Harvard Journal of Law & Technology
Volume 37, Number 3 Symposium 2023

IN SUPPORT OF STANDARDS FOR DIGITAL ADVERTISING

*Christo Wilson**

ABSTRACT

Despite being the financial foundation for the modern digital economy, online advertising lacks both technical and regulatory standards governing the collection of tracking data from users and the display of digital advertisements. This lack of standards is at the root of many problems that rob users of their privacy, autonomy, and rights under the law, such as the right to opt out of personalized advertising or request access to data collected about them. To name just a few problems: (1) users' online behavior continues to be tracked with impunity because there is a strong financial incentive to "innovate" new tracking technologies, and there is no regulatory framework to constrain these technologies; (2) users are often frustrated when attempting to activate their data rights because it is unclear what unique identifier their data is associated with; (3) controlling where and when advertisements are displayed online is an error-prone and laborious task because there are no machine-readable standards for the disclosure of promoted content. While emerging technical standards like Global Privacy Control are undoubtedly a step forward for online privacy, they are not designed to address these specific problems.

In this Essay, I argue that additional technical and regulatory standards designed to work in tandem would go a long way towards addressing these problems. I propose two complementary efforts: (1) standardize and mandate the use of application programming interfaces ("APIs") for retrieving tracking identifiers on all major software platforms (e.g., Android and iOS apps, the Web); and (2) standardize and mandate the use of an <ad> tag to disclose digital advertisements. I discuss the technical details of these proposed standards, contrast them with previous and current technical efforts, and argue that these standards would be relatively straightforward to adopt in practice. I also discuss the regulatory dimensions of these standards, the benefits they would bring to users and regulators, and policy challenges.

---

* Associate Professor, Khoury College of Computer Sciences, Northeastern University. I thank the attendees at the *Harvard JOLT*-UIowa IBL Symposium: Beyond the FTC, for their invaluable feedback. I also thank the editors of the *Harvard Journal of Law & Technology* for their thoughtful revisions.

TABLE OF CONTENTS

I. INTRODUCTION

Digital advertising is a $600-billion-dollar industry.[1] It is the primary source of revenue for tech titans, like Google and Meta,[2] as well as for countless publishers and app developers. Digital advertising impacts the lives of every Internet user through the data that is collected for targeted advertising, the privacy risks associated with this data collection, and the monetization of human attention at massive scale.

Despite the importance of advertising to the modern digital economy, there is a surprising lack of systemic governance in this space. I use "governance" to refer to two things: first, the regulatory governance, or the use of law to constrain the behaviors of stakeholders in the digital advertising space; and second, the technical governance, or the use of technical specifications to streamline interactions between stakeholders in the digital advertising space. In this formulation, "systemic governance" is governance that is grounded in the needs of users, implemented in accordance with novel technical standards, and enforced through regulatory measures that mandate compliance with the technical standards. While there is governance writ large in the digital advertising space (e.g., via the General Data Protection Regulation ("GDPR")),[3] I argue that current governance fails to be systemic because it either focuses solely on the needs of industry actors or does not

1. *See Digital Advertising – Worldwide*, STATISTA, https://www.statista.com/outlook/dmo/digital-advertising/worldwide [https://perma.cc/T8LN-MA3L].

2. Billy Duberstein, *Why Google's U.S. Ad Revenue Will Decline but Facebook's Will Grow in 2020*, MOTLEY FOOL (June 23, 2020, 8:10 AM), https://www.fool.com/investing/2020/06/23/why-googles-us-ad-revenue-will-decline-but-faceboo.aspx [https://perma.cc/2TQP-3PPX].

3. Regulation 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, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) [hereinafter GDPR].

address the full range of harms and associated needs experienced by ordinary people.

Regulatory governance on its own has failed to curtail the ills associated with digital advertising. The United States' Federal Trade Commission's ("FTC's") notice and consent framework has not created meaningful transparency around data collection practices.[4] The FTC's guidelines around clear and conspicuous labeling of ads[5] are being constantly tested — even ignored — as disclosures become less prominent,[6] misleading language obfuscates ads,[7] and platforms fail to enforce their disclosure guidelines on content creators.[8] The GDPR improves upon the status quo by demanding affirmative consent for tracking and granting new rights to data subjects.[9] However, the lack of mandatory technical standards has given the industry the opportunity to "self-regulate" in ways that eschew the law's intent. For example, the Interactive Advertising Bureau's ("IAB's") Transparency & Consent Framework ("TCF") for collecting and communicating consent in Europe[10] has facilitated the widespread adoption of dark patterns that

4. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS ii–iii (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [https://perma.cc/MR6P-9WGB].

5. FED. TRADE COMM'N, .COM DISCLOSURES: HOW TO MAKE EFFECTIVE DISCLOSURES IN DIGITAL ADVERTISING 6–7 (2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcom disclosures.pdf [https://perma.cc/U676-DPJV].

6. Ginny Marvin, *A Visual History of Google Ad Labeling in Search Results*, SEARCH ENGINE LAND (Jan. 28, 2020, 8:30 AM), https://searchengineland.com/search-ad-labeling-history-google-bing-254332 [https://perma.cc/U439-SZVB].

7. *See* Muhammad Ahmad Bashir, Sajjad Arshad & Christo Wilson, *"Recommended for You": A First Look at Content Recommendation Networks*, PROC. 2016 INTERNET MEASUREMENT CONF. 17, 20 (2016), https://dl.acm.org/doi/pdf/10.1145/2987443.2987469 [https://perma.cc/B2KS-CPM5].

8. *See* Arunesh Mathur, Arvind Narayanan & Marshini Chetty, *Endorsements on Social Media: An Empirical Study of Affiliate Marketing Disclosures on YouTube and Pinterest*, PROC. ACM ON HUM.-COMPUT. INTERACTION, Nov. 2018, at 20, https://dl.acm.org/doi/pdf/10.1145/3274388 [https://perma.cc/4MPV-PB2Q].

9. GDPR, *supra* note 3, arts. 6, 15. Article 6 covers the need for consent before processing data. Article 15 covers data subject access rights.

