Harvard Journal of Law & Technology
Volume 39, Number 1 Fall 2025

BAN COOKIE BANNERS: A CASE STUDY IN TECH REGULATION[†]

Kate Klonick[*]

ABSTRACT

Few experiences on the modern internet are as universally reviled as the cookie banner. They clutter websites with pop-ups, interrupt user flow, make information harder to access, and demand repetitive, meaningless clicks. What was once heralded as a tool to advance individual autonomy and privacy has, in practice, become a daily annoyance that breeds cynicism with the very concept of consent itself. Cookie banners do not empower; they weary. They do not inform; they obscure. They do not prevent surveillance; they normalize it.

The tragedy of the cookie banner is that it embodies the best intentions but worst solutionism of modern regulation: the fantasy that complex problems such as digital surveillance can be solved by forcing individuals to click "I agree." At best, this fantasy has produced a regime of performative compliance that neither informs users nor limits data exploitation and degrades internet usability. But at worst, it has crowded out more substantive reforms by offering the illusion of protection while leaving surveillance capitalism intact. Government can point to the highly visible cookie banner and declare its promise met in addressing data privacy issues. Industry, now that a compliance solution has been agreed on and normalized, prefers a known system with which they can easily comply and are unmotivated to push for a reform. While users, faced with endless click-throughs, learn not to assert their rights but to surrender them reflexively. In this sense, cookie banners are not merely bad design. They are a cautionary tale of regulatory failure. Born from European data protection laws, exported worldwide through market forces, and mirrored in other government regulations, banners represent the triumph of ritual over reality in technology law.

To this end, this Article argues one thing and one thing only: that cookie banners should be abolished. They do not protect privacy, they erode meaningful consent, and they impose unnecessary costs on information access, usability, and even the environment. Most of all,

---

[†] Response to: Robin Bradley Kar & Xiaowei Yu, *The Contractual Death and Rebirth of Privacy*, 38 HARV. J.L. & TECH. 1103 (2025).

[*] Associate Professor of Law, St. John's University School of Law. The author is grateful to Ryan Calo, Dave Hoffman, Daphne Keller, Meg Leta-Jones, Larry Lessig, Jack Balkin and the Yale Information Society Project and Paul Schwartz and his privacy seminar at University of Berkeley Law School for helpful comments on this Article.

their existence stands in the way of future progress and a new regulatory solution. In order to understand how regulation can go so wrong — and how to move beyond it — this Article traces the history of cookie banner mandates, catalogues their failures, and makes a simple plea: to end cookie banners so that the law can move towards new interventions to protect individuals' privacy with something more than a hollow click.

TABLE OF CONTENTS

I. INTRODUCTION

In the 1990s and early 2000s, the internet was plagued by a scourge of pop-up advertisements. They were intrusive, manipulative, and universally despised — so much so that Ethan Zuckerman, the man credited with inventing the pop-up ad, has publicly expressed regret for unleashing them and begged forgiveness.[1] For younger users, this era is a half-forgotten fable, erased by the rise of modern browsers and ad blockers. Yet in a twist of irony, regulators have effectively mandated their return over the last twenty-five years. Today, through well-

1. Ethan Zuckerman, *The Internet's Original Sin*, THE ATLANTIC (Aug. 14, 2014), https://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/ [https://perma.cc/RP6W-NUB5].

intentioned privacy laws, users face cookie banners: legally required pop-ups that now punctuate nearly every online interaction. These banners are not the occasional annoyance of a disreputable site but a ubiquitous condition of using the internet itself, a ritualized, inescapable interruption.

The case against cookie banners is overwhelming. They have eroded the very concept of meaningful consent by reducing it to a hollow ritual. As scholarship on adhesion contracts, mandated disclosure, and notice in privacy law make clear, individuals do not and cannot read or understand the terms they are presented under mandatory notice regimes like perfunctory click-through banners.[2] Instead, they treat the act of clicking "accept" or "reject" as an automated necessity to getting where they want to go, not just ritualizing consent but making it entirely performative. Demoralized users are trapped in an empty Weberian ritual of administrative resignation rather than empowerment.[3]

Nor do banners prevent harm. Even if users understood them perfectly, cookies themselves are no longer the central engine of surveillance; advertising technology has moved on to device fingerprinting, cross-site profiling, and real-time bidding.[4] Banners thus regulate the wrong thing. More than ineffective, cookie banners' designs are often riddled with dark patterns — interfaces engineered to maximize acceptance and minimize resistance — ensuring that users "consent" in form while surrendering in substance.[5] The result is not protection from, but normalization of surveillance. We must account for the cumulative cost of these failures: banners slow browsing and access to information, corrode user trust, crowd out stronger reforms, and waste energy at global scale.[6] They are, in short, a useless and counterproductive solution to a problem they in no way meaningfully address.

---

2. This work is well-summarized in the Article to which this Article responds, *see* Robin Bradley Kar & Xiaowei Yu, *The Contractual Death and Rebirth of Privacy*, 38 HARV. J.L. & TECH. 1103, 1107–08 n.17–18 (2024); *see also* M. Ryan Calo, *Against Notice Skepticism in Privacy (And Everywhere)*, 87 NOTRE DAME L. REV. 1027, 1033 (2012) (summarizing much of the literature around notice skepticism in privacy and arguing that nevertheless it is premature to abandon notice as a mechanism of privacy regulation).

3. Examples of such notices and the burden they place on individuals abound. *See, e.g.*, RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE 188–93 (2008) (listing examples of mandatory notice); Paula J. Dalley, *The Use and Misuse of Disclosure as a Regulatory System*, 34 FLA. ST. U. L. REV. 1089, 1092 (2007) (discussing the "dozens, possibly hundreds" of disclosure notices in regulation); Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent* (Oct. 2009) (unpublished manuscript), http://www.nyu.edu/projects/nissenbaum/papers/EDSIIOnNotice.pdf [https://perma.cc/Q27Y-74HL] (concluding even an opt-in regime in online behavioral advertising lacks legitimacy or efficacy).

4. *See infra* Section III.A.2.

5. *See infra* Section III.A.1.

6. *See infra* Sections III.A.3, III.A.5.

In truth, this is an Article about much more than cookie banners. It is an Article about how we regulate technology, and the extent to which even the most well-meaning of regulatory solutions can ultimately work against the interests of the citizens and users they are meant to protect. In this sense, the twenty-five-year history of cookies and their regulation is a perfect case study. It speaks to governments' agility, or lack thereof, in identifying problems and drafting solutions to fast-moving technology. It showcases the role of industry in normalizing and ossifying compliance regimes and their incentives for keeping these outdated regulations in place.[7] It demonstrates the ways in which those compliance mechanisms do little or nothing to prevent the harms they were meant to address, most of which are now technologically irrelevant.[8] But most of all, it showcases that even when regulatory solutions are unmitigated failures, they can persist for a quarter of a century, blocking public conversation about new solutions.[9]

To this last point, at least, there is good news: in September 2025, the European Commission announced a "simplification" initiative to review measures looking at "outdated rules on the use of cookies and other tracking technologies."[10] The initiative aims to require "pragmatic and immediate clarifications to limit consent fatigue, provide legal clarity on rightful access and processing, and enhanced data availability to businesses."[11] This opportunity changes the tenor of this Article from an academic illustration to a policy-reform *cri de coeur*. It is incumbent upon Europe to eliminate the law that gives rise to cookie banner compliance, and in doing so, begin a much-needed conversation about what the regulatory future might look like where people are *actually* empowered to protect their data and privacy.

This Article proceeds in three Parts. Part II reconstructs the legal history that produced cookie banners, tracing their origins in the European Union's ePrivacy Directive, their reinforcement under the General Data Protection Regulation ("GDPR"), their global spread through the Brussels Effect, and their eventual echo in U.S. regimes like the California Consumer Privacy Act ("CCPA"). Part III offers a critique some fifteen years after the concept of the modern cookie banner finally emerged, cataloguing the many ways cookie banners have failed: eroding meaningful consent, failing to prevent harm, introducing friction and fatigue, functioning as performative regulation, blocking more meaningful reforms, and even contributing to

7. *See infra* Section III.A.2 and 6.

8. *See infra* Section III.A.2.

9. *See infra* Section III.A.6.

10. European Commission, Simplification — Digital Package and Omnibus Call for Evidence (Sep. 16, 2025), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus_en [https://perma.cc/SYP7-UTJS].

11. *Id.*

environmental waste. Part IV is the simplest prescriptive directive, aimed with new hope at the European Commission: cookie banners should be abolished rather than rehabilitated, and a conversation about regulatory options to protect individual data and privacy reopened.

II. A BRIEF HISTORY OF COOKIE BANNERS

Cookies are not the same as cookie banners. This distinction is perhaps obvious to readers who have gotten to this point in this Article, but to consumers who do not know how the web works, the ubiquity of fifteen years of pop-ups to "Accept or Decline Cookies" has perhaps served to confuse these concepts.

So let us unpack these two ideas in the briefest of terms: *Cookies* are small text files that are stored by a user's web browser at the request of a website.[12] The architecture of the internet, built primarily on Hypertext Transfer Protocol ("HTTP"), means that each click of your mouse and each movement to a new page is an identity-less novel interaction. This is a problem if you're trying to string together any kind of long-term interaction with a website for a user, like allowing them to put things in a shopping cart or explore subpages of an encyclopedia. Cookies were developed as a solution to that problem, allowing users to build cookies up like bread crumbs in their interactions with certain sites so they could have coherent interactions and trace their online browsing paths backwards and forwards.[13] Of course, companies also quickly realized that the same mechanism could also be used for more expansive forms of data collection — by placing third-party cookies across websites, advertising networks and analytics firms could track user behavior, build profiles on those users, and then deliver highly-targeted advertising.[14] Thus, while cookies were (and are) essential to a functional internet, they also became a fundamental component of the digital advertising technology industry.[15]

Shoshana Zuboff describes the relationship between consumer online data tracking and targeted advertising through mechanisms like cookies as "surveillance capitalism."[16] Surveillance capitalism is a particularly powerful framing as it captures two major fears consumers have in an age of sudden online-everything: one, that they are being

12. MEG LETA JONES, THE CHARACTER OF CONSENT: THE HISTORY OF COOKIES AND THE FUTURE OF TECHNOLOGY POLICY 1–5 (MIT Press, 2024). The following summary of the history of cookie banners is entirely reliant on Jones' incredible work, which is a complete and comprehensive treatment of the technological, historical, and legal buildout of cookies alongside a brilliant theoretical critique.

13. JAMES GRIMMELMANN, INTERNET LAW: CASES AND PROBLEMS 377–79 (2025).

14. *Id.* at 378.

