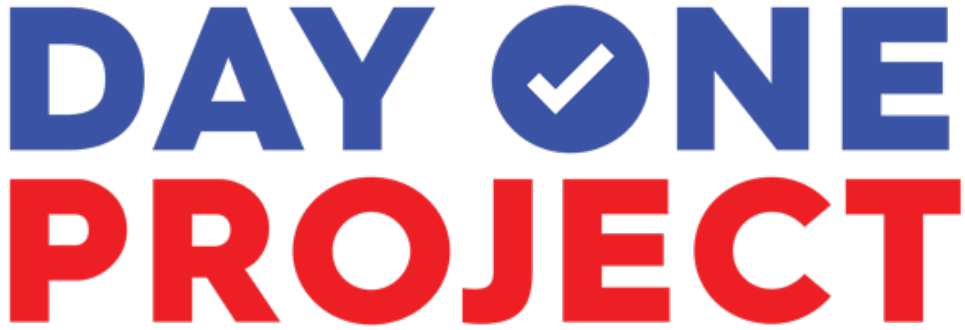

Eliminating Cookie Click-Thrus: A Strategy for Enhancing Digital Privacy

Meg Leta Jones

December 2020

The Day One Project offers a platform for ideas that represent a broad range of perspectives across S&T disciplines. The views and opinions expressed in this proposal are those of the author(s) and do not reflect the views and opinions of the Day One Project or its S&T Leadership Council.

Summary

Everyone hates cookie notifications, click-thrus, and pop-ups. While cookies[1] give the web more functionality, their excessive use and attendant consent system can interfere with user experience and raises serious privacy concerns. The next administration should commit to *finally* resolving these and related issues by creating a digital privacy task force within the White House Office of Science and Technology Policy (OSTP). The task force would coordinate relevant agencies—including the Federal Trade Commission, Federal Communications Commission, and Department of Commerce—in working with Congress, state actors, and European Union partners to develop meaningful data-privacy protections.

Challenge and Opportunity

Cookie notifications are the irritating pop-up windows that appear when visiting many websites (Figure 1). These pop-ups aren't just problematic because they're annoying. Rather, they represent a clear failure on behalf of both the private sector and the government to take internet privacy seriously. By notionally providing users the opportunity to opt out, opt in, or otherwise control cookie tracking, cookie notifications provide cover for companies to track consumer behavior on the web to an astonishingly extensive and invasive degree. These notifications are emblematic of broader underlying issues with digital privacy.

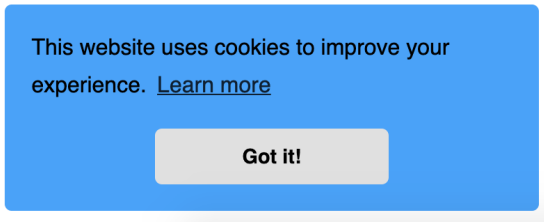

Figure 1. Example of a cookie notification.

Issue 1. Americans are not satisfied with existing privacy protections. Americans have been concerned about their digital privacy for over two decades. A 2000 Pew study found that 86% of Americans supported opt-in privacy policies and 54% reported that tracking users is harmful and invasive.[2] Although efforts have been introduced by internet platforms and advertisers to create limited opt-out strategies, Pew found in 2019 that "roughly eight-in-ten or more U.S. adults say they have very little or no control over the data that the government (84%) or companies (81%) collect about them."[3]

[1] A cookie is a string of data passed by a web server to an individual user's web browser when the user visits a website. Web browsers store these data strings on the user's computer hard drive, then pass them back to the server when the user revisits or further explores the site. Cookies can personalize the user's web experience by recording and remembering the user's activity (for instance, by keeping items in a shopping cart even if the user navigates away from the store webpage), but can also be used to track an individual's web activity without their consent. Bad actors who illicitly gain access to cookies can also use those cookies to spy on users.

[2] Fox, S. (2000). Trust and privacy online: Why Americans want to rewrite the rules. Pew Research Center, August 20.

[3] Auxier, B.; et al. (2019). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research Center, November 15.