10. *See The Transparency & Consent Framework (TCF) v2.2*, IAB EUROPE, https://iabeurope.eu/transparency-consent-framework [https://perma.cc/6TL7-GAVZ].

pervert the idea of consent[11] while failing to accurately and consistently communicate people's choices.[12]

Technical governance of digital advertising on its own also has a poor track record of helping people. Widely adopted technical standards tend to have been developed by and center on industry actors. Examples include standardized sizes for banner ads,[13] data formats for soliciting and responding to bids in programmatic ad exchanges,[14] and de facto standards for cookie synchronization and data sharing.[15] Grassroots technical standards grounded in helping people understand privacy practices and communicate privacy choices — such as the Platform for Privacy Preferences Project[16] and Do Not Track ("DNT")[17] — were intentionally sabotaged by industry actors.[18] The standards were also mostly ignored in practice because there was no mandate that industry actors adopt or comply with them.

---

11. *See generally* Martino Trevisan, Stefano Traverso, Eleonora Bassi & Marco Mellia, *4 Years of EU Cookie Law: Results and Lessons Learned*, PROC. ON PRIV. ENHANCING TECHS. 126, 131–33, 140 (2019); Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger & Lalana Kagal, *Dark Patterns After the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence*, PROC. 2020 CHI CONF. ON HUM. FACTORS COMPUTING SYS., Apr. 2020, at 5 (2020); Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth & Damian Clifford, *Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective*, PROC. 2021 CHI CONF. ON HUM. FACTORS COMPUTING SYS., May 2021, at 11–12 (2021); Paul Graßl, Hanna Schraffenberger, Frederik Zuiderveen Borgesius & Moniek Buijzen, *Dark and Bright Patterns in Cookie Consent Requests*, 3 J. DIGIT. RSCH. 1, 2 (2021); Hana Habib, Megan Li, Ellie Young & Lorrie Cranor, *"Okay, Whatever": An Evaluation of Cookie Consent Interfaces*, PROC. 2022 CHI CONF. ON HUM. FACTORS COMPUTING SYS., Apr. 2022, at 16.

12. *See generally* Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier et al., *Can I Opt Out Yet?: GDPR and the Global Illusion of Cookie Control*, Proc. 2019 ACM ASIA CONF. ON COMPUT. & COMMC'N SEC., July 2019, at 5–6 (2019); Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub & Thorsten Holz, *We Value Your Privacy . . . Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy*, NETWORK & DISTRIBUTED SYS. SEC. SYMP. 2019, Feb. 2019, at 12; Célestin Matte, Nataliia Bielova & Cristiana Santos, *Do Cookie Banners Respect My Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework*, IEEE SYMP. ON SEC. & PRIV., May 2020, at 4–5.

13. *See, e.g.*, *IAB New Ad Portfolio: Advertising Creative Guidelines*, IAB TECH LAB, https://iabtechlab.com/standards/new-ad-portfolio [https://perma.cc/EY5X-PYVJ].

14. *See, e.g.*, *OpenRTB (Real-Time Bidding)*, IAB TECH LAB, https://iabtechlab.com/standards/openrtb [https://perma.cc/2JSL-PJKG].

15. *See, e.g.*, *Cookie Matching*, GOOGLE, https://developers.google.com/authorized-buyers/rtb/cookie-guide [https://perma.cc/7NZQ-AJQN].

16. *See generally* Lorrie Cranor, Brooks Dobbs, Serge Egelman, Giles Hogben, Jack Humphrey, Marc Langheinrich et al., *The Platform for Privacy Preferences 1.1 (P3P1.1) Specification* (World Wide Web Consortium, working group note), https://www.w3.org/TR/P3P11 [https://perma.cc/9UGW-X6GW].

17. *See generally* W3C Tracking Protection Working Group, *Tracking Preference Expression (DNT)*, WORLD WIDE WEB CONSORTIUM (2019), https://www.w3.org/TR/tracking-dnt [https://perma.cc/F473-83AA].

18. *See, e.g.*, Stephen Shankland, *Apache Web Software Overrides IE10 Do-Not-Track Setting*, CNET (Sept. 7, 2012, 9:34 AM), https://www.cnet.com/tech/services-and-software/apache-web-software-overrides-ie10-do-not-track-setting [https://perma.cc/N4RJ-5ZYC].

There are emerging examples of technical and regulatory standards which have been designed to work in tandem, demonstrating that systemic governance may be a viable path forward for quickly improving online privacy and reining in the digital advertising industry.[19] In iOS 14.5, Apple introduced App Tracking Transparency ("ATT"), a system that leverages technical and policy measures to implement an opt-in regime for third-party tracking.[20] On the technical side, apps must use APIs provided by iOS to ask for a user's permission before they may access the device's unique advertising identifier (known as "IDFA").[21] On the policy side, Apple requires apps to obtain user permission before using any identifiers to track users, with the penalty for noncompliance being ejection from the App Store.[22] ATT is not perfect: it does not programmatically prevent the tracking of users (i.e., apps can still surreptitiously use fingerprinting to generate stable unique identifiers for users), and compliance is predicated on strong enforcement by Apple (which, unfortunately, may be lax).[23] But these faults also afflict other attempts to impose consent requirements on digital advertisers (e.g., DNT and the TCF, mentioned above). Further, ATT has dramatically improved peoples' privacy in ways that prior efforts have not, as evidenced by the massive losses faced by online ad networks.[24]

Global Privacy Control ("GPC") is another emerging example of systemic governance. Like its predecessor DNT, GPC is a standard that allows people to easily communicate to websites their preference to opt out of tracking.[25] GPC is intermediated by the web browser, which avoids the annoyance, confusion, and potential for dark patterns that are inherent in per-website opt-out notifications. And, unlike DNT, GPC is recognized as a global opt-out mechanism under the California

19. These examples are meant to highlight how the combination of technical and regulatory standards can work in harmony to achieve privacy goals. However, as these examples concern the policies of a private actor (Apple), I do not consider them to be systemic governance.

20. *See If an App Asks to Track Your Activity*, APPLE, https://support.apple.com/en-us/HT212025 [https://perma.cc/GD69-7YGP].

21. *Id.*; *see App Tracking Transparency*, APPLE, https://developer.apple.com/documentation/apptrackingtransparency [https://perma.cc/AH9B-JKXD].

22. *See User Privacy and Data Use*, APPLE, https://developer.apple.com/app-store/user-privacy-and-data-use [https://perma.cc/T3TL-2LK5].

23. Geoffrey A. Fowler & Tatum Hunter, *When You 'Ask App Not to Track,' Some iPhone Apps Keep Snooping Anyway*, WASH. POST (Sept. 23, 2021, 6:00 AM), https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking [https://perma.cc/CHE9-26R4].