15. *Id.*

16. Shoshana Zuboff, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 8 (2019).

watched, and two, that they are being commoditized.[17] Underpinning both of those feelings is the practical disempowerment of the average user and consumer who is suddenly trapped in an inescapable and opaque world of technology.[18] While scholars continue to debate whether targeted advertising and data collection result in concrete, demonstrable harms,[19] that question is outside the scope of this Article — and, in many respects, irrelevant. Users find themselves increasingly dependent on technologies owned and operated by private companies, technologies they could neither fully understand nor meaningfully control. In that environment — even if only phenomenological — regulatory action gives a feeling of democratic agency, and the promise of choice through cookie banners offers a sense of individual autonomy.

The groundswell of feeling creating the push for consumer privacy reform consolidated in the early 2000s and helps explain why cookies became the focus of regulatory action. At that point, cookies were at the fore of online technology creating consumer privacy concerns over targeted advertising.[20] Far ahead of the United States in taking on internet regulation, European policymakers glommed on to cookies as a vehicle for mass, non-transparent data collection that undermined informational self-determination.[21] Regulators could not just ban cookies because they were an essential part of functional internet, but they could address consumers' *sense* of powerlessness and hidden surveillance by mandating disclosure that cookies were being used. Thus, the *cookie banner* was born: a mandatory pop-up that operators must display to users who visit their site to give them the optionality of accepting or declining the use of cookies.

The regulatory history of how this solution was generated and proliferated around the world is the focus of the remainder of this Part. First, cookies became a regulatory concern not because they were inherently harmful, but because their widespread repurposing for behavioral advertising turned them into a symbol of the broader struggle between user privacy and commercial surveillance.[22] Second, this myopic focus led to two and a half decades of well-intentioned but ultimately insidious, wasteful, and ineffective regulation. It provides a

17. *See* Yuxi Wu, Sydney Bice, W. Keith Edwards & Sauvik Das, *The Slow Violence of Surveillance Capitalism: How Online Behavioral Advertising Harms People*, in Proc. 2023 ACM Conf. on Fairness, Accountability, & Transparency (2023) (survey of 420 participants detailing the "slow violence" inflicted by online behavioral advertising); *see generally id.*

18. Zuboff, *supra* note 16, at 278.

19. *See, e.g.*, Derek E. Bambauer, *Target(ed) Advertising*, 58 U.C. DAVIS L. REV. 1429 (2025) (summarizing and analyzing the controversy around targeted advertising).

20. *See* JONES, *supra* note 12, at 134.

21. *See id.* at 148–50.

22. *See id.* at 141–42.

cautionary tale of how the cure can become much worse than the disease.

A. Origins: EU ePrivacy Directive

Cookies entered the public consciousness and became a source of public concern as possible privacy violations around 1996.[23] David Whalen, who ran one of the only early sources of technical information on cookies called "Cookie Central," characterized this period of media coverage as "when the world went nuts. It wasn't hard to find a story about how internet sites are 'violating' our privacy with these things called cookies. And, of course, the public didn't know much about it other than to be scared of them. . . . People just thought cookies were another attempt by nefarious developers to steal their information."[24] In the U.S., the efforts to address this popular fear took many forms at all levels of government — from technical standards groups to federal agency reports to Congressional hearings to State Attorneys General suits to private class action. But all ultimately failed.[25] As Meg Leta Jones, author of *The Character of Consent*, the authoritative history of cookies and their regulation, correctly identifies, U.S. regulatory failure over cookies was not only because the cookies issue itself was complex, but "because the ill-fitting laws presented the opportunity for convenient confusion and inconsistency among areas of law."[26]

The United States, however, was not the only major market and democracy where cookies were striking fear in internet users. Europe had all the same issues with cookies and privacy — but unlike the U.S., they had the regulatory advantage of two separate sets of already legally recognized privacy rights that could be brought to bear on the issue.[27] Following these broad protections for privacy and communications in Europe, individual nations' constitutional rights to privacy and data protections simultaneously evolved.[28]

This legal foundation made Europe's task of passing regulation around the cookie privacy fears immeasurably more straightforward than the United States' efforts. By 2002, the first decisive step toward the cookie banner regime was the EU's adoption of the ePrivacy

---

23. *Id.* at 134 (citing Tim Jackson, *This Bug in Your PC Is a Smart Cookie*, FIN. TIMES (Feb. 12, 1996)).

24. *Id.* at 134.

25. *See, e.g.*, *id.* at 142–48 (detailing these various efforts against DoubleClick).

26. *Id.* at 142.

27. *Id.* at 149 (noting that Article 8 of the 1950 European Convention on Human Rights provided a "right to respect for privacy and family life" and that Articles 7 and 8 of the 2000 Charter of Fundamental Rights protected the right to private and family life and personal data, respectively).

28. *Id.* (citing legal scholar David Erdos).

Directive in 2002, specifically Article 5(3).[29] Though initial drafts of the directive which began in the European Commission in 1997 contained no explicit mention of cookies, a Dutch Parliament member proposed a provision in 2000 to prohibit cookies "unless a prior explicit, well-informed and freely given consent of the users concerned has been obtained."[30] The advertising industry saw this amendment as an opt-*in* requirement that would effectively destroy the fundamental role cookies played in web infrastructure, and duly lobbied to "[s]ave the [c]ookies."[31] Part of that lobbying effort was pointing out how cookies were a vital part of e-commerce — something Europe was extremely eager to develop.[32] The result was an opt-*out* compromise in the final version of the directive in which cookies were

> . . . only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the *right to refuse* such processing by the data controller.[33]

Had this version marked the end of European intervention into regulating cookies, this Article might not have cause to exist, but of course, it did not.

A few things happened over the following years which gave the European Parliament reason to readdress the issue and change terms of the regulation around cookies to a consent based model. First, as previously discussed, U.S. efforts to further solve privacy concerns raised by cookies continued to fail, leaving Europe alone to regulate.[34] Second, in 2007 Google decided to enter the targeted advertising business and bought DoubleClick, the world's largest ad tracking network for $3.1 billion.[35] This decision set off a flurry of major platforms purchasing ad tech — AOL bought AdTech and Tacoda, Yahoo bought Right Media, British WPP bought 24/7 Real Media, and Microsoft bought aQuantive.[36] The mergers brought on increased

29. Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 [hereinafter Directive 2002/58/EC].

30. JONES, *supra* note 12, at 151 (citing Committee on Citizens' Freedoms and Rights, Justice and Home Affairs Proposal for a Directive of the European Parliament and Council Concerning the Processing of Personal Data and the Protection of Privacy in Electronic Communications Sector, COM (2000) 385 final (Oct. 24, 2001)).

31. *Id.*

32. *Id.*

33. *Id.* at 152 (citing Directive 2002/58/EC, *supra* note 29, at art. 5(3)).

34. *Cf.* JONES, *supra* note 12, at 145–46.

35. *Id.* at 146.

36. *Id.* at 152 n.52.

public scrutiny of the data practices underlying these massive ad networks and further pushed the EU Parliament to look again at the 2002 eDirective pertaining to cookies in 2007.[37]

It was during this period that the Commission introduced language in draft amendments that contained a provision requiring consent to store information.[38] Though the precise mechanism of the consent regime changed over the amendment process, the ultimate amendment of Article 5(3) that was passed in Directive 2009/136/EC stated that such storage of user information "is only allowed on condition that the subscriber or user concerned has given his or her consent."[39] Despite now being credited as the language that introduced the consent-based cookie banners regime, that did not seem to be the initial intent.[40] A 2009 Addendum to the directive specifically reassured that "amended Article 5(3) is not intended to alter the existing requirement that such consent be exercised as a right to refuse the use of cookies or similar technologies used for legitimate purposes."[41] Seemingly, this just maintained the "right to refuse cookies, which was no change at all."[42] But in 2010 the Article 29 Working Party — a group comprised of data protection regulators from EU nation-states[43] — unilaterally altered the

37. *Id.* at 152–53.

38. Jan Tomisek, *Cookies and EU Law: History, Future Regulation and Critique*, 35 TECH. AND REG. 38–39 (2023) https://doi.org/10.26116/techreg.2023.004 [https://perma.cc/5HS6-4V5J] ("The EU law on cookies was therefore first proposed in 2000 and adopted in 2002, but it is only since 2009 that the consent requirement has been included.").

39. *Id.* (quoting Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws).

40. *Id.* at 39.

41. JONES, *supra* note 12, at 153 (citing European Council, Addendum to "I/A" note of 18 November 2009: Adoption of the proposal for a Directive of the European Parliament and of the Council amending the Directives 2002/21//EC on a common regulatory framework for electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services (LA þ S) (third reading) — statements, 15864/09).

42. *Id.*

43. The Article 29 Working Party (often WP29) was not part of the European Parliament, but rather an independent advisory body on data protection and privacy created under Article 29 of Directive 95/46/EC (the 1995 EU Data Protection Directive). Its role was to advise the Commission on data protection matters, issue opinions and recommendations interpreting the Directive, promote uniform application of data-protection rules across the EU, and engage with non-EU authorities on data-transfer adequacy. *See* Directive 95/46/EC, of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 29, 1995 O.J. (L 281) 31, 50. It was dissolved in 2018 and replaced by European Data Protection Board ("EDPB") under Article 68 of the GDPR. *See* Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), art. 68, 2016 O.J. (L 119) 1, 56 [hereinafter GDPR].

interpretation of the directive. In an opinion on online behavioral advertising, the group clarified that the "consent" language in the 2007 directive was to be understood as a requirement to provide "clear notice and effective consent."[44] In 2011, it further clarified this meant "prior" consent.[45]

To understand the mess this new advisory opinion created, it is critical to understand that directives issued by the European Parliament only instruct individual European member states as to what outcome must be achieved. States then have flexibility and independence to create national regulation to achieve those outcomes, which creates significant variation.[46] Thus, in the nine years since the original eDirective was passed, the ever-changing view from Brussels meant that as national laws rolled out, the laws increasingly varied in what they required for compliance.[47] One of the great strengths of the European Union was not only a single market but also a relatively unbalkanized internet, where privacy requirements did not suddenly change depending on whether a user logged in from Paris or Amsterdam. The ad tech industry, left to determine a threshold for compliance that would best meet this wild variation in national laws, went with the broadest possible interpretation of the 2009 eDirective, deciding that: "1) cookie notices should be prominently displayed; 2) action, like remaining on a site, amounts to consent; 3) users must be given means for controlling cookies, except those designated necessary; and 4) clear and comprehensive information about cookies in a cookie policy must be available."[48] Hitting these marks meant cookie notifications suddenly turned into pop-ups and banners with linked privacy policies that we still recognize today.

B. Overlay and Amplification: General Data Protection Regulation

If the ePrivacy Directive created the legal space for (and the shape of) cookie banners, the GDPR amplified and systematized those

---

44. JONES, *supra* note 12, at 153–54.

45. *Id.* This 2011 clarification was made to bring the 2007 eDirective in line with the Data Protection Directive.

