Google Privacy & Security interfaces

Dominic Battré
Robert Brauer
Google Privacy Principles

1. Use information to provide our users with valuable products and services.
2. Develop products that reflect strong privacy standards and practices.
3. Make the collection of personal information transparent.
4. Give users meaningful choices to protect their privacy.
5. Be a responsible steward of the information we hold.
Where we involve these principles

Account Management

3rd-party Permissions

Chrome
Account management

“What does Google know about me?”

“Is my data safe with Google?”

“What is Google using my data for?”

“How do I get rid of things?”
Account Dashboard

Providing a looking glass and management for data connected to a Google account
Account History

Curated control for privacy-sensitive collection of important data types
Secure your account

Proactively helping people to get their account into a secure state
Data Liberation

Giving users full control over their personal account data
3rd-party permissions

“What data am I sharing?”

“What is this [service] doing with my information?”

“Why does [service] need this permission?”

“How can I make sure that I can trust this app?”
Sign in with Google

Supporting data sharing opportunities while keeping up awareness
We are working to make Chrome the most privacy-aware browser in the world by providing transparency and control over information you share when you're online.

- User Education
- Privacy Reviews and Documentation
- Privacy Features
Chrome Privacy

- **Past**
  - Extension APIs, Content Settings, Click to Play, DNT

- **Present**
  - Identity Management
  - Incognito Mode
  - W3C WebAppSec: Content Security Policy, Mixed Content, Subresource Integrity, Credential Management
Thanks

Dominic Battré
Robert Brauer