24. Emma Roth, *Apple's App Tracking Policy Reportedly Cost Social Media Platforms Nearly $10 Billion*, VERGE (Oct. 31, 2021, 6:13 PM), https://www.theverge.com/2021/10/31/22756135/apple-app-tracking-transparency-policy-snapchat-facebook-twitter-youtube-lose-10-billion [https://perma.cc/SYW9-RUA9].

25. *Proposal*, GLOB. PRIV. CONTROL, https://privacycg.github.io/gpc-spec [https://perma.cc/TX2A-NYWA].

Consumer Privacy Act ("CCPA")[26] and its successor California Privacy Rights Act ("CPRA"),[27] giving it the force of law.[28]

In this Essay, I argue that the principle of systemic governance should be expanded beyond universal opt-outs to two additional areas implicated by digital advertising:

(1) **Mandatory Identifiers for Advertisers.** More platforms should offer APIs that produce unique tracking identifiers for client software, like Apple's ATT. Regulation should mandate that software running on these platforms use the identifiers produced by the API — and no other — for tracking purposes. This would extend the privacy gains which iOS users currently enjoy to other platforms like the Web.[29] Additionally, forcing digital advertisers to identify users via canonical identifiers would improve users' ability to activate their data subject rights under laws like GDPR or CPRA.

(2) **Machine-Readable Ad Disclosures.** Regulation should require that digital ads carry a standardized, machine-readable disclosure. Platforms that support these machine-readable disclosures could then offer users a robust and reliable set of tools for clearly, conspicuously, and uniformly identifying ads (e.g., through visual or auditory signals), as well as notifying users when they are interacting with ads.

As I discuss below, these two ideas would be relatively straightforward to standardize and deploy at the technical level. Browsers could be updated to support these standards, or support could be added via a browser extension. For desktop and mobile apps, support would need to be built into the operating system — a more challenging but not unprecedented proposition. On the legal side, these technical standards would require new laws or regulations to drive their adoption, but the language of these regulations would be clear and narrow. Most importantly, if adopted, these ideas would empower people with new online privacy tools that could be both powerful and easy to use.

---

26. CAL. CIV. CODE § 1798.100 (West).

27. *Id.* (amended 2020).

28. CAL. CODE REGS. § 999.315; *see also* Maximilian Hils, Daniel W. Woods & Rainer Böhme, *Privacy Preference Signals: Past, Present and Future*, 2021 PROC. ON PRIV. ENHANCING TECHS. 249, 252.

29. I use the phrase "the Web" to refer to the technology stack — primarily Hypertext Markup Language ("HTML") and the JavaScript Document Object Model APIs — that are used to build websites and web applications. People interact with the Web through a web browser, or, in some cases, desktop and mobile apps built using the same technology stack.

II. MANDATORY IDENTIFIERS FOR ADVERTISERS

While global opt-out mechanisms like GPC are important for halting flows of data to digital advertisers, they are not meant to address cases where data has already been collected. This may happen, for example, because a person chooses to opt into tracking or because a person was tracked before they activated an opt-out mechanism. In these cases, data subject rights, rather than consent laws, are the appropriate legal mechanism for resolving questions about previously collected data. The GDPR, CPRA, and other United States state-level laws include provisions that grant data subjects the right to request collected data, modify this data, or have data deleted.

Data subject rights are only actionable, however, if people can successfully identify themselves to businesses. In some contexts (e.g., when a website or app requires people to create a user account), identification is simple. Unfortunately, in the context of digital advertising, identification is far more complicated. There are hundreds of businesses that collect, share, and sell data in the digital advertising ecosystem,[30] and people rarely have direct relationships with those businesses (notable exceptions being large platform owners like Google, Meta, Twitter, and TikTok).[31] Rather than associating data with accounts chosen by people, digital advertisers use a variety of techniques to assign unique identifiers to people. As I discuss below, the lack of control over how identifiers are selected or stored by digital advertisers makes it difficult — sometimes impossible — for people to identify themselves and activate their rights. This identification barrier undermines the intent of data subject access rights within a key context — digital advertising — at the very moment when these rights are becoming more widely available.

One solution is constructing a technical and regulatory edifice that forces digital advertisers to use specific unique identifiers — generated and managed by a person's own device — for tracking purposes. Modern operating systems like iOS, Android, and Windows already include APIs that provide unique identifiers to apps for tracking purposes.[32]

---

30. *See, e.g.*, Steven Englehardt & Arvind Narayanan, *Online Tracking: A 1-Million-Site Measurement and Analysis*, PROC. 2016 ACM SIGSAC CONF. ON COMPUT. & COMMC'NS SEC. 1388, 1395 (2016); Muhammad Ahmad Bashir, Sajjad Arshad, Engin Kirda, William Robertson & Christo Wilson, *A Longitudinal Analysis of the ads.txt Standard*, PROC. INTERNET MEASUREMENT CONF. 294, 300 (2019).

31. *See LUMAscapes*, LUMA, https://lumapartners.com/lumascapes [https://perma.cc/4XHY-MAHN]. The various LUMAscapes diagrams visually categorize the hundreds of companies in the digital advertising ecosystem.

32. *AdSupport*, APPLE, https://developer.apple.com/documentation/adsupport [https://perma.cc/4BB3-T6A7]; *Get a User-Resettable Advertising ID*, GOOGLE, https://developer.android.com/training/articles/ad-id [https://perma.cc/9PNN-HYWT]; *AdvertisingManager.AdvertisingId Property*, MICROSOFT, https://learn.microsoft.com/en-

Three major items are missing to turn the status quo into the proposed edifice:

(1) Laws or regulations mandating that API-generated identifiers, and no others, be used by digital advertisers whenever possible.

(2) More robust user-facing tools on the person's device that allow users to see which identifiers were shared with which websites and apps over time, in order to facilitate the identifiers' use in subject data access requests.

(3) Greater adoption of unique identifier APIs by platforms, particularly by web browsers, so that these capabilities are available outside of the mobile app ecosystem.

No existing law or regulation approaches (1), not even Apple's ATT policy (which permits advertisers to use non-IDFA identifiers if a person consents to tracking).[33] Attaining (1) will require policymakers to engage with technical experts to craft workable, comprehensive policy language and to overcome tech-industry lobbying to put this language into force. Achieving (2) is a straightforward exercise in user interface development. Reaching (3) will require obtaining buy-in from a variety of stakeholders, in particular web browser developers and web standards bodies like the World Wide Web Consortium ("W3C").