Issue 2. **The notice and consent strategy is not working to protect privacy.** Many companies "check the box" of digital privacy by simply notifying users of the ways in which their digital data are being used (e.g., via cookie notifications or by displaying a privacy policy) and requiring users to consent (e.g., via clicking out of a cookie notification or hitting the "agree" button at the bottom of a privacy policy). This approach does not protect digital privacy in any meaningful way. Years of survey research show that well over half of Americans mistakenly believe that the existence of a privacy policy means that a website will not share personal information with other websites or companies at all—when in fact a privacy policy simply states how that information is or is not being shared.[4] Other research has shown significant inconsistencies in the interpretation of privacy policies by experts and non-experts.[5] The fact that few members of the general public understand the details of privacy policies is unsurprising. In 2009, researchers calculated that it would take 76 work days for users read every privacy policy on every unique site they visited.[6] These challenges create insurmountable problems for privacy self-management[7] and have led to "privacy resignation".[8] In other words, internet users don't make an active choice to grant access to their data in exchange for the benefits of a service—we simply feel helpless to do otherwise.[9]

Issue 3. **Americans want stronger data-privacy protections.** Polling consistently reveals near-universal demand for privacy legislation. The 2019 Pew report found that 79% of Americans are not confident "that companies will admit mistakes and take responsibility when they misuse or compromise data", and that 75% are not confident that companies "will be held accountable by government if they misuse data".[10] A multiyear survey from Morning Consult found that 79% of registered voters want Congress to prioritize a bill to improve protection for online data.[11]

Issue 4. **The United States faces tension with the European Union (EU) over data protection.** The EU's 2018 General Data Protection Regulation changed the definition of consent for cookies. This change is one of the main reasons why cookie notifications have recently proliferated on the global internet. Today, EU law specifically regulates cookies via the ePrivacy Directive. An ongoing effort to update this directive presents a great opportunity for transatlantic compromise

[4] Turow, J.; Hennessy, M.; Draper, N. (2018). Persistent misperceptions: Americans' misplaced confidence in privacy policies, 2003–2015. Journal of Broadcasting & Electronic Media, 62(3): 461–478.
[5] Reidenberg, J.R.; et al. (2015). Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding. Berkeley Technology Law Journal, 30.
[6] And this was back when users spent only an average of 75 minutes a day online. See McDonald, A.M.; Cranor, L.F. (2008). The cost of reading privacy policies. I/S: A Journal of Law and Policy for the Information Society, 4(3): 543–568.
[7] Solove, D. (2013). Privacy Self-Management and the Consent Dilemma. Harvard Law Review, 126: 1880–1903.
[8] Draper, N.A.; Turow, J. (2019). The corporate cultivation of digital resignation. New Media & Society, 21(8): 1824–1839.
[9] In a 2015 survey, 91% of adults disagreed with the statement that "if companies give me a discount, it is a fair exchange for them to collect information about me without my knowing," and 66% reported that they do not want advertisements "tailored to their interests." See Turow, J.; Hennessy, M.; Draper, N. (2015). The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation. Annenberg School for Communication Departmental Paper.
[10] Auxier, B.; et al. (2019). Americans and Privacy.
[11] A 2019 Morning Consult poll shows almost identical numbers to its 2018 findings. See Sabin, S. (2019). Most Voters Say Congress Should Make Privacy Legislation a Priority Next Year. Morning Consult, December 18. https://morningconsult.com/2019/12/18/most-voters-say-congress-should-make-privacy-legislation-a-priority-next-year/.

and consistency with regard to digital data protection.[12] Cookies remains a sticking point between the United States and the EU in these negotiations. An internationally harmonized approach to cookie consent is needed to ensure that the global web protects user privacy without being overly detrimental to user experience.

Plan of Action

The next administration should establish a digital privacy task force within the White House Office of Science and Technology Policy (OSTP). The task force would focus on replacing cookie notifications with more meaningful digital-privacy protections. This concrete goal would spur progress on three broader outcomes:

(1) Stronger political drive to address American demands for online privacy.
(2) International coordination—especially with the European Union—around strategies for protecting digital data.
(3) Effective White House leadership on future digital policy issues.

To rid the internet of cookie notifications and establish itself as a leader on digital policy, the next administration will need to grapple with tough technical, political, and societal issues. Collaboration will be required across key agencies (including the Federal Trade Commission (FTC), Federal Communications Commission (FCC), and Department of Commerce (DOC)), as well as with members of Congress, EU officials, state actors, browser developers, companies, civil liberties groups, and academics. The next administration can also build on existing policy efforts to strengthen digital privacy. Such policy efforts include federal bills like the SAFE DATA Act[14] and the Online Privacy Act;[15] state initiatives (especially legislative efforts in California and Illinois); and international negotiations around transborder data flows to the United States and related to the EU's ePrivacy Regulation.