46. *See* Consolidated Version of the Treaty on the Functioning of the European Union art. 288, Oct. 26, 2012, 2012 O.J. (C 326) 47; *see also* PAUL CRAIG & GRÁINNE DE BÚRCA, EU LAW: TEXT, CASES, AND MATERIALS 144–45 (7th ed. 2020) (explaining that regulations are directly applicable and uniform, while directives require national implementation); DAMIAN CHALMERS, GARETH DAVIES, GIORGIO MONTI & VEERLE HEYVAERT, EUROPEAN UNION LAW: CASES AND MATERIALS 106–16 (3d ed. 2014).

47. JONES, *supra* note 12, at 154 (citing Interactive Advertising Bureau, *Europe's Cookie Laws: E- Privacy Implementation Center* (2016)). Some states, such as the United Kingdom, interpreted the consent obligation more permissively, initially allowing implied consent banners. Others, such as the Netherlands, pressed for stricter opt-in consent. This divergence foreshadowed the debates that would intensify under the GDPR. *Id.* at 154 n.60.

48. *Id.* at 154 (citing Eduardo Ustaran, *Cookie Consent — What's Changed?*, INT'L ASS'N PRIVACY PROF'LS (July 22, 2014)).

obligations in ways that entrenched banners as a global phenomenon. The EU adopted the GDPR in 2016, and it took effect May 25, 2018, as a comprehensive overhaul of EU data protection law.[49] Unlike directives, the GDPR was a regulation, directly applicable in all member states without the need for national transposition.

A common misunderstanding is that the GDPR is the reason we have cookie banners today. This notion is only true in part. As discussed, the eDirective took on the subject matter of cookies long before the GDPR. However, while the GDPR does not specifically regulate cookies, its language further alters the meaning of "consent" — a term introduced benignly in the 2009 eDirective Amendment.[50] Article 6 of the GDPR sets out lawful bases for processing personal data, with consent as one of the most important.[51] Article 7 specifies the conditions for consent: it must be freely given, specific, informed, and unambiguous, demonstrated by a clear affirmative act.[52] Article 13 requires disclosure of the purposes of processing and categories of data recipients.[53] As industry has interpreted it, these clarifications imply that banners cannot simply request consent in the abstract; they have to inform users about the types of cookies (e.g., necessary, functional, advertising) and their purposes.[54] Recital 32 of the GDPR clarifies that silence, pre-ticked boxes, or inactivity do not constitute consent.[55]

In practice, the result was that cookie disclosure compliance tolerated under the 2002 Directive — such as banners stating "by continuing to browse you consent to cookies" — was no longer defensible. Opt-out was out. Under the GDPR, valid consent required a positive opt-in, such as clicking "Accept" on a banner or a pop-up, and an explanation to users of the types of cookies that were being deployed on the site. The GDPR thus hardened the legal baseline established by the ePrivacy Directive, effectively forcing websites to deploy banners with active choice mechanisms.[56]

---

49. For a comprehensive understanding of the duality of online governance at play in the GDPR, see Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529 (2019).

50. *See supra* note 30 and accompanying text.

51. GDPR, *supra* note 43, at art. 6.

52. *Id.* at art. 7.

53. *Id.* at art. 13.

54. OneTrust LLC, The Ultimate Cookie Handbook for Privacy Professionals 7 (Nov. 2020), https://www.dataguidance.com/sites/default/files/20201228-onetrust-cookieconsent-handbook-digital.pdf (describing a "commonly accepted classification" of cookies by purpose, including "strictly necessary," "functional," and "targeting (advertising)" cookies).

55. GDPR, *supra* note 43, at recital 32.

56. JONES, *supra* note 12, at 167 (explaining that the "GDPR's shift to explicit, prior consent unequivocally changed the default to cookies to opt-in and requires specific consent" such as cookies banners).

Perhaps most importantly, the GDPR's direct regulatory impact was to suddenly increase the cost of non-compliance. The GDPR empowered national data protection authorities to impose fines of up to four percent of global annual revenue for violations.[57] EU nations updated guidelines accordingly. For example, the French Data Protection Authority ("CNIL") updated its national cookie guidelines in 2020 stating consent must be "unambiguous" and the absence of "active and specific consent must be interpreted as refusal."[58] These were not empty threats, instead resulting in high-profile enforcement actions. In January 2021, CNIL fined Google €150 million and Facebook €60 million for failing to provide "equivalent" solutions to allow users to refuse cookies as easily as they can accept them.[59]

The combined effect of these provisions was to standardize opt-in cookie banners across Europe and beyond. Whereas the 2002 eDirective and the nine years of dithering thereafter had allowed for significant national divergence, the GDPR's directly applicable rules created uniform standards: banners had to request affirmative opt-in consent and provide granular information.[60] By 2018, interacting with cookie banners had become unavoidable on virtually every major website serving EU users.

But the GDPR also had broader symbolic importance. It signaled that the EU was committed to a rights-based approach to data protection, framing privacy as a fundamental right under Article 8 of the EU Charter of Fundamental Rights. By contrast, U.S. privacy law remained sectoral and market-driven. This divergence magnified the GDPR's extraterritorial influence, setting the stage for the "Brussels Effect."

C. Global Implementation via Brussels Effect

The consolidation of cookie consent requirements under the GDPR did not remain confined to Europe. Instead, the GDPR's rules reverberated across the global internet economy, exemplifying the

57. *Id.*

58. *Id.* at 171.

59. Mathieu Rosemain, *Google hit with 150 mln euro French fine for cookie breaches*, REUTERS (Jan. 6, 2022), https://www.reuters.com/world/europe/france-imposes-fines-facebook-ireland-google-2022-01-06/ [https://perma.cc/X4RP-SS68].

60. The GDPR thickens the idea of "consent" to require "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." GDPR, *supra* note 43, at art. 4(11). Recital 32 of the GDPR explains further that "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement." *Id.* at pmbl. ¶ 32.

"Brussels Effect."[61] This phrase coined by legal scholar Anu Bradford in her foundational book describes the EU's ability to export its regulatory standards beyond its borders through the power of its single market.[62] Because access to EU consumers is economically indispensable, multinational firms often adopt EU standards globally, rather than taking on the cost and logistical difficulty of maintaining separate compliance regimes for different jurisdictions.[63]

Cookie banners are perhaps the best and most recent illustration of the Brussels Effect in action. For a company like Google, Facebook, or Amazon, building and maintaining separate consent interfaces for EU and non-EU users would be technologically burdensome and reputationally risky. Instead, it was cheaper, faster, and easier for firms to simply adopt opt-in cookie banners worldwide, even where local law did not demand them. This created a situation where users in the United States, Asia, and Latin America encountered cookie banners not because of local legal mandates, but because EU law effectively set the global baseline for market compliance.

The Brussels Effect also operated indirectly through regulatory emulation. As of 2021, 142 countries had passed data privacy laws often modeled on the GDPR.[64] Policymakers outside Europe observed the GDPR's prominence and sought to align their own privacy frameworks with EU standards. This was particularly true in countries with close trading relationships with the EU, which faced practical pressure to ensure "adequacy" determinations for cross-border data flows under Article 45 GDPR.[65] The EU's adequacy mechanism under GDPR Article 45 functioned as a lever: because the absence of adequacy can make EU-third-country transfers legally and operationally costly, third countries faced pressure to approximate EU-style data protection rules.[66] In practice, this alignment often extended

61. *See generally* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012) (describing the Brussels Effect as the phenomenon where the European Union unilaterally sets global standards because of the size and wealth of its market, which forces multinational corporations to adopt its regulations worldwide).

62. Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1744–45 (2021).

63. *Id.* at 1745.

64. Graham Greenleaf, *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance*, 169 PRIV. L. & BUS. INT'L REP. 25, 26 (2021) (noting the GDPR's influence on global legislative emulation).

65. Anupam Chander & Paul Schwartz, *Privacy and/or Trade*, 90 U. CHI. L. REV. 49, 54 (2023) (stating that while "[a]lmost all of the discussions of 'adequacy,' a core feature of global data privacy, focus on how the European Union determines whether a foreign jurisdiction's data protection law meets" a GDPR standard, that there are now "adequacy standards in sixty-one countries outside the European Union").

66. Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 786–89 (2019) (explaining that because the EU can prohibit data flows absent adequacy, the GDPR adequacy mechanism gives the EU "leverage regarding the terms for data processing in non-EU nations," and describing how Japan amended its privacy law in ways that "moved it significantly closer to the EU system" in the course of adequacy negotiations).

beyond the GDPR's transfer provisions to the broader EU privacy compliance environment that governs data-driven commerce — including the EU's ePrivacy "cookie" rules that structure notice and consent for tracking technologies.[67]

The result was a form of de facto globalization of cookie banners. By 2019, internet users around the world encountered banners, regardless of whether their own jurisdictions had enacted equivalent statutes.[68] This global spread was not driven by a coherent transnational legislative process, but by the extraterritorial effect and gravitational pull of EU law. This phenomenon underscores an irony: although the EU intended to protect European citizens, its rules reshaped the user experience of billions worldwide. The Brussels Effect thus magnified both the reach and the frustrations of cookie banners. While banners were designed to enhance autonomy, their global proliferation often produced banner fatigue and mechanical clicking, problems examined further in Part III of this Article.

D. U.S. Regulatory Echo: California Consumer Privacy Act

In contrast to the EU, the United States' privacy law is sector-specific, focusing on domains such as health (HIPAA), finance (GLBA), or children (COPPA).[69] This fragmented approach created a striking transatlantic divergence. While EU law mandated explicit consent for cookies, the sectoral nature of the United States privacy laws and haphazard attempts to go after cookies specifically resulted in little or no comprehensive regulation governing cookies. The situation shifted with California's passage of the CCPA on June 28, 2018, which took effect on January 1, 2020.[70] Though not cookie-specific, the CCPA introduced broad rights of access, deletion, and opt-out of the "sale" of personal information.[71] For online advertising ecosystems dependent on cookies, the CCPA created significant compliance obligations. Firms were required to disclose categories of personal

67. Meg Leta Jones & Jenny Lee, *Comparing Consent to Cookies: A Case for Protecting Non-Use*, 53 CORNELL INT'L L.J. 97, 118–23 (2020) (describing ePrivacy Directive art. 5(3)'s requirement of clear information about cookie purposes and a right to refuse, and the later "EU Cookie Directive" amendments moving toward prior consent for tracking cookies).

68. *See, e.g.*, Anas Baig & Maria Khan, *Cookie Laws & Regulations: Explained*, SECURITI (July 12, 2021), https://securiti.ai/blog/cookie-laws/ [https://perma.cc/QZA6-49R2].

69. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104–191, 110 Stat. 1936 (1996) (codified at 42 U.S.C. § 1320d); Gramm-Leach-Bliley Act (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801–6809); Children's Online Privacy Protection Act of 1998 (COPPA), Pub. L. No. 105–277, 112 Stat. 2681–728 (1998) (codified at 15 U.S.C. §§ 6501–506).

70. California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–199.100 (West 2023).

71. *Id.*

information they collected, the purposes of use, and whether such data was sold to third parties.[72]

The CCPA also mandated a "clear and conspicuous" link on websites labeled "Do Not Sell My Personal Information," enabling consumers to opt-out of data sharing.[73] While distinct from GDPR's affirmative opt-in model, this requirement pressured companies to reconfigure cookie consent mechanisms for California residents. Just as Europe's policies affect the world via the Brussels Effect, so too does California have such an effect on the rest of the United States, making the CCPA the default in the U.S. generally. In practice, many companies ultimately adapted their existing GDPR banners to serve dual purposes: informing EU users about opt-in consent and informing Californians about opt-out rights.[74]

Though markedly distinct in its requirements, the CCPA is nonetheless a regulatory echo of the EU framework in the United States. It did not replicate the GDPR's structure, but it created parallel disclosure and control expectations that reinforced the banner regime. Furthermore, the CCPA's prominence spurred other states to consider similar laws, creating the potential for a patchwork of U.S. state-level regulations.[75] Importantly, the CCPA illustrated the limits of federal inaction. In the absence of Congressional or agency action, California emerged as the de facto regulator of U.S. privacy. Just as the EU leveraged market size to export its standards globally, California leveraged its economic weight to influence national practice.[76] Many companies extended CCPA rights to all U.S. users, rather than building state-specific systems, replicating the Brussels Effect in domestic miniature.[77]

The CCPA's impact on cookie banners was thus both direct and indirect. Directly, it required disclosures and opt-out mechanisms that companies often integrated into banners or preference centers.[78] Indirectly, it normalized the expectation that U.S. users, like their European counterparts, should confront consent interfaces when browsing the web. By 2020, cookie banners were no longer a uniquely

---

72. *Id.*

73. *See* Cal. Civ. Code § 1798.135(a)(1) (West 2023).

74. *Cf.* JONES, *supra* note 12, at 175.

75. *See, e.g.*, Int'l Ass'n of Privacy Pros. [IAPP], US State Comprehensive Privacy Laws Report 2025 (2025), https://iapp.org/resources/article/us-state-privacy-laws-overview [https://perma.cc/KW55-4F6H] (giving summary and overview of the different types of privacy laws underway in other U.S. states).

76. *See* Chander et al., *supra* note 62, at 1737 (arguing that California has "emerged as a kind of privacy superregulator, catalyzing privacy law in the United States").

77. *Id.* at 1737 (stating "we are witnessing what might be characterized as a regulatory race on both sides of the ocean"). *But see generally* Jens Frankenreiter, *The Missing "California Effect" in Data Privacy Law*, 39 YALE J. ON REG. 1068 (2022) (discussing the effects of the CCPA on U.S. law and its limited comparability to the extraterritorial effect of the GDPR).

78. JONES, *supra* note 12, at 175–76.

European phenomenon; through the GDPR, Brussels Effect, and California Code, they had become entrenched in the U.S. internet landscape as well, thanks in large part to compliance decisions from some of the world's largest transnational technology companies.[79]

* * * * *

The trajectory traced here shows how cookie banners emerged from the interaction of law, technology, and market power. Beginning with the EU's ePrivacy Directive in 2002 and its 2009 amendment, lawmakers sought to ensure user consent for cookies. Vagueness, national variation, and industry fear of non-compliance led to banners and pop-ups as the default mode of compliance to notify users of cookies.[80] The GDPR then amplified these requirements by switching consent from opt-out to opt-in and granting Europe's national data protection authorities the power to enforce them with unprecedented severity.[81] The Brussels Effect carried these rules beyond Europe, pressuring global companies to adopt opt-in banners near universally.[82] In the United States, the CCPA created a regulatory echo, embedding banner logic into the American internet.[83]

The result is the world we now inhabit: an online environment in which cookie banners are nearly inescapable. Yet as Part III of this Article will argue, this banner-based regime has produced serious problems — problems far worse than whatever privacy risks were created by cookies. Rather than enhancing autonomy, banners often overwhelm users, trivialize consent, and distort the experience of the web. They illustrate how regulatory good intentions can ossify into poor design, with consequences for not just digital privacy and usability, but for broader social concepts of consent and contract.

Understanding how we arrived here — through EU directives, GDPR amplification, global diffusion, and U.S. echoes — provides the necessary foundation for critique. The next Part will therefore turn to that critique, showing why the laws that produced cookie banners have ultimately failed to deliver on their promise of meaningful privacy protection.

---

79. *See id.* at 177–81 (discussing Apple's role in "breath[ing] back life into digital consent").

80. *See supra* Section II.A.

81. *See supra* Section II.B.

82. *See supra* Section II.C.

83. *See supra* Section II.D.

III. TWENTY-FIVE YEARS LATER: A CRITIQUE OF COOKIE BANNERS

Cookies are, at bottom, technical artifacts: small text files used to maintain state across otherwise stateless browsing requests.[84] As such, they are best understood as neutral elements of the web's architecture, equally capable of supporting user-friendly functions like shopping carts or enabling invasive cross-site tracking.[85] Far less neutral is the legal and cultural story of cookie *banners* and their effect on the world. Unlike cookies, which are embedded into the technical substrate of the internet, banners exist only because legislatures and regulators chose to mandate their use. They are a product of political decision-making, not technical necessity, and their continued ubiquity is thus subject to change through law and policy rather than engineering constraint.

In the wake of the GDPR and heightened enforcement by European data protection authorities, Google announced in 2020 that it would retire third-party cookies from its Chrome browser, setting a deadline that was eventually extended to mid-2024.[86] But as of today, that prediction has not materialized. Google's retirement of cookies was delayed yet again, and it is now unlikely that cookies will disappear entirely from the online ecosystem.[87] Moreover, as this Part will show, even if cookies did fade, they are no longer the central villain in the economy of digital surveillance. Newer technologies — such as device fingerprinting, probabilistic identity graphs, and behavioral inference through machine learning — pose privacy risks as significant as, or greater than, those associated with cookies.[88]

This Part proceeds in two stages. Section A explores the negative consequences of the cookie banner regime, including its erosion of meaningful consent, its ineffectiveness at preventing harm, its creation of friction for information access, its function as performative regulation, its role in foreclosing more meaningful reforms, and its

---

84. *Id.* at 1–5.

85. GRIMMELMANN, *supra* note 13.

86. *Compare* Sara Fischer, *Google to Phase Out Third-Party Cookies,* AXIOS (Jan. 14, 2020), https://www.axios.com/2020/01/14/google-cookies-phase-out-third-party [https://perma.cc/YT46-WHMC], *with* Lena Cohen, *Google Breaks Promise to Block Third-Party Cookies*, EFF (Aug. 2, 2024), https://www.eff.org/deeplinks/2024/08/google-breaks-promise-block-third-party-cookies [https://perma.cc/J67C-QGTL].

87. Emma Roth, *Google is Scrapping Its Planned Changes for Third-Party Cookies in Chrome*, THE VERGE (Apr. 22, 2025), https://www.theverge.com/news/653964/google-privacy-sandbox-plans-scrapped-third-party-cookies [https://perma.cc/9SMP-PLVT].

88. *See generally* Kyle Crichton, Lorrie Faith Cranor & Nicolas Christin, *Rethinking Fingerprinting: An Assessment of Behavior-based Methods at Scale and Implications for Web Tracking*, 2025 PROC. ON PRIVACY ENHANCING TECHS. 7944, https://petsymposium.org/popets/2025/popets-2025-0158.pdf [https://perma.cc/7ZZQ-AT87] (analyzing how behavioral fingerprinting can be more privacy invasive than discontinuous tracking technologies like cookies).

environmental costs. Section B then considers the positives that can fairly be attributed to the banner regime, including increased visibility of data practices and heightened privacy awareness. Together, these critiques and acknowledgments provide the foundation for Part IV's prescriptive analysis, which asks how law might move beyond banners toward more effective and sustainable privacy protections.

A. The Negative

1. Erosion of Meaningful Consent

Notice and consent is both a common method of regulation and a foundational mechanism through which law secures its legitimacy.[89] It is a particularly frequent tool in privacy law, because it seemingly allows "people to determine for themselves when, how, and to what extent information about them is communicated to others."[90] Cookie banners are paradigmatic of this and rest on the premise that individual consent can thus legitimate extensive data collection. But as countless privacy scholars have pointed out, in practicality these "consent" banners are routinely neither free nor informed.[91] Interface owners script the timing, framing, and friction of the choice; users face asymmetric information and time pressure; a single click is treated as authorization for complex, downstream data uses.[92] Critically, even apparent assent can be hasty, confused, or structurally coerced.[93] Thus, self-reliant consent collapses under information asymmetries and

89. Calo, *supra* note 2, at 1027–28 (referring to "Lon Fuller's inclusion of notice in law's 'internal mortality' or Friederic von Hayek's distinction between 'arbitrariness and the rule of law'"); *see generally* Elizabeth Edenberg & Meg Leta Jones, *Analyzing the Legal Roots and Moral Core of Digital Consent*, 21 NEW MEDIA & SOC'Y 1804 (2019) (analyzing how legal frameworks for digital consent developed in order to see where there may be common international moral ground); MARGARET RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2012) (arguing that non-negotiable standard form contracts, or "boilerplate," undermine the rule of law by eroding consent and individual rights).

90. Kar & Yu, *supra* note 2, at 1104 (quoting ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967)).

91. Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1476–91 (2019) (cataloging unwitting, coerced, and incapacitated "consent"); *see also* NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS (2019) (arguing validity of consent depends on a meaningful ability to refuse and on adequate knowledge, conditions that are not present with click-through or banner-style assent); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–81 (2013); Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 343, 343 (Jane K. Winn ed., 2006); Barocas & Nissenbaum, *supra* note 3, at 1.

92. *See* Richards & Hartzog, *supra* note 91, at 1488–90.