Next, I provide additional details and context about tracking identifiers, extant problems with activating data subject access rights, and the benefits and challenges of my proposal.

A. Existing Identifiers are Insufficient for Activating Data Subject Rights

Digital advertisers are rapacious collectors of personal data to facilitate targeted advertising. They are most interested in collecting longitudinal data about people so that they can build profiles that contain, among other information, physical location,[34] demographics,[35] and

---

us/uwp/api/windows.system.userprofile.advertisingmanager.advertisingid?view=winrt-22621 [https://perma.cc/4T2U-6W5K].

33. *See If an App Asks to Track Your Activity*, APPLE, https://support.apple.com/en-us/HT212025 [https://perma.cc/GD69-7YGP].

34. Jingjing Ren, Ashwin Rao, Martina Lindorfer, Arnaud Legout & David Choffnes, *ReCon: Revealing and Controlling PII Leaks in Mobile Network Traffic*, PROC. 14TH ANN. INTL. CONF. ON MOBILE SYS., APPLICATIONS & SERV. 361, 364 (2016).

35. Giridhari Venkatadri, Piotr Sapiezynski, Elissa M. Redmiles, Alan Mislove, Oana Goga, Michelle Mazurek et al., *Auditing Offline Data Brokers via Facebook's Advertising Platform*, WEB CONF. 2019, May 2019, at 2.

interests.[36] To achieve data collection over time, digital advertisers assign or compute unique identifiers that they associate with each device on the Internet, which typically corresponds to a specific person (i.e., the device owner) or household.

Historically, third-party cookies have been the primary mechanism used by digital advertisers to assign unique identifiers to Web users.[37] In this context, each digital advertiser generates a unique, random identifier stored in each web browser within a cookie.[38] Over time, the digital advertiser may read their cookie whenever they interact with this browser, thus enabling longitudinal re-identification and the construction of a data profile.[39]

Some digital advertisers enable people to request the data that has been collected about them by leveraging the third-party cookies. This scenario is deceptively straightforward: the data subject visits the digital advertiser's website and then the advertiser looks up the subject's data based on the identifier stored in their cookie. However, this process is extremely brittle: cookies expire over time and may be cleared at users' discretion. Further, digital advertisers may choose to replace their cookie with a new one — containing a new unique identifier — at any time. In these scenarios, the data collected by the digital advertiser that was associated with the original unique identifier is no longer accessible.

Third-party cookies are currently being phased out,[40] so some digital advertisers are migrating to other stateful, unique identifiers.[41] The Trade Desk is leading an industry consortium around the Unified ID 2.0 ("UID 2.0") standard, which aims to use a user's cryptographically hashed email address and/or phone number as a stable, unique identifier.[42] If a website or app is able to convince a person to divulge their email address or phone number, digital advertisers can recompute the

---

36. Muhammad Ahmad Bashir, Umar Farooq, Maryam Shahid, Muhammad Fareed Zaffar & Christo Wilson, *Quantity vs. Quality: Evaluating User Interest Profiles Using Ad Preference Managers*, NETWORK & DISTRIBUTED SYS. SEC. SYMP. 2019, Feb. 2019, at 3.

37. *See* Aaron Cahn, Scott Alfeld, Paul Barford & S. Muthukrishnan, *An Empirical Study of Web Cookies*, PROC. 25TH INT'L CONF. ON WORLD WIDE WEB 891, 894 (2016). There are additional mechanisms in web browsers that allow digital advertisers to store unique identifiers — e.g., ETags and LocalStorage — but these offer similar functionality as cookies. Thus, I do not discuss them in depth.

38. Steven Englehardt, Dillon Reisman, Christian Eubank, Peter Zimmerman, Jonathan Mayer, Arvind Narayanan et al., *Cookies That Give You Away: The Surveillance Implications of Web Tracking*, PROC. 25TH INT'L CONF. ON WORLD WIDE WEB 289, 290 (2015).

39. Bashir et al., *supra* note 36, at 1–2.

40. As of this writing, third-party cookies are set to be phased out in 2024. *See The Privacy Sandbox Timeline for the Web*, PRIV. SANDBOX, https://privacysandbox.com/open-web/#the-privacy-sandbox-timeline [https://perma.cc/VP5M-77LQ].

41. "Stateful identifiers" are identifiers that are stored persistently on a computer, as opposed to "stateless identifiers" like fingerprints, which can be regenerated at any time.

42. *See Unified ID 2.0*, TRADEDESK, https://www.thetradedesk.com/us/about-us/industry-initiatives/unified-id-solution-2-0 [https://perma.cc/FE58-9T3G].

UID 2.0 for that person in that context and add this new data to the profile associated with that UID 2.0.

Unique identifiers derived from personal information, like UID 2.0, cannot safely be used to authenticate requests for subject data.[43] A given person's email address and phone number are effectively public information.[44] This makes it easy for an attacker to compute the UID 2.0 of a victim, request the associated subject data from digital advertisers, and then receive copies of the victim's data.

Rather than rely on stateful identifiers, some digital advertisers use probabilistic identifiers known as fingerprints.[45] All computers are slightly different. Online advertisers can measure these subtle differences and use them to compute a semi-unique identifier — the fingerprint — for a given computer.[46] Online advertisers then associate tracking data and profiles with the fingerprint.[47] There is no way to remove all these subtle differences from computers, and technologically-sound methods for preventing the computation of fingerprints entail sacrificing almost all the usability of modern computing platforms.[48]

Fingerprints are impractical identifiers for activating data subject rights. Fingerprints tend to be stable for limited periods of time, but operating system updates, web browser updates, or changes to system settings often cause fingerprints to change. Thus, fingerprints are sufficiently stable to enable short-term tracking of a person's behavior but change often enough to preclude using them as reliable identifiers for activating data subject rights over long time periods.[49] Furthermore, digital advertisers can calculate fingerprints using an infinite number of algorithms.[50] This precludes the possibility of a platform — i.e., the operating system or web browser — fingerprinting itself periodically and storing the identifiers to facilitate the activation of data subject rights at some point in the future.

Yet another approach used to authenticate people when they attempt to invoke their data subject rights is, essentially, standard background checking: a business may demand that a data subject provide hard evidence of their identity (e.g., scans of national identity

---

43. Unique identifiers that are derived from personal information are, in general, a privacy nightmare. Because a person's email address and phone number tend to be stable over time, any identifier derived from them will also be stable and uniform across digital advertisers, thus enabling advertisers to track people over time and across devices.