Implementation should be carried out across five key components:

(1) **Build**: The White House should spearhead this initiative by creating a knowledgeable and motivated taskforce that includes members from the FTC (where these efforts have been housed to date with limited success), the FCC (where privacy in communication may be suitably addressed but has had a limited role), and DOC (where prior administrations have situated negotiations with the EU).
(2) **Lead**: The taskforce should be led by a designated member of the OSTP.
(3) **Organize**: The taskforce will need to organize existing efforts across the states, congress, and the European Union.

[12] Jones, M.L.; Lee, J. (2020). Comparing Consent to Cookies: A Case for Protecting Non-Use. Cornell International Law Journal, 53(1).
[14] SAFE DATA Act of 2020, S. 4626, 116th Congress (2019–2020).
[15] Online Privacy Act of 2019, H.R. 4978, 116th Congress (2019–2020).

(4) Drive: The taskforce will need to keep momentum going on this effort and maintain the dual goals of providing a better user experience and meaningful data privacy

(5) Mobilize: Non-federal actors will need to be invested in this effort and prepared to implement a unifying solution by technology industry players large and small, browsers, civil liberty groups, academics and activists.

Frequently Asked Questions

Haven't we tried fixing the cookie-consent system before?

Yes, but it didn't work. In 2010, the Federal Trade Commission became involved in a Do Not Track (DNT) initiative that would allow users to opt out of data collection. A multi-stakeholder working group was created to figure out the details of the initiative. After years of back and forth, the group finally came up with a recommendation in 2016, which resulted in most browsers including a "Do Not Track" setting that users can turn on today. But very few sites actually respect the setting. For instance, Google Chrome has a Do Not Track setting, but Google websites ignore it.

We have made progress in the ten years since the DNT initiative was conceptualized. A user's decision to stay on a site used to be considered implicit consent to tracking (and still is in some places), but pressure from states like California and international actors like the European Union have changed compliance demands and user experiences. The broader technology, social, and political landscapes have changed as well. Today, Silicon Valley is viewed with skepticism as well as admiration, international cooperation is needed to resolve the most basic arrangements for crossborder data transfers, and states are passing computer-privacy laws across a range of contexts for the first time.

Why not leave this to companies or states?

Although California and the European Union have passed laws in recent years to create meaningful consent, the problems with cookie click-thrus are due to a lack of coordination. The ePrivacy Directive and GDPR present one set of confusing demands and the new California law presents another, meanwhile other states are debating bills and the EU is turning the ePrivacy Directive into an ePrivacy Regulation. Additionally, some members of Congress have shown interest in passing federal data protection and privacy legislation that include various practices around consent. Each negotiation touches on how browser settings might be used to provide consent, but no standard has been established. So inconsistent and often meaningless consent notifications continue to get in the way of a better user experience. Even though self-regulation is often considered a failure in this space, companies, non-profits, and activists could play an important role in standardizing user engagement. These efforts need to be coordinated.

About the Author

Meg Leta Jones is an Associate Professor in the Communication, Culture & Technology Department at Georgetown University, where she researches rules and technological change with a focus on privacy, memory, innovation, and automation in digital information and computing technologies. She is also a faculty fellow in the Georgetown Ethics Lab, core faculty member of the Science, Technology, and International Affairs program in Georgetown's School of Foreign Service, an affiliate faculty member at the Institute for Technology Law & Policy in the Georgetown Law Center, and visiting affiliate faculty at the Brussels Privacy Hub at Vrije Universiteit Brussel.

Meg holds a Ph.D. in Technology, Media, and Society from the University of Colorado's School of Engineering & Applied Sciences and a J.D. from the University of Illinois. Her research covers comparative information and communication technology law, critical internet and algorithm studies, governance of emerging technologies, and the legal history of technology. Her first book, *Ctrl+Z: The Right to be Forgotten* is about the social, legal, and technical issues surrounding digital oblivion. Her next book, *Cookies*, tells the transatlantic history of digital consent through a familiar technical object. More details about her work can be found at her at research site iSPYLab.net.

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans, and readying them for Day One of the next presidential term. For more about the Day One Project, visit **dayoneproject.org**.