumer accesses the internet
- Explicitly confer jurisdiction to the FTC, the expert agency in consumer protection
- Include robust privacy protections

The Business Roundtable framework achieves these goals through four main principles:

1

Champion Consumer Privacy and Promote Accountability.

It should include robust protections for personal data that enhance consumer trust and demonstrate U.S. leadership as a champion for privacy by including clear and comprehensive obligations regarding the collection, use, and sharing of personal data, and accountability measures to ensure that those obligations are met.

2

Foster Innovation and Competitiveness.

It should be technology-neutral and take a principles-based approach in order for organizations to adopt privacy protections that are appropriate to specific risks as well as provide for continued innovation and economic competitiveness in a dynamic and constantly evolving technology landscape.

3

Harmonize Regulations.

It should eliminate fragmentation of regulation in the United States by harmonizing approaches to consumer privacy across federal and state jurisdictions through a comprehensive national standard that ensures consistent privacy protections and avoids a state-by-state approach to regulating consumer privacy.

4

Achieve Global Interoperability.

It should facilitate international transfers of personal data and electronic commerce and promote consumer privacy regimes that are interoperable, meaning it should support consumer privacy while also respecting and bridging differences between U.S. and foreign privacy regimes.

1. https://www.iisp.gatech.edu/working-paper-online-privacy-and-isps
2. https://www.law.upenn.edu/live/files/7952-kearns-finalpdf; https://www.recode.net/2017/8/24/16197218/top-10-mobile-apps-2017-comscore-chart-facebook-google; https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf; https://newsroom.fb.com/news/2018/04/data-off-facebook/