93. *See id.*

market power, delivering the appearance (not the reality) of autonomy.[94]

Of course, notice and consent are not unique regulatory solutions to privacy problems — they are also fundamental to contract law, which, like privacy, is concerned with individual "freedom to give something away as well as the freedom not to."[95] In *The Contractual Death and Rebirth of Privacy*, Robin Bradley Kar and Xiaowei Yu explain how this common solution set of notice and consent in the digital context has melded contract doctrine with privacy law and led to "one of the most significant challenges to privacy and freedom of the modern era."[96] Kar and Yu contend that the larger problem of contemporary privacy "consent" is due to the hollowing out of the concept through a contract-law doctrinal drift: courts increasingly treating boilerplate privacy policies as enforceable agreements even when users lack any shared understanding of what they are said to accept.[97] This creates a "paradigm slip" from traditional contract — a moral right centered on jointly communicated meaning — to "pseudo-contract," in which unilateral, unread text acquires legal force.[98] It is this court-fueled interpretation of privacy policies and cookies banners as legal contract that they describe as the "contractual death of privacy."[99]

But regardless of where one roots the problem — in the doctrinal turn of contract, or in a myriad of other design, system, and human inadequacies — the effect on users is the same: they are asked to perform impossible acts of reading and comprehension, and their single click is then leveraged to justify surveillance practices they cannot understand or meaningfully evaluate.[100] Kar and Yu helpfully split these objections, which cut across both privacy and contract, into two categories: practical obstacles to adequate notice and authentic consent and justificatory objections to the poor quality of that consent.[101]

The practical obstacles to meaningful consent are well documented. Aleecia McDonald and Lorrie Faith Cranor famously

---

94. *Id.* at 1492, 1496; *see also* ANITA ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2011) (arguing for mandating some privacy protections notwithstanding immediate user preferences).

95. Kar & Yu, *supra* note 2, at 1104.

96. *Id.* at 1108.

97. *Id.* at 1106.

98. Robin Bradley Kar & Margaret Jane Radin, *Pseudo-Contract and Shared Meaning Analysis*, 132 HARV. L. REV. 1135, 1137, 1140 (2019) (describing and naming the idea of "paradigm slip" from traditional contract — a moral right centered on jointly communicated meaning — to "pseudo-contract," in which unilateral, unread text acquires legal force).

99. Kar & Yu, *supra* note 2, at 1119–20.

100. *Id.* at 1103; *see also* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 821–22 (2000) (critiquing self-reliant consent under conditions of information asymmetry).

101. Kar & Yu, *supra* note 2, at 1126.

calculated that reading all privacy policies encountered in a year would take 244 hours — nearly forty minutes each day.[102] Jonathan Obar and Anne Oeldorf-Hirsch demonstrated experimentally that ninety-eight percent of participants agreed to fictitious policies that required surrendering their firstborn child, proving that users routinely click "I agree" without reading.[103] Pew surveys confirm that large majorities misunderstand what privacy policies do, with fifty-two percent of Americans believing incorrectly that the mere existence of a policy means their data will not be shared.[104] These findings illustrate what Kar and Yu stress: the obstacles of time, information, and intelligibility doom the project of individual privacy self-management. Importantly, however, contractualization did not create these problems, though it certainly further entrenched them by wrapping them in the legitimating form of contract law.

The obstacles to meaningful consent are equally profound. Anita Allen has long argued that privacy cannot be left entirely to individual consent because people will often bargain it away under pressure, ignorance, or shortsightedness; governments sometimes must protect "unpopular" privacy interests even against individuals' immediate choices.[105] Paul Schwartz likewise critiqued the U.S. model of "self-reliant" privacy as illusory, because information asymmetries and market power mean that "consent" cannot provide a genuine foundation for autonomy.[106] Neil Richards and Woodrow Hartzog catalog the "pathologies of digital consent" — unwitting, coerced, incapacitated — that arise when firms design consent rituals to secure acquiescence rather than deliberation.[107] Margaret Jane Radin shows how boilerplate contracts erode substantive rights while maintaining a façade of voluntariness: the law treats alienation of rights as legitimate even when no one has read or understood the terms.[108] Daniel Solove's critique of "privacy self-management" reaches the same conclusion: individuals lack the time, information, and cognitive resources to meaningfully manage the data flows surrounding them.[109] And Omri Ben-Shahar and Carl Schneider's work on mandated disclosure generalizes the lesson: disclosure-based regimes fail systematically

---

102. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 563 (2008).

103. Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO. COMMC'N & SOC'Y 128, 143 (2020).

104. Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RSCH. CTR. (Dec. 4, 2014), https://www.pewresearch.org/short-reads/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/ [https://perma.cc/V59A-JLCP].

105. ALLEN, *supra* note 94.

106. Schwartz, *supra* note 100, at 821–23.

107. Richards & Hartzog, *supra* note 91, at 1461.

108. RADIN, *supra* note 89.

109. Solove, *supra* note 91, at 1880–81, 1889.

across contexts because individuals cannot absorb or act on the information disclosed.[110]

Behavioral economics deepens the indictment. Daniel Kahneman and Amos Tversky's research on heuristics and biases demonstrates that individuals facing complexity and uncertainty rely on mental shortcuts, overweight salient features, and systematically undervalue long-term risks.[111] Online consent interfaces exploit these cognitive patterns through "dark patterns" — manipulative design choices that nudge users toward accepting all cookies and bury or obscure options to reject them all.[112] The problem is not only that policies are unreadable; it is that even if they were read, human cognitive limitations make it impossible to process and rationally act on them in the aggregate. Nevertheless, the European approach has been to address these issues by simply increasing the standard of what counts as "consent" in compliance with cookie banners. In *Bundesverband der Verbraucherzentralen v. Planet49 GmbH*, the Court of Justice of the European Union held that pre-ticked boxes cannot constitute valid consent for cookies, and that GDPR's standards apply regardless of whether cookies store "personal data."[113] The European Data Protection Board's 2020 Consent Guidelines reject "cookie walls" and clarify that scrolling or swiping do not constitute consent.[114] This has not solved the problem. Multiple empirical studies of cookie banners in the wild[115] show that even formally compliant banners are optimized to maximize acceptance, reproducing the very same defects identified in

---

110. OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE (2014).

111. *See generally* DANIEL KAHNEMAN, THINKING, FAST AND SLOW (2011); Amos Tversky & Daniel Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, 185 SCI. 1124 (1974).

112. Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger & Lalana Kagal, *Dark Patterns After the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence*, 2020 PROC. CHI CONF. ON HUM. FACTORS COMPUTING SYS. (scraping thousands of consent pop-ups to run field experiments, finding that removing the opt-out option increased acceptance rates by twenty-three percentage points, while offering granular controls on the first layer decreased acceptance by eight to twenty percentage points); Nataliia Bielova, Laura Litvine, Anysia Nguyen, Mariam Chammat, Vincent Toubiana & Estelle Hary, *The Effect of Design Patterns on (Present and Future) Consent Choices*, 2024 PROC. USENIX SEC. SYMP. (showing dark-pattern design in consent banners nudges users toward accepting cookies, reducing likelihood of exploring alternative choices or information); Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub & Thorsten Holz, *(Un)informed Consent: Studying GDPR Consent Notices in the Field*, 2019 PROC. ACM SIGSAC CONF. ON COMPUT. & COMMC'N SEC. (finding in an in-the-wild study that sixty-two percent of popular EU sites displayed notices within months of the GDPR, but that design choices systematically nudged toward acceptance, with missing or hidden rejection options especially common).

113. Case C-673/17, Bundesverband der Verbraucherzentralen v. Planet49 GmbH, ECLI:EU:C:2019:801 (Oct. 1, 2019).

114. *Guidelines 05/2020 on Consent under Regulation 2016/679*, at 12, 19 (May 4, 2020) https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf [https://perma.cc/4BH6-V4WA].

115. *See supra* note 112.

the U.S. literature. Regulation may raise the floor, but the ceiling remains bounded by human cognition and structural design asymmetry.

Seen in this light, Kar and Yu are right to identify the legitimizing power of contract in online notice of consent as troubling, but wrong to treat it as the decisive inflection point.[116] The erosion of meaningful consent is deeper and more structural and its effects on society more profoundly entrenched in our societal fabric through the acts of billions of humans around the world clicking mindlessly through hundreds of banners a day, than they are by doctrinal contract opinions meted out by thousands of judges across United States jurisdictions. Contractualization no doubt adds another layer of formalism, but the underlying defects — practical impossibility and justificatory illegitimacy — predated it and persist regardless. But their proposed solution to the "death of privacy" via doctrinal contract reform mistakes the regulatory history of cookie banners as of a piece with the broader trajectory of adhesion contracts in online privacy law and common-law drift in doctrines of assent.[117] This conflation obscures a critical distinction. Unlike traditional boilerplate agreements, cookie banners are not the byproduct of judicial interpretation or incremental doctrinal erosion. They are regulatory artifacts, mandated by the ePrivacy Directive and the GDPR.[118] Their existence does not rest on courts enforcing exploitative terms but on legislatures requiring a ritual of "consent" that cannot meaningfully be given.

Cookie banners thus distill into one ritualized interface the failure of notice and consent in technology regulation. They are impractical in their means as documented by McDonald, Cranor, Obar, Kahneman, and Tversky; illegitimate in their ends as diagnosed by Allen, Schwartz, Richards and Hartzog, Radin, Solove, and Ben-Shahar and Schneider[119]; and thus empty doctrinal fictions entrenched by courts and regulators in both the U.S. and Europe. They are the most visible expression of a model that outsources privacy protection to individuals while denying them any meaningful capacity to exercise it. Far from empowering users, cookie banners exemplify and amplify the erosion of meaningful consent.

2. Outdated and Ineffective at Preventing Harm

Any evaluation of cookie banners must eventually address the threshold question of harm. The nature of "privacy harms" has long been contested, with scholars noting the difficulty of categorization and

116. *See generally* Kar & Yu, *supra* note 2.
117. *Id.*
118. *See* discussion *supra* Sections II.A–B.
119. *See supra* notes 105–10 and accompanying text.

measurement.[120] Samuel Warren and Louis Brandeis famously framed the "right to privacy" as a dignitary harm — "the right to be let alone."[121] Danielle Citron and Daniel Solove have provided more granular taxonomies, distinguishing physical, economic, reputational, psychological, and autonomy harms, and arguing that privacy violations are often socially distributed rather than individually atomized.[122] Ryan Calo has distinguished subjective harms (feelings of exposure or loss of control) from objective ones (data misuse, discrimination, or manipulation).[123] The result is a vast literature documenting that privacy harms are multiple, diffuse, and often amorphous. This Section does not attempt to resolve that debate. For present purposes, it assumes that surveillance-based digital advertising constitutes a cognizable privacy harm — subjective or objective, dignitary or taxonomic. The question then is whether cookie banners effectively prevent or mitigate that harm.

On this score, banners fare poorly. As a foundational matter, cookies themselves are no longer the central source of advertising surveillance, and thus no longer the root cause of the privacy concerns brought on by surveillance capitalism. Third-party cookies historically facilitated cross-site tracking by storing persistent identifiers, but the online advertising industry has steadily migrated toward more sophisticated techniques: device and browser fingerprinting, probabilistic identity graphs, cohort analysis, and server-side tracking infrastructures.[124] Though Google's delays at ending its use of cookies underscore how entrenched they remain, the strategic shift to alternatives like Google's "Privacy Sandbox" shows that industry actors no longer treat cookies as the linchpin of targeted advertising.[125] From a harm-prevention perspective, then, banners are increasingly regulating the *wrong* thing. They present users with meaningless rituals of consent[126] over cookies while the advertising ecosystem has already diversified into non-cookie techniques largely outside the scope of banner governance.

