LEADERSHIP CENTER FOR ATTORNEY GENERAL STUDIES

Rethinking Digital Privacy: Why "Consent" Isn't Enough and How We Can Do Better

Authors: AG Studies Staff and Policy Fellows

In today's hyper-connected world, our personal information is constantly being collected, used, and shared online. From the apps on our phones to the websites we visit, we leave digital footprints everywhere. We are often told that we're in control, thanks to privacy policies and consent buttons we click. But how much control do we really have? And is the current system truly protecting our interests? Evidence suggests it's falling short, and as technology like artificial intelligence (AI) becomes more integrated into our lives, the need for a better approach is becoming urgent. This essay explores the shortcomings of current privacy rules, proposes better alternatives, and discusses how key state officials, like State Attorneys General, can help drive these necessary changes.

The Illusion of Control: Why Current Privacy Rules Fail Us

For decades, privacy protection has revolved around the idea of "consent." You've encountered it countless times: the pop-up asking you to accept cookies, the lengthy privacy policy you scroll past, the checkboxes you tick. Generally, these methods fall into three categories:

Implied Consent: This assumes you're okay with data collection unless you actively object. The problem? Most people don't proactively manage dozens of privacy settings across different sites and apps.

Informed Consent: This requires companies to give you "clear" information before you agree. However, studies show this often creates a false sense of security. Seeing a policy might make us think we're protected, leading us to share more data, even if we don't fully grasp the implications hidden in the fine print. Who has time to read, let alone understand, pages of legalese for every service they use?

Empowered Consent: This aims to give users more active control, requiring explicit clicks or choices. Paradoxically, research indicates that even when given more control and information, people sometimes end up disclosing more personal information, perhaps because the extra steps build trust in the platform, regardless of its actual practices.

The core issue is that these models rely on assumptions about how people behave online that don't match reality. We face decision fatigue – it's overwhelming to constantly make choices about privacy. We often lack the time or expertise to understand what we agree to. And as AI agents and interconnected smart devices become more common, asking for consent for every single interaction becomes impractical and potentially meaningless. How can you meaningfully

consent when an AI assistant is making decisions and sharing data on your behalf in complex ways you can't easily track?

A Path Forward: Privacy by Default and Clearer Communication

If the current system isn't working, what's the alternative? Two promising ideas are gaining traction: device-centric privacy and narrative-based communication.

Device-Centric Privacy: Imagine setting your core privacy preferences once, when you set up a new phone or computer, rather than app by app. This approach focuses on building privacy from the start:

- Setup Choices: Key privacy settings (like location tracking or data sharing permissions) could be configured during the initial device setup.
- Privacy-Forward Defaults: Instead of settings defaulting to maximum data collection (opt-out), they could default to maximum privacy (opt-in), requiring you to actively choose to share more.
- Universal Controls: Mechanisms like the Global Privacy Control could allow you to signal your preferences automatically across websites and services that respect the signal.

Narrative-Based Privacy Communication: Instead of dense legal documents, imagine clear, simple explanations – perhaps short videos, comics, or relatable scenarios – showing exactly how your data might be used, stored, or sold in different situations. Standardizing these "privacy stories" across platforms could make it much easier for everyone to quickly understand the real-world impact of their choices.

These approaches shift the burden away from the individual having to be a constant privacy watchdog and place more responsibility on tech companies to build privacy into their products from the ground up. It’s about making privacy the easy, default choice, not an obstacle course.

Why This Matters to You (and How State Attorneys General Can Help)

This isn't just a technical issue; it's about your right to control your personal information and navigate the digital world safely. Better privacy defaults mean less worry about hidden data collection, fewer overwhelming pop-ups, and more genuine control over your digital life. It reduces the risk of your data being misused or ending up in unexpected places.

State Attorneys General often play the role of chief consumer protection officers, and they have a critical role to play in making this shift happen. They can:

- Investigate and Educate: Launch inquiries into how current consent mechanisms are failing consumers and educate lawmakers and the public about the need for change.

- Champion New Frameworks: Work with experts, consumer groups, and industry stakeholders to develop practical guidelines for device-centric and narrative-based privacy.

- Promote Pilot Programs: Encourage or propose legislation for pilot programs with tech companies to test and refine these new approaches.

- Develop Standards: Push for standardized "privacy narratives" and clear metrics to ensure companies are implementing these measures effectively.

- Enforce Consumer Protection: Use their existing authority to protect consumers from deceptive privacy practices and advocate for stronger laws that incorporate privacy-by-default principles.

- Create Feedback Channels: Establish easy ways for consumers to report privacy violations and provide feedback on what's working and what isn't.

The current approach to digital privacy isn't sustainable. By embracing privacy-by-default settings at the device level and demanding clearer, narrative-based explanations, we can create a digital environment that respects user autonomy and genuinely protects our information. State Attorneys General are key allies in this effort, capable of driving the research, regulation, and enforcement needed to turn these better ideas into reality.

Sources and Additional Readings:

1. Josh Golin & Jeff Chester, *Device-Level Age Verification Is Our Best Shot at Protecting Kids Online | Opinion*, Newsweek (Mar. 13, 2025), https://www.newsweek.com/device-level-age-verification-our-best-shot-protecting-kids-online-opinion-2001748.
2. Alex Weinert, *Raising the baseline security for all organizations in the world*, Microsoft Tech Cmty. (Apr. 13, 2023), https://techcommunity.microsoft.com/blog/identity/raising-the-baseline-security-for-all-organizations-in-the-world/3299048.
3. *About Global Privacy Control*, Glob. Privacy Control, https://globalprivacycontrol.org/#about (last visited Apr. 14, 2025).
4. Sang Ho Suh et al., *PrivacyToon: A Privacy Policy Summarization and Visualization Framework based on Comics Metaphor*, https://sanghosuh.github.io/papers/privacytoon.pdf (last visited Apr. 14, 2025).
5. Phillip Ramati, *Federal laws needed to protect users from confusing privacy policies, research shows*, The Den (Feb. 21, 2024), https://den.mercer.edu/federal-laws-needed-to-protect-users-from-confusing-privacy-policies-research-shows/.