44. Peter Snyder, Periwinkle Doerfler, Chris Kanich & Damon McCoy, *Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing*, PROC. 2017 INTERNET MEASUREMENT CONF. 432, 433 (2017).

45. *See* Pierre Laperdrix, Nataliia Bielova, Benoit Baudry & Gildas Avoine. *Browser Fingerprinting: A Survey*, ACM TRANSACTIONS ON WEB, Apr. 2020, at 11–12.

46. *See id.*

47. *See id.*

48. *Id.* at 14.

49. *See id.* at 8.

50. *See id.* at 11–12.

documents) or answer knowledge-based questions (e.g., "what was your street address in 1999?") to authenticate themselves.[51] While there are contexts where this level of rigorous authentication is appropriate, this is not the case with most or all digital advertisers. Many digital advertisers cannot use this authentication approach at all because they only know data subjects by their unique identifiers, not by evidence of their identity or self-knowledge. Furthermore, even if a digital advertiser did ask data subjects to present hard evidence of their identity, people might feel justifiably concerned about handing extremely sensitive personal information over to a business that they do not know or have any direct relationship with.

B. ATT For Everyone, Everywhere

As Apple's ATT system has demonstrated, centralizing the creation of unique identifiers on the platform creates powerful capabilities for managing privacy. On iOS, apps cannot access the IDFA until they have obtained consent from the user — basically, an opt-in model for tracking. The consent process is managed by iOS, so it is consistent and free of dark patterns. iOS allows users to permanently disable the IDFA to opt out of tracking entirely or to reset the IDFA so that past and future activity is more difficult to correlate. On Android, Google is finally updating their AAID APIs such that opting out of tracking also prevents apps from reading the AAID.[52]

This Essay proposes regulations mandating that digital advertisers only use unique identifiers produced by platform APIs for the purposes of tracking, giving ATT and similar APIs the force of law alongside platforms' own policies. To ensure that unique identifiers from platform APIs do not erode privacy or security, regulations should state that these APIs must adopt a privacy-by-default posture. First, like the ATT implementation on iOS, these APIs should be opt-in: an app or website cannot receive a unique identifier from the API until the user explicitly chooses to allow it. Second, these APIs should return a different unique identifier per app and per website to prevent cross-context tracking. Enforcing different unique identifiers per context also ensures that these APIs cannot be abused for fingerprinting. Third, these APIs

---

51. *See* Mariano Di Martino, Pieter Robyns, Winnie Weyts, Peter Quax, Wim Lamotte & Ken Andries, *Personal Information Leakage by Abusing the GDPR "Right of Access*,*"* PROC. 15TH SYMP. ON USABLE PRIV. & SEC. 371, 374–75 (2019); Luca Bufalieri, Massimo La Morgia, Alessandro Mei & Julinda Stefa, *GDPR: When the Right to Access Personal Data Becomes a Threat*, PROC. IEEE INT'L CONF. ON WEB SERV., May 2020, at 3; Coline Boniface, Imane Fouad, Nataliia Bielova, Cédric Lauradoux & Cristiana Santos, *Security Analysis of Subject Access Request Procedures*, 2019 ANNUAL PRIV. FORUM, June 2019, at 7.

52. *See AdvertisingIdClient.Info*, GOOGLE, https://developers.google.com/android/reference/com/google/android/gms/ads/identifier/AdvertisingIdClient.Info [https://perma.cc/CA8X-VDAE].

should be accessible only to apps and websites that adopt encryption across all their network communications. Taken together, these three stipulations ensure that these APIs cannot be abused for surreptitious eavesdropping,[53] as well as ensuring that they offer less utility to law enforcement than existing problematic identifiers like International Mobile Equipment Identity ("IMEI").

Standardizing the unique identifiers used by digital advertisers and centralizing control over identifiers on peoples' devices helps to solve the data subject access rights problem. Operating systems and user-agents (e.g., web browsers) that implement the relevant APIs can easily record all the unique identifiers provided to client software (e.g., apps and websites). Creating a user interface for people to view these identifiers so that they may be presented to businesses as part of requests for data is straightforward. This basic system works even if the identifiers given out have changed over time, as the complete history of identifiers can be stored, presented to users, and even made searchable by time or by recipient.

We can envision a wide range of user interface designs that would add further utility to this functionality. Operating systems and user-agents could allow users to disable the unique identifier APIs entirely, at which point users would never again be asked to consent to tracking on that device. Additionally, user-agents could cluster apps and websites together by category (e.g., shopping, social networking, fitness, etc.) and present a user interface for managing tracking preferences per category (e.g., the default opt-out, opt in with unique identifiers per service, or opt in with a single unique identifier across all services in the category). Users could then quickly express their preferences within categories where they would like to receive targeted ads.

Mandating that digital advertisers use unique identifiers provided by platform APIs for tracking purposes would set a clear behavioral standard for industry participants. Stipulating that this mandate only applies to software running on platforms that have the requisite APIs would alleviate ambiguity for developers about where the rules apply. We can even envision a process where the FTC or another regulator maintains a list of platforms on which the mandates apply, to be updated on a periodic basis. Realistically, even a short list that covered the Web, the four most popular operating systems, and a small number of embedded operating systems used in smart TVs would cover the vast majority of user-facing software.[54]

Ideally, this mandate must be coupled with strong enforcement. This could be done by allowing for a right of private action against

---

53. *See* Englehardt et al., *supra* note 38, at 296.

54. *See Operating System Market Share Worldwide*, STATCOUNTER, https://gs.statcounter.com/os-market-share [https://perma.cc/KG69-SSNB].

digital advertisers who use unsanctioned unique identifiers, or by empowering a federal or state agency (e.g., the California Privacy Protection Agency) to levy fines for non-compliance.

While digital advertisers will surely protest any attempt to constrain their behavior,[55] the reality is that they already face restrictions on their use of certain classes of unique identifiers. For example, the Google Play Store Developer Policy restricts the use of device identifiers (e.g., IMEI) for tracking, and Apple's App Store policies prohibit fingerprinting.[56] On mobile devices, the Apple IDFA and its equivalent on Android, AAID, are already de facto standards used to identify people in programmatic advertising exchanges.[57] Regulation mandating the use of these unique identifiers simply codifies what is already a widespread practice.