The result is that cookies banners, even where users decline to accept cookies, rarely prevent harm, because they do not regulate the dominant tracking technologies; they do not secure meaningful user

120. *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 830 (2022); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1142 (2011).

121. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

122. Citron & Solove, *supra* note 120, at 818–19.

123. Calo, *supra* note 120, at 1143, 1148–49.

124. *See generally supra* note 88 (summarizing literature discussing these more popular alternatives to cookies in targeted advertising).

125. Google, *Protecting Privacy Online*, THE PRIVACY SANDBOX, https://privacysandbox.com [https://perma.cc/AB5N-DMSS].

126. Even if cookies remained a central technology for ad tracking, banners would not provide meaningful remediation to those harms. *See supra* Section III.A.1.

choices; and they do not reduce the downstream harms of surveillance advertising. At best, they function as legal cover, shifting responsibility to individuals while the structures of digital surveillance remain intact. At worst, they normalize the very practices they were meant to contest, by conditioning users to click through and acquiesce. Cookie banners are thus ineffective not only because they regulate an increasingly outdated technology, but because their very design and function convert harm prevention into ritual performance.

3. Friction to Information

Beyond undermining genuine consent, cookie banners also impose substantial real-world friction, disrupting information flow and dragging down productivity. While privacy harms are often characterized as abstract or diffuse, the time cost of interacting with banners is quite concrete: Europeans collectively spend 575 million hours per year clicking through cookie prompts, the equivalent of 287,500 full-time employees clicking on banners.[127] This isn't a benign inconvenience — it reflects a systemic drag on attention, productivity, and the economy at large. The relentless interruptions mean users (especially in Europe) experience widespread "banner fatigue." Also known as "consent fatigue" or "privacy fatigue," this is the notion that repeated requests for a user to actively consent or not consent to accessing information wears down the user psychologically and diminishes their likelihood to continue to seek information.[128] Every new site visit becomes an involuntary pause, with users primed to click through quickly, often without engaging the information or appreciating the notice. The economic impact of this is clear — people are less likely to buy the more friction is placed between searching and

127. *Europeans Spend 575 Million Hours per Year Clicking Through Cookie Banners*, LEGISCOPE (Oct. 23, 2025), https://www.legiscope.com/blog/hidden-productivity-drain-cookie-banners.html [https://perma.cc/8QWX-WB64] (estimate scaled from EU population, site interactions, and average banner interaction time).

128. *See, e.g.*, Hanbyul Choi, Jonghwa Park & Yoonhyuk Jung, *The Role of Privacy Fatigue in Online Privacy Behavior*, 81 COMPS. HUM. BEHAV. 42, 42–51 (2018) https://doi.org/10.1016/j.chb.2017.12.001 (empirically conceptualizing privacy fatigue in order to examine its role in online privacy behavior); *Technical Report of the Joint Research Centre of the European Commission on Testing the Effect of Cookie Banners on Behaviour*, 12–14 (2016), https://publications.jrc.ec.europa.eu/repository/bitstream/JRC103997/jrc103997.pdf [https://perma.cc/3KJD-YVJ8] (demonstrating that banner design alters acceptance rates, number of users seeking more information, and time spent engaging with cookie policies). This is an analogous idea to the notion of "digital resignation" coined by Nora Draper and Joseph Turow, which they describe as "the condition produced when people desire to control the information digital entities have about them but feel unable to do so." Nora A. Draper & Joseph Turow, *The Corporate Cultivation of Digital Resignation*, NEW MED. & SOC'Y 1 (Mar. 8, 2019), https://www.cs.cornell.edu/~shmat/courses/cs5436/draper-turow.pdf [https://perma.cc/8A8Q-C5V7].

purchasing — but more importantly they degrade the access to information that is essential to an informed citizenry.

4. Performative Regulation

Cookie banners also exemplify a broader problem in privacy law: the transformation of substantive regulation into mere performance. Instead of materially limiting surveillance, banners convert compliance into a theatrical ritual that signals legality without changing outcomes.[129] Companies deploy banners not because they want to empower users, but because the law compels them to stage a choice.[130] In practice, the banners often funnel users toward the same result — acceptance of tracking — through pre-set defaults, layered menus, or manipulative design.[131] Regulators can point to visible compliance, and companies can point to user "consent," yet the underlying practices of data collection and behavioral profiling proceed largely undisturbed.

This kind of performative regulation is damaging for at least two reasons. First, it corrodes trust in both institutions and law. When users experience a mandated ritual that plainly lacks substance, they conclude — reasonably — that privacy regulation is toothless.[132] Second, it entrenches surveillance capitalism by normalizing the act of consent itself. Users habituated to clicking "accept" dozens of times a day internalize the idea that privacy is something routinely bargained away.[133] Instead of pushing industry toward less intrusive models, banners entrench the very dynamics they were meant to resist. In effect, the banner becomes the performance by which law sustains the legitimacy of ongoing surveillance.

5. Environmental Impact

Cookie banners also impose an overlooked environmental burden. Each banner and consent management protocol often requires additional code to be loaded, rendered, and executed, generating extra processing time on user devices and servers and transmitting more data

129. *See* Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CAL. L. REV. 1221, 1228–33 (2022).

130. *See* Kar & Yu, *supra* note 2, at 1119–20.

131. *See supra* Section III.A.1.

132. JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 110–15 (2012) (arguing that hollow privacy rituals undermine democratic legitimacy).

133. *Id.* at 120–24; *see also* Allen, *supra* note 94, at 118 (arguing that repeated waivers normalize the erosion of privacy values).

across networks.[134] This additional rendering creates additional processing time or page load time on browsers and consumes more energy.[135] Estimates suggest cookie consent banners and their associated infrastructure consume approximately ten million kilowatt-hours of electricity per day worldwide.[136] This energy use carries an associated carbon footprint estimated at 11,442 metric tons of carbon dioxide a month.[137] While the energy cost of a single banner impression may be negligible, the ubiquity of banners across billions of pageviews multiplies these marginal costs into a measurable ecological impact and a negative-sum outcome of regulatory design.

6. Prevents New Meaningful Regulation

Perhaps the most pernicious consequence of the cookie banner regime is that it crowds out more effective regulatory responses. Once a legal system builds its privacy protections on the scaffold of consent banners, lawmakers and regulators can point to the banners themselves as evidence that privacy has been addressed. In this way, a minimal and largely symbolic measure becomes the ceiling rather than the floor of protection.

Scholars of mandated disclosure have long warned about this dynamic. Omri Ben-Shahar and Carl Schneider describe disclosure as a "cheap" fix that reassures policymakers they have acted, while

---

134. Nikolas Wehner, Michael Seufert, Raimund Schatz & Tobias Hoßfeld, *Do You Agree? Contrasting Google's Core Web Vitals and the Impact of Cookie Consent Banners with Actual Web QoE. Quality and User Experience*, 8 QUAL. & USER EXPERIENCE 1, 3, 16 (2023) (describing the impact of cookie banners on user experience using page load time as a metric and finding banners increase page load time); Maximilian Hils, Daniel W. Woods, & Rainer Böhme, *Measuring the Emergence of Consent Management on the Web*, ACM INTERNET MEASUREMENT CONF. 2020 317, 318, 324 (measuring consent management protocols like pop-up banners on user interfaces creating "waiting time" for users and reporting that, for consent management protocol deployment can trigger substantial additional HTTP(S) requests, additional data transfer, and "additional JavaScript timeouts," i.e., extra execution and network activity attributable to the consent mechanism).

135. *See generally* Nadja Peters, Sangyoung Park, Samarjit Chakraborty, Benedikt Meurer, Hannes Payer & Daniel Clifford, *Web Browser Workload Characterization for Power Consumption*, 2016 IEEE INT'L CONF. ON HARDWARE/SOFTWARE CODESIGN & SYS. SYNTHESIS (CODES+ISSS) (breaking down browser CPU time and CPU energy for page loading into downloading, rendering, displaying; finding the renderer can consume up to ~70% of energy and further attributing renderer energy across HTML/CSS/JavaScript). *But see generally* Joshua Aslan, Kieran Mayers, Jonathan G. Koomey & Chris France, *Electricity Intensity of Internet Data Transmission: Untangling the Estimates*, 22 J. INDUS. ECOLOGY 785 (2017) (discussing the difficulty of measuring electricity use on internet services and data transmission and analyzing the different methodologies used).

136. Erwin Sotiri, *How Much Energy EU Cookie Consent Policy Costs?*, JURISCONSUL (Feb. 6, 2024), https://www.jurisconsul.com/post/cookie-policy-energy-cost [https://perma.cc/QR5F-HYJF].

137. Alex LaCasse, *Measuring the Carbon Cost of Browsing Cookies*, IAPP (Apr. 26, 2022), https://iapp.org/news/a/carbolytics-measuring-the-carbon-cost-of-browsing-cookies [https://perma.cc/6C5D-CNA8].

leaving underlying power imbalances untouched.[138] Privacy scholars echo the point: Dan Solove criticizes "privacy self-management" for consuming regulatory oxygen that might otherwise support structural reforms,[139] while Julie Cohen warns that privatizing governance through consent rituals forecloses attention to more systemic problems.[140] Once banners became the chosen mechanism, political energy that might have been directed toward substantive limits on behavioral advertising, data retention, or cross-site tracking was dissipated into designing, tweaking, and enforcing banner compliance.

It is not just government that allows the existence of law to forgo ongoing change. Industry is also responsible.[141] This is not only because industry lobbying groups have increased influence on regulatory processes, but because firms often seek out regulation to reduce their risk and legal uncertainty and then prefer stasis within that regulation.[142] That stasis is preferred because once firms have figured out and tested the boundaries of compliance with the law, it is logically far easier and less costly to maintain an established regulatory regime than to learn how to comply with new requirements. The existence of the law and the high visibility of cookies banners also allows firms to perform good lawful behavior — not just for government regulators but for their own users.

The establishment of the cookie banner notice and consent ritual thus favors both regulators and the industry they are regulating. Firms can point to their banners and compliance regimes and regulators can defend their work for citizens' online privacy themselves by pointing to visible banners and their compliance rates. In practice, this creates a form of regulatory inertia. By the time enforcement bodies acknowledge that banners are ineffective, the practice is entrenched, businesses are invested in compliance infrastructures, and new reform proposals are met with the hypothetical objection that such regulation for cookies already exists. In this sense, banners not only fail to solve the problem; they actively prevent more robust solutions from being developed.

---

138. Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PENN. L. REV. 647, 682 (2011).

