Big Tech's Shift to Privacy

An overview of the technology sector's recent public expressions of privacy initiatives and values.

Facebook

Transparent product development & private messaging.

- Shift from public one-to-many communications to private one-to-one messaging.
- Six principles: private interactions, encryption, reduced permanence, safety, interoperability, secure data storage.
- "Simpler platform ... focused on privacy" — specifically, encrypted services.
- Reducing permanence: "[W]e won't keep messages or stories around for longer than is necessary to deliver the service or longer than people want them."
- Interoperability between Facebook's messaging services.
- Commitment to transparently develop changes to the platform and the company's products in a manner consistent with the expressed goal of increasingly private interactions.
- Encryption.

Stance on federal privacy law:
Supports a common global framework, including new privacy regulation in the U.S.

Microsoft

User choice & control, pervasive values, transparent documentation.

- "Privacy is a fundamental human right."
- Six principles: control, transparency, security, strong legal protections, no content-based targeting, benefits to you.
- Commitment to transparency, providing "meaningful choices" and user "control"; for example:
  - Categorizing data as "required" or "optional" and presenting relevant choices for the collection of each to a user.
  - Product documentation that explains why "required" data is necessary.
  - Biannual data collection report with emphasis on explanation of data collection practices.
- Sensor-level access controls in Windows privacy settings.
- Consolidated homepage to find Microsoft services-specific settings pages.
- Stated position: Platform providers have a collective responsibility to "[t]hink ... about trust in everything we build."
- Consumer-accessible details about the company's development processes and contractual commitments.

Stance on federal privacy law:
Supports a "strong federal law" that is "worthy of preemption."

Apple

On-device processing, encryption, developer guidelines.

- "Privacy is a fundamental human right."
- On-device processing and broad use of encryption.
- Emphasis on strict privacy guidelines for developers and user-controlled permissions; enforcement within the App Store.
- Machine learning to limit third-party cookie tracking in Safari browser.
- Differential privacy.
- "Sign In with Apple" allows for third-party sign-in without revealing user's email address.

Stance on federal privacy law:
Supports comprehensive federal privacy legislation that reflects privacy as a fundamental human right.

Google

Data access & control.

- Easy access to user controls and incognito mode.
- Centralized "Google Account" to access data stored and saved.
- Quick access to sharing settings from most apps/services.
- User-controlled auto-deletion.
- Emphasis on federated learning to train algorithms and on-device processing.
- Differential privacy, including open-source TensorFlow Privacy library.
- Make two-factor authentication more accessible.
- Commitment not to sell personal information to third parties.

Stance on federal privacy law:
Supports comprehensive federal privacy legislation.

This review is not an assessment and comparison of each company's privacy notice and associated disclosures; rather, its focus is on each company's promotional efforts to communicate its approach to privacy. The omission of a value or privacy strategy from a company's column does not necessarily indicate that the company does not hold that value or practice that strategy. Instead, it is indicative of the fact that the company chooses to emphasize to consumers different elements of its approach to privacy.

Please view the **sources used in this review** for more details.

iapp