That said, some digital advertisers have been pushing the envelope in terms of developing and deploying new and invasive tracking methods.[58] Mandating that only unique identifiers from platform APIs be used for tracking purposes transforms an unwinnable technical arms race against highly motivated advertisers into a more tractable human accountability problem. Currently, there is no law constraining the unique identifiers used by digital advertisers, so long as advertisers' practices are disclosed. Breaking the arms race properly situates the most aggressive forms of tracking and the businesses that employ them as legally risky outliers.

While the major mobile operating systems, and to some extent major desktop operating systems, have adopted APIs to dole out tracking identifiers, the major web browsers have not adopted a similar API for the JavaScript Document Object Model, despite prior standardization efforts at the W3C.[59] This is a significant problem, as the Web is both

---

55. *See, e.g.*, Tony Romm, *'There's Going to be a Fight Here to Weaken It': Inside the Lobbying War Over California's Landmark Privacy Law*, WASH. POST (Feb. 8, 2019, 5:20 PM), https://www.washingtonpost.com/technology/2019/02/08/theres-going-be-fight-here-weaken-it-inside-lobbying-war-over-californias-landmark-privacy-law [https://perma.cc/XC5H-3S5X] (describing lobbying by digital advertisers attempting to weaken the CCPA).

56. *User Data*, GOOGLE, https://support.google.com/googleplay/android-developer/answer/10144311 [https://perma.cc/Q9XJ-MLWA]; *User Privacy and Data Use*, APPLE, https://developer.apple.com/app-store/user-privacy-and-data-use [https://perma.cc/B6ZS-LYV5].

57. Bennet Cyphers, *How to Disable Ad ID Tracking on iOS and Android, and Why You Should Do It Now*, ELEC. FRONTIER FOUND. (May 11, 2022), https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now [https://perma.cc/3NJ7-452E].

58. *See, e.g.*, Samy Kamkar, *Evercookie*, http://samy.pl/evercookie [https://perma.cc/6QTV-H9L3]; Englehardt, *supra* note 30, at 1389–90 (2016); Muhammad Ahmad Bashir, Sajjad Arshad, Engin Kirda, William Robertson & Christo Wilson, *How Tracking Companies Circumvented Ad Blockers Using WebSockets*, PROC. INTERNET MEASUREMENT CONF. 471, 472–74 (2018).

59. *See DID Working Group*, https://www.w3.org/2019/did-wg [https://perma.cc/67RB-JGMV]; *Federated Identity Working Group*, W3C, https://www.w3.org/community/fed-id

(1) an important platform and (2) rife with shady tracking practices. Currently, browser developers like Mozilla, Apple, and Brave would justifiably resist including APIs for tracking identifiers, as this would offer no privacy benefits to users. Yet, if the use of these APIs were mandated, these APIs would become viable mechanisms for improving user privacy and facilitating data subject rights. Browser vendors could opt to make the unique identifiers from the underlying operating system available to websites. However, this is not ideal: a single unique identifier assigned by the operating system to the web browser application itself would be made available to all websites. Instead, a more granular implementation, where the web browser manages the creation of unique identifiers on a per-website basis by default to prevent cross-site tracking, would maximize the privacy benefits of these APIs.

III. MACHINE-READABLE AD DISCLOSURES

While the FTC has long required that ads include clear and conspicuous disclosures, digital advertisers have been observed to stretch and ignore the rules. For example, in 2020, Google rolled back a change to how search ads were displayed, which made ads effectively indistinguishable from organic search results.[60] Native advertising networks like Outbrain and Taboola — infamous purveyors of "chum boxes" full of salacious, click-bait ads — often label the sponsored content they purvey with ambiguous labels such as "you may like from the Web" or "from around the Web."[61] Lastly, studies that have examined the adoption of dark patterns have documented how digital advertisers incorporate sponsored content into apps and websites in a variety of ways that are not always transparent to users.[62]

Influencer sponsorships on social media are a particularly problematic area of digital advertising disclosure. While the FTC has penalized

---

[https://perma.cc/58DE-EA3N]; *WebID Community Group*, W3C, https://www.w3.org/community/webid [https://perma.cc/2ANM-YZUM].

60. Nick Statt, *Google is Backtracking on its Controversial Desktop Search Results Redesign*, VERGE (Jan. 24, 2020, 1:21 PM), https://www.theverge.com/2020/1/24/21080424/google-search-result-ads-desktop-favicon-redesign-backtrack-controversial-experiment [https://perma.cc/H2ZT-ZLUB].

61. Bashir et al., *supra* note 7, at 17, 20.

62. *See* Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba & Alberto Bacchelli, *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, PROC. 2020 CHI CONF. ON HUM. FACTORS COMPUTING SYS., Apr. 2020, at 5; Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog & Christo Wilson, *A Comparative Study of Dark Patterns Across Mobile and Web Modalities*, PROC. ACM ON HUM.-COMPUT. INTERACTION, Oct. 2021, at 13–16; Monica Kowalczyk, Johanna Gunawan, David Choffnes, Daniel J. Dubois, Woodrow Hartzog & Christo Wilson. *Understanding Dark Patterns in Home IoT Devices* PROC. 2023 CHI CONF. ON HUM. FACTORS COMPUTING SYS., Apr. 2023, at 9.

companies for failing to disclose promotion on social media,[63] these failures remain widespread.[64] Major platforms typically have policies mandating that influencers disclose sponsorships, but the mechanisms for disclosure vary widely. YouTube, for example, mandates that content creators self-identify videos as being sponsored by checking a box, and then YouTube inserts a disclosure into the video every time it is played.[65] Instagram also allows creators to tag content as sponsored — in which case Instagram displays a label next to the content when it is viewed — but also permits creators to self-identify sponsorship within their content.[66] In the latter case, this lack of uniformity in how disclosures are presented to users may lead to confusion, as well as permit unscrupulous influencers to bury disclosures in ways that arguably obey the letter but not the spirit of the law.

Digital advertising disclosure goes beyond the simple fact of whether something is sponsored or not. Disclosure impacts how people are expected to interact with this content. Many digital advertisers implement the Ad Choices standard, which requires advertisers to display a triangular "i" icon in the upper right-hand corner of their banner ads.[67] The idea behind this standard is that people may click the Ad Choices icon to learn more about how digital ads are targeted online and engage the ability to opt out of further targeted ads.[68] While the Ad Choices standard is better than nothing, the icon is so small as to be nearly invisible. Further, on the off chance a person does notice the icon, it is not clear how they will understand that the icon links to information and choices about digital ads in general, as opposed to taking them to the specific advertiser's website.