139. Solove, *supra* note 91, at 1892–96.

140. Julie Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1917 (2013).

141. This is the idea of so-called regulatory capture which "refers to the subversion of regulatory agencies by the firms they regulate." Richard A. Posner, *The Concept of Regulatory Capture: A Short, Inglorious History, in* PREVENTING REGULATORY CAPTURE: SPECIAL INTEREST INFLUENCE AND HOW TO LIMIT IT (Daniel Carpenter & David A. Moss eds., 2013). This concept is originally credited to George J. Stigler, *The Theory of Economic Regulation*, 2 BELL J. ECON. & MGMT. SCI. 3 (1971) (arguing that regulation often reflects the interests of the regulated who control the regulatory process).

142. Stigler, *supra* note 141, at 3 ("Regulation may be actively sought by an industry, or it may be thrust upon it. A central thesis of this paper is that, as a rule, regulation is acquired by the industry and is designed and operated primarily for its benefit.").

B. The Positive

1. Visibility of Data Practices and General Privacy Awareness

Perhaps the most defensible achievement of cookie banners is that they rendered data collection practices visible to ordinary users. Before the EU's ePrivacy Directive and its 2009 amendment, much of online tracking occurred silently, with third-party cookies placed without general user awareness.[143] Like a giant public service announcement, banners forced websites to acknowledge these practices at the point of entry, reminding users that their browsing generates data and that consent is legally implicated. This visibility effect is not trivial. Privacy law often struggles with the problem of salience: harmful practices remain invisible to those affected until that harm has arguably occurred.[144] By requiring banners, regulators created a daily reminder that surveillance exists.

Cookie banners' high visibility has not only made people more aware of the tracking infrastructure around them, but cookie banners also have served as a catalyst for broader privacy awareness. However, it is important to note that surveys indicate that while users might have heightened awareness of available choices as a result of cookie banners, these choices can be manipulated by the design of the banners and so called "dark patterns."[145] Nevertheless, what had once been the concern of specialists became part of everyday experience, seeding awareness that later facilitated acceptance of stronger reforms like the GDPR and the CCPA. Because privacy law often advances not only through technical rules but through cultural legitimation, by forcing repeated encounters with privacy choices (however hollow) banners created a population more attuned to the language of consent, data rights, and opt-outs.

2. Formal Equality

Though a marginal contribution, the EU's cookie banner regime demonstrates how formal equality operates as a stabilizing feature of

---

143. JONES, *supra* note 12, at 134 (describing the emergence of public awareness around cookies in the mid-1990s).

144. Julie Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 181 (2008) (discussing the relationship between privacy, visibility, and its impact on categorizing "harm" for the purposes of U.S. jurisprudence).

145. *See generally* Jan M. Bauer, Regitze Berstrøm, Rune Foss-Madsen, *Are You Sure, You Want a Cookie? – The Effects of Choice Architecture on Users' Decisions About Sharing Private Online Data*, 120 COMP. HUM. BEHAV. (2021) (showing how choice architecture of cookie banners can be understood as a difference between outcome and process); Hana Habib, Megan Li, Ellie Young & Lorrie Cranor, *"Okay, Whatever": An Evaluation of Cookie Consent Interfaces*, 2022 CONF. ON HUM. FACTORS COMPUTING SYS. (analyzing different cookie consent interfaces to determine the best model for usability).

data-protection law. The ePrivacy Directive and later the GDPR, require that every entity that stores or accesses information on a user's device must obtain prior informed consent, regardless of size, industry, or purpose.[146] This universal requirement exemplifies equality before the law in its formal sense — identical obligations for all data controllers and equal informational rights for all users.[147] The approach yields the classical benefits of formal equality: legal uniformity and predictability across Member States[148] administrative neutrality through impersonal application[149] and normative legitimacy grounded in the equal worth of all data subjects.[150] Its endurance across two decades — surviving technological change and regulatory revision — illustrates the durability of formal equality as a structural feature of EU legality rather than a transient policy choice.[151]

There are significant limits to the equality afforded by this formalism. Equal procedural duties do not ensure equal substantive privacy: uniform banners often overwhelm users with consent requests, leading to "consent fatigue" and routinized acceptance; compliance burdens fall unevenly, imposing proportionally heavier costs on small websites than on large platforms, and the abstract notion of "informed" consent rarely translates into meaningful user understanding.[152] Thus, while cookie banners embody the virtues of formal equality — clarity, consistency, and legal impartiality — they also reveal its core weakness: sameness of rule can entrench, rather than alleviate, substantive inequalities in informational power.

---

146. Directive 2002/58/EC, *supra* note 29; GDPR, *supra* note 43, at art. 4(32).

147. Directive 2002/58/EC, *supra* note 29, at art. 5(3); GDPR, *supra* note 43, at arts. 4(11), 6–7.

148. *See generally* A.V. DICEY, INTRODUCTION TO THE STUDY OF THE LAW OF THE CONSTITUTION 193 (Macmillan, 10th ed., 1959) (arguing equality before the law *produces* predictability and restraint of arbitrary power, since all individuals, regardless of rank, are subject to the same courts and laws).

149. *See generally* LON L. FULLER, THE MORALITY OF LAW 110 (1964) (describing generality, among other things as conditions of law that preserve fairness and predictability under the law).

150. G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948); International Covenant on Civil and Political Rights art. 26, Dec. 16, 1966, 999 U.N.T.S. 171.

151. *See generally* H.L.A. HART, THE CONCEPT OF LAW 77–96 (1961); RON DWORKIN, TAKING RIGHTS SERIOUSLY 81–130 (1977). Hart and Dworkin each describe equality as embedded in the rule of law's generality and consistency — Hart by showing that stable legal systems depend on uniform application of primary and secondary rules, and Dworkin by arguing that rights-based adjudication constrains shifting policy preferences — together illustrating that formal equality endures as a structural condition of legal order rather than a contingent legislative choice, including within the EU's rights-based legal framework.

152. *See* arguments *supra* Section III.A.

IV. THE SOLUTION: BAN COOKIE BANNERS

The European Union's regulatory system is distinctive in its built-in capacity for continuous legal revision and iterative governance. Unlike most national systems, EU lawmaking incorporates formal mechanisms — such as ex post evaluation, delegated acts, and periodic Commission reviews — that require institutions to assess how directives and regulations function in practice and to update them accordingly.[153] The European Commission routinely issues "fitness checks" and REFIT evaluations to measure proportionality and effectiveness, while Parliament and Council can request amendments through ordinary legislative procedure without reopening the entire treaty framework. This cyclical process, reinforced by the Commission's quasi-executive role and by judicial interpretation from the Court of Justice of the European Union, allows EU law to evolve dynamically while preserving legal continuity — making the Union one of the few legal orders designed to treat legislation itself as a living, reviewable instrument.

On September 16, 2025 the European Commission announced a "simplification" initiative to review measures looking at "outdated rules on the use of cookies and other tracking technologies . . . ."[154] The initiative aims to require "pragmatic and immediate clarifications to limit consent fatigue, provide legal clarity on rightful access and processing, and enhanced data availability to businesses."[155] This opportunity makes the solutions proposed in this Article far less hypothetical and the options much more clear. There are two straightforward arguments for reform to the laws that have led to cookie banners. The first is to make changes to the procedures of notice and required consent that have led to ineffectiveness and harmful side-effects.[156] The second obvious reform is expansion of the coverage of notice and consent to the new types of ad technology tracking tools websites use beyond cookies.[157] While these reform approaches both seem moderate and reasonable, for the reasons provided below, no reform solution that adheres to a notice and consent regime will effectively address the underlying harms of ad tracking without continuing to perpetuate the broader harms currently caused by cookies banners. The only solution is to end notice and consent mandates —

153. European Commission, *Evaluating laws, policies and funding programmes*, https://commission.europa.eu/law/law-making-process/evaluating-and-improving-existing-laws/evaluating-laws_en [https://perma.cc/GWE4-R9TD].

154. European Commission, *supra* note 10.

155. *Id.*

156. *See supra* Section III.A.

157. *See supra* Section III.A.2.

cookie banners — for ad tracking and open an entirely new conversation for regulatory reform.

A. "Why Govern Broken Tools?"

In the midst of the COVID-19 pandemic, privacy scholar Ryan Calo was asked to write a brief essay about the possibility of creating privacy protective regimes and governance structures to allow for digital contact tracing through Bluetooth technology.[158] After reviewing the feasibility and studies on efficacy, Calo concluded that the practical technical use of Bluetooth for contact tracing "amounts to a lot of noise," and its potential ability to provide better public health "is limited."[159] "In other words," Calo argues, "it is not clear why societies should attempt to find a Goldilocks form of governance for DCT [digital contact tracing] at all . . . . [T]he proper response to the failures of DCT may not be a better balance of privacy, civic participation, and emergency response. It may be to invest scarce public dollars elsewhere."[160] So too is the deployment of online notice and consent for cookies tracking so fundamentally flawed, that reform of the law either in legal procedure or technical purview is an exercise in futility.

It is worth noting, however, for those that see the problems of online privacy and notice and consent as comorbid with contract law, this is not necessarily the case. Despite diagnosing "the contractual death of privacy," Kar and Yu claim to propose a cure, or at least a way towards resurrection.[161] While they argue that the contractualization of privacy policies have been corrosive to the idea of consent, they see contract law as a source of reform. Instead of treating privacy policies as enforceable boilerplate that strip rights, courts should interpret contacts as "grounded 'in a nuanced and careful assessment of the common understands that parties produce when they use language to form contracts.'"[162] They envision a model where courts scrutinize the content of privacy terms, reject waivers of fundamental rights, and hold firms to higher standards of fairness and honesty in data practices under a "shared meaning analysis."[163] In their framing, this would mark a "rebirth" of privacy through contract: transforming privacy agreements from adhesion disclaimers into vehicles for better understanding the intentions and reasoning of the parties. In short, Kar & Yu's

158. Ryan Calo, *Why Govern Broken Tools?*, 50 J.L. MED. & ETHICS 805 (2022).
159. *Id.*
160. *Id.* at 806.
161. Kar & Yu, *supra* note 2, at 1137.
162. *Id.* at 1138 (citing Kar & Radin, *supra* note 98, at 1143).
163. *Id.* at 1137–41.

prescription is not to abandon privacy through contract, but to rehabilitate contract law that it may be a better solution to privacy.