In summary, I argue that the lack of uniform and usable digital ad disclosures facilitates a variety of problematic outcomes: it breeds confusion among users about how to identify digital ads and sponsored content across a wide variety of contexts; it allows advertisers to downplay their own transparency and control tools; and it creates space for unscrupulous advertisers and influencers to avoid disclosing sponsorship at all.

---

63. *See, e.g.*, Order, Lord & Taylor, LLC, FTC Docket No. C-4576 (May 20, 2016), https://www.ftc.gov/system/files/documents/cases/160523lordtaylordo.pdf [https://perma.cc/3J94-B238].

64. *Cf.* Mathur et al., *supra* note 8, at 20 (describing how the FTC's enforcement guidelines do not appear effective).

65. *See Add Paid Product Placements, Sponsorships & Endorsements*, GOOGLE, https://support.google.com/youtube/answer/154235 [https://perma.cc/93H2-VXHE].

66. *See* Instagram Business Team, *Deconstructing Disclosures: Do Creators Need To Say When They're Getting Paid?*, META (Nov. 24, 2020), https://business.instagram.com/blog/deconstructing-disclosures-do-creators-need-to-say-when-theyre-getting-paid [https://perma.cc/V3YS-N2NK].

67. *See* YOURADCHOICES, https://youradchoices.com [https://perma.cc/F9G7-EDX2].

68. *See id.*

One potential solution to these problems is to define a technical standard for machine-readable sponsored content disclosures, coupled with a mandate that digital advertisers adopt this standard. For example, imagine that all digital ads and sponsored content on websites were required to carry an <ad> HTML tag,[69] or something roughly equivalent. As I will discuss, many platforms (e.g., web browsers and operating systems) already require that user interfaces be expressed in a structured markup language (e.g., HTML or a specific flavor of XML), meaning that platforms already permit the inclusion of new tags and attributes in a way that is backwards-compatible. Platforms could insert highly noticeable and uniform disclosures around sponsored content (e.g., visual or auditory indicators) as well as provide prominent links to transparency and preference management tools.

Two major items would be needed to realize this vision for machine-readable sponsored content disclosures:

(1) Law or regulation mandating that sponsored content include a machine-readable disclosure in contexts where the sponsored content is being displayed on a platform that supports the associated technical standard.

(2) Modifying platforms — specifically, web browsers and operating systems — to understand and act on the standardized machine-readable disclosures.

Item (1) simply extends the FTC's existing ad disclosure guidelines, which are designed for people, to the realm of computer-mediated digital communication. Lawmakers or regulators will need to update existing disclosure guidelines to incorporate the new, machine-readable disclosure. Achieving item (2) will require obtaining buy-in from a variety of stakeholders, such as web browser developers, web standards bodies like the W3C, and operating system vendors. However, if the technical standards are developed carefully, these new disclosure tags should have no effect on older versions of platforms that have not been updated to understand the new standard. (I discuss backward compatibility in detail below.) The natural upgrade process of consumer technology ensures that most people will eventually use a platform — i.e., a new smartphone, a new desktop computer, an updated web browser, etc. — that supports the machine-readable disclosure standards.

Next, I discuss one potential approach to increasing control and transparency for digital ads based on existing ad blocking technology

69. HTML webpages contain content and structural metadata. The latter describes what kind of content is present in the webpage. HTML "tags" are how structural metadata is encoded in webpages. Examples of existing tags include <img>, which embeds an image in a webpage, and <a>, which denotes an anchor (more commonly known as a hyperlink).

and explain why this approach is insufficient. I also provide more details about the benefits and challenges of my proposed <ad> tag.

A. Ad Blockers Do Not Solve the Disclosure Problem

There are a variety of ad blocking tools[70] — typically implemented as web browser extensions or specialized apps on iOS — that attempt to prevent devices from downloading or displaying digital ads. Since ad blockers already have the capability to identify many digital ads, one could imagine repurposing this infrastructure for transparency (i.e., adding additional disclosures to digital ads rather than blocking ads altogether).

While repurposing ad blockers appears to be a tempting solution to the problem of insufficient digital ad disclosures, this approach is insufficient and unworkable for several reasons. The first major problem stems from how ad blockers identify digital ads — by observing network requests being sent to digital advertisers that appear on lists that are curated by crowdsourced volunteers.[71] However, these lists are neither comprehensive nor granular enough to identify individual pieces of sponsored content on social media services. Additionally, digital advertisers adopt anti-ad-blocking techniques to try to circumvent these technologies,[72] which reduces their effectiveness.

Researchers have begun to develop more sophisticated approaches to ad blocking that rely on perception and machine learning.[73] Machine

---

70. *See, e.g.*, *Privacy Badger*, ELEC. FRONTIER FOUND., https://privacybadger.org [https://perma.cc/TAL3-99G4]; ADBLOCK, https://getadblock.com/en/iOS [https://perma.cc/5ZDQ-72CV].

71. *See* Mshabab Alrizah, Sencun Zhu, Xinyu Xing & Gang Wang, *Errors, Misunderstandings, and Attacks: Analyzing the Crowdsourcing Process of Ad-Blocking Systems*, PROC. 2019 ACM INTERNET MEASUREMENT CONF. 230, 230 (2019); Saad Sajid Hashmi, Muhammad Ikram & Mohamed Ali Kaafar, *A Longitudinal Analysis of Online Ad-Blocking Blacklists*, 2019 IEEE 44TH LCN SYMP. ON EMERGING TOPICS IN NETWORKING, Oct. 2019, at 2; Peter Snyder, Antoine Vastel & Ben Livshits, *Who Filters the Filters: Understanding the Growth, Usefulness and Efficiency of Crowdsourced Ad Blocking*, 4(2) PROC. ACM ON MEASUREMENT & ANALYSIS COMPUT. SYST., June 2020, at 1.

72. *See generally* Rishab Nithyanand, Sheharbano Khattak, Mobin Javed, Narseo Vallina-Rodriguez, Marjan Falahrastegar, Julia E. Powles et al., *Adblocking and Counter-Blocking: A Slice of the Arms Race*, PROC. 6TH USENIX WORKSHOP ON FREE & OPEN COMMC'NS ON INTERNET at 1; Muhammad Haris Mughees, Zhiyun Qian & Zubair Shafiq, *Detecting Anti Ad-Blockers in the Wild*, PROC. ON PRIV. ENHANCING TECHS., July 2017, at 1–2; Kiran Garimella, Orestis Kostakis & Michael Mathioudakis, *Ad-Blocking: A Study on Performance, Privacy and Counter-Measures*, PROC. 2017 ACM WEB SCI. CONF., June 2017, at 2.