This solution, however, conflates the genesis of two different types of online privacy reforms: those whose "paradigm slip" has come as a result of judge-made changes in the law and those that have come about as a result of top-down regulation. Cookie banners are the latter. Their existence stems from legislative choices in the ePrivacy Directive and GDPR, not judicial interpretation of online privacy policies. As such, the straightforward solution to the problem of adhesion contracts in the banner context is not to reconceptualize them as enforceable duties or shared meaning analysis but to simply abolish them altogether. Banners fail both substantively (they do not prevent surveillance harms) and procedurally (they cannot deliver meaningful consent), and their persistence only entrenches a failed model of privacy self-management. A more effective approach is to repeal banner mandates and replace them with structural protections: direct regulation of tracking technologies, privacy by design at the browser and operating-system level, firm-side duties of fairness and proportionality, and sustainability considerations that eliminate the ecological waste banners impose.

The futility of solution in doctrinal contract reform in the fundamental notion of consent lies in the way individuals experience form contracts. As Roseanna Sommers and others have shown, ordinary people understand contracts through entrenched mental schemas: they imagine them as long, unreadable documents filled with hidden strings, documents that bind whether or not they are read.[164] A single click or signature feels like the magic moment of obligation.[165] David Hoffman, in parallel, has argued that these forms operate less as bargains than as scripts: cheap, mass-produced rituals that condition

164. Roseanna Sommers, *Contract Schemas*, 17 ANN. REV. L. & SOC. SCI. 293, 295 (2021) (reviewing literature on lay conceptions of contracts and finding schemas activated by unreadable legalese and formal signatures); Dennis P. Stolle, *A Social Scientific Look at the Effects and Effectiveness of Plain Language Contract Drafting*, 23–26 (May, 1998) (Ph.D. dissertation, University of Nebraska) (focus group study describing contracts as "daunting" documents in small print and legalese, full of "loopholes" and "strings"); Dennis P. Stolle & Andrew J. Slain, *Standard Form Contracts and Contract Schemas: A Preliminary Investigation of the Effects of Exculpatory Clauses on Consumers' Propensity to Sue*, 15 BEHAV. SCI. & L. 83, 88–91 (1997) (describing 1990s experiments showing participants assumed waivers even when none were present); Zev J. Eigen, *The Devil in the Details: The Interrelationship among Citizenship, Rule of Law and Form-Adhesive Contracts* , 41 CONN. L. REV. 381, 409–25 (2008) (describing empirical evidence that people perceive contracts as unreadable and fail to process terms); Tess Wilkinson-Ryan & David Hoffman, *The Common Sense of Contract Formation,* 67 STAN. L. REV. 1269 (2015) (examining empirically when and how people form contracts and when they believe a contract to exist); Meirav Furth-Matzkin & Roseanna Sommers, *Consumer Psychology and the Problem of Fine Print Fraud*, 72 STAN. L. REV. 503, 527–29 (2020) (finding participants assumed they had waived rights even when contracts explicitly preserved them).

165. Sommers, *supra* note 164, at 302.

behavior and externalize costs.[166] The ritual of form itself — signing, clicking, acquiescing — shapes conduct, deters assertion of rights, and entrenches inequality.[167] Cookie banners exemplify this pathology. They are not read, not understood, not negotiated; yet they discipline users to believe they have consented, and they provide firms with the appearance of legitimacy.

Mandated disclosure only compounds this problem. As Omri Ben-Shahar and Carl Schneider have demonstrated across dozens of fields, disclosure requirements chronically fail: lawmakers overestimate their value, firms manipulate them, and individuals cannot or will not make use of them.[168] Banners are disclosure in its purest and most pernicious form. They appear at the threshold of every website, demanding impossible acts of comprehension in real time, and then converting the inevitable click into evidence of informed consent. Like credit-card APR boxes or health-care consent forms, they promise empowerment but deliver resignation, crowding out more substantive forms of regulation.[169]

B. Not Reform, No More Forms

Seen in this light, the problem with banners cannot be solved by layering new contractual duties or judicial interpretations on top of a broken form. The defect is structural: banners rest on a faith in individual consent that psychological research, empirical studies, and decades of legal scholarship have shown to be misplaced. They do not inform, they do not empower, they do not prevent harm. They are rituals of adhesion that exploit how people think about contracts, scripts that discipline behavior regardless of enforceability, and disclosures that predictably fail to achieve their ends.

The solution is simple: get rid of them. Similar to Calo's directive not to govern broken tools, there is good support for simply eliminating a notice and consent approach among contract law scholars. In his critique of the "empire of forms," Hoffman calls for fewer contracts specifically — arguing that the law should not try to polish or salvage mass forms but should drastically reduce their number, reserving enforceability for a smaller set of agreements where real assent is

166. David A. Hoffman, *Defeating the Empire of Forms*, 109 VA. L. REV. 1367, 1374–75 (2024).

167. *Id.*

168. Ben-Shahar & Schneider, *supra* note 138, at 678–84; *see also* Tess Wilkinson-Ryan, *The Perverse Consequences of Disclosing Standard Terms*, 103 CORNELL L. REV. 117, 123 (2017).

169. *See* Ben-Shahar & Schneider, *supra* note 138, at 705–09 (describing cavalcade of contracts assailing hypothetical consumer).

plausible.[170] Indeed, rather than continue to tolerate the infinite loop of banner failure, law should insist on "fewer forms" and disallow those that impose significant burdens without delivering meaningful value. Cookie banners fall squarely in this category.[171] They are ubiquitous, manipulative, and substantively empty. Applying Hoffman's prescription leads to a simple conclusion: rather than rebirthing banners through contract, we should abolish them outright, freeing privacy law to pursue substantive protections unburdened by the false promise of ritualized consent.

It is critical to note that ending cookie banners does not mean abandoning privacy protection. On the contrary, their elimination would clear the way for stronger, structural solutions that address surveillance harms directly rather than outsourcing responsibility to impossible rituals of consent. A range of alternatives are already visible in law, policy, and scholarship.

One promising path is the development of browser- and device-level privacy signals. The Global Privacy Control (GPC) allows users to broadcast a single preference not to be tracked, and both the California Attorney General and European regulators have recognized it as a valid expression of consent.[172] An enforceable successor to the failed "Do Not Track" initiative[173] would further consolidate user choice at the technical layer, removing the need for repetitive banner interactions.

A second approach is to apply substantive restrictions on behavioral advertising itself. Rather than asking individuals to waive rights, regulators could ban invasive practices like real-time bidding and cross-site profiling.[174] The GDPR already contains principles of data minimization and purpose limitation which requires data collection only where necessary and for specified ends. Those, if

---

170. Hoffman, *supra* note 166, at 1372–77 (proposing that low-stakes written form contracts be unenforceable unless subject to heightened requirements, effectively reversing the Statute of Frauds).

171. *Id.* at 1421–22 (discussing European regulators' approach to requiring Facebook to give choice to consumers).

172. GLOBAL PRIVACY CONTROL, https://globalprivacycontrol.org [https://perma.cc/42VD-QBXR]; California Attorney General, *Enforcement Case Examples* (2021), https://oag.ca.gov/privacy/ccpa/enforcement [https://perma.cc/4JF9-MA24].

173. The "Do Not Track" initiative was a failed proposal that attempted to limit online tracking. It proposed using a web header to send a signal from a user's browser directly to sites they visited indicated they did not want to be tracked, but because no browsers adopted it and no enforcement mechanisms ever came into play, it never had purchase as viable alternative. *See* EFF.org, *Issues*: *Do Not Track*, https://www.eff.org/issues/do-not-track [https://perma.cc/6W4W-3G5K].

174. *See generally* Michael Veale & Federik Zuiderveen Borgesius, *Adtech and Real-Time Bidding Under European Data Protection Law*, 23 GERMAN L.J. 226 (2022), https://www.cambridge.org/core/journals/german-law-journal/article/adtech-and-realtime-bidding-under-european-data-protection-law/017F027B4E78EBCAE1DCBC1E12B93B9D [https://perma.cc/UF4C-RMGG].

enforced, would significantly reduce tracking without any banners at all.[175]

Third, some scholars propose shifting the frame from consent to fiduciary responsibility. Treating platforms and advertisers as "information fiduciaries" would impose duties of care, loyalty, and confidentiality, ensuring that firms act in the best interests of their users. These models, advanced by Jack Balkin, Neil Richards, and Woodrow Hartzog, build on the recognition that users cannot meaningfully negotiate privacy in any contractual sense but should be entitled to loyalty-like protections from those who hold their data.[176]

Fourth, a regime of privacy by design would embed protections directly into technical systems. Privacy should be the default setting, built into architecture and protocols rather than left to individuals to toggle.[177] The emphasis of privacy by design is on structural safeguards rather than consent rituals, shifting the burden from users to firms and designers. This model extends beyond the narrow scope of cookie banners, aiming to ensure that accountability, fairness, and trust are hardwired into technologies and systems from the outset.[178] Perhaps most urgently, regulators should address the manipulative design of interfaces such as "dark patterns" which show that consent interfaces are engineered to drive acceptance, undermining any claim to voluntariness. Laws like the California Privacy Rights Act now empower regulators to ban such manipulative design.

In short, the path forward is not to repair or expand the purview of cookie banners but to end them, so that we might finally move beyond them: toward browser-level privacy controls, substantive limits on surveillance, fiduciary duties for firms, privacy by design, and sustainable regulation. These alternatives promise real protections, not

---

175. GDPR, *supra* note 43, at art. 5(1)(b)–(c); *see also* Paul M. Schwartz & Karl Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 163–64 (2017).

176. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1215–22 (2016); Richards & Hartzog, *supra* note 129, at 978–80 (2022).

177. *See* INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, PRIVACY BY DESIGN (2011), https://www.ipc.on.ca/en/media/1826/download [https://perma.cc/B4FN-2TYA]; Ira Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1450 (2011).

178. Danielle Citron has called for "technological due process," embedding fairness and accountability into systems to prevent structural harms before they occur. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U.L. REV. 1249, 1283–88 (2008). Woodrow Hartzog similarly emphasizes that privacy law should regulate design choices, not just disclosures, urging policymakers to prohibit manipulative defaults and mandate protective architectures. WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 8–13, 168–72 (2018) (advocating for regulation of design choices as privacy law's central project). Others argue that privacy by design should operate in tandem with duties of loyalty and care, so that firms are required to build systems that protect users' dignity and trust as a matter of law, not optional compliance. Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 452–59 (2016) (arguing that design-based obligations should align with duties of loyalty and care).

the hollow theater of banners, and they should be the foundation of the next generation of privacy law.

V. CONCLUSION

This Article is a simple plea for immediate policy reform to end an ineffective and harmful form of technology regulation. But beyond its advocacy, it is also meant to be a case study and provocation. The regulation that led to cookie banners started twenty-five years ago. What have those laws and the systems they produced shown us about the agility of government to identify problems and create solutions? What have they shown us about the motives and entrenchment of industry? What light have they shone on human behavior? What have they revealed about the way in which technological regulation moves between jurisdictions and markets? What do they tell us about the utility of the concepts of consent and autonomy in legal regulation? Most of all, what do these regulations and the world they created teach us about what we want from our technological regulation in the future?