73. Grant Storey, Dillon Reisman, Jonathan Mayer & Arvind Narayanan, *The Future of Ad Blocking: An Analytical Framework and New Techniques*, at 2, 5, https://arxiv.org/pdf/1705.08568.pdf [https://perma.cc/TE46-6YAD]; Zainul Abi Din, Panagiotis Tigas, Samuel T. King & Benjamin Livshits, *PERCIVAL: Making In-Browser Perceptual Ad Blocking Practical with Deep Learning*, PROC. USENIX ANN. TECH. CONF. 387, 387 (2020).

learning is no panacea, however, as techniques to avoid these newer systems have also been developed.[74]

Focusing on the cat-and-mouse game between ad blockers and anti-ad-blockers misses the forest for the trees: the onus of properly disclosing ads should be on advertisers and digital advertising intermediaries. Solutions that center around communities building and maintaining countermeasure technology, as well as on individual users adopting these countermeasures, place all of the burden that should be borne by advertisers onto users.

B. The <ad> Tag

My proposal is straightforward: we should embrace technology by requiring that digital ads and sponsored content include a machine-readable label. Digital ads and sponsored content on the Web are served in HTML format (ads in apps are also typically served as HTML and displayed in an embedded web view). Thus, I colloquially refer to my proposal as an <ad> tag. Modern operating systems like Windows, Android, and iOS give app developers the option to specify their user interfaces in structured markup languages (e.g., flavors of XML),[75] so my tag operationalization also applies to these platforms. Many contemporary "desktop" apps are just repackaged web applications (e.g., Progressive Web Apps or websites encapsulated inside a framework like Electron),[76] which further extends the applicability of my concept.

My proposed machine-readable advertising label does not necessarily need to be implemented as an HTML or XML tag. Other potential approaches include a standardized HTML or XML attribute (e.g., " ") or Cascading Style Sheet class name (e.g., " "), although the latter may cause incompatibilities with existing software. Regardless of the specific implementation, developers would need to apply the machine-readable advertising label to user interface elements that surround each ad within the user interface. This rule would apply whether ads were displayed in line with other, non-sponsored content (e.g., banner or native ads) or apart from non-sponsored content (e.g., pop-up ads).

Mandatory, machine-readable ad disclosures would bring a variety of benefits to users. Software running on the client could visually highlight digital ads and sponsored content in a uniform way (e.g., by

74. *See* Florian Tramèr, Pascal Dupré, Gili Rusak, Giancarlo Pellegrino & Dan Boneh, *AdVersarial: Perceptual Ad Blocking Meets Adversarial Machine Learning*, PROC. 2019 ACM SIGSAC CONF. ON COMPUT. & COMMC'NS SEC., Nov. 2019, at 2, 13 (2019).

75. *See, e.g.*, *Develop a UI with Views*, GOOGLE, https://developer.android.com/studio/write/layout-editor [https://perma.cc/8LQH-3AGJ].

76. Marcin Dryka & Olga Gierszal, *7 Famous Electron App Examples [2023]*, BRAINHUB, https://brainhub.eu/library/electron-app-examples [https://perma.cc/2KMU-MN7A].

adding prominent, human-readable labels, changing the background color of ads, or putting a distinct border around ads to visually distinguish them from other user interface elements). The client software could enable users to customize these visual indicators. An <ad> tag would also bring accessibility benefits by enabling client software to communicate the presence of ads in non-visual ways (e.g., through audio prompts). Client software could also warn people when they were interacting with ads or sponsored content (e.g., by popping up an interstitial dialog when a person clicks or taps on an ad). And if users really wanted to, they could configure their client software to hide ads entirely or permit them in specific contexts.

A key aspect of my machine-readable disclosures proposal concerns who is responsible for compliance and how they should comply. First, advertisers and content creators would be responsible for disclosing the existence of paid promotion to the intermediaries that show their content to people. In some cases, this communication is implied (e.g., when a small business uploads an ad to Google or Meta's advertising tools). In other cases, this communication will need to be explicit (e.g., when an influencer uploads a sponsored video to YouTube or TikTok, they will need to communicate the fact of paid promotion to the platform). Second, the intermediaries would be responsible for including the <ad> tag around digital ads or sponsored content that they present to users. For example, it would be Google's responsibility to wrap ads on Google Search with the <ad> tag, not the individual advertisers' responsibility. YouTube would need to wrap sponsored videos and video ads with the <ad> tag. Desktop or mobile apps would need to wrap the space where banner ads are included in their user interface with the <ad> tag.

This division of responsibility is crucial, as the intermediaries who display digital ads and sponsored content are in the best position — the only position in some cases — to ensure that the <ad> tag is correctly and consistently applied to content. This is similar to how traditional publishers, like newspapers and magazines, will put small "sponsored" or "paid" disclaimers near the borders of full-page ads. Some online publishers and digital advertising intermediaries engage in similar practices, such as putting the AdChoices icon on banner ads or watermarking all sponsored videos with a disclosure.

An <ad> tag would enhance competition and legal compliance in the digital advertising space. As it stands, there is a race to the bottom among publishers and digital advertising intermediaries with respect to digital ad disclosures. This behavior makes sense, given that there is a strong economic incentive to increase clicks on sponsored content by obfuscating the content's true nature. An <ad> tag levels the playing field across all publishers and digital advertising intermediaries by completely removing the presentation of disclosures from their hands.

Publishers and digital advertising intermediaries are left with a binary choice: apply the <ad> tag appropriately and obey the law or fail to apply the <ad> tag and break the law. No longer is there a gray area where publishers and digital advertising intermediaries compete to reduce the effectiveness of ad disclosures and increase clicks on ads. Uniform disclosures may benefit ad buyers, as they may reduce the number of unintentional misclicks on their ads — low-quality clicks that advertisers often pay for but receive no benefit from.[77]

A significant challenge facing my proposal is motivating platform developers to add support for this technical standard to their client software. The simplest case is the Web, which does not strictly need the involvement of web browser developers. Rather, support for an <ad> tag could be immediately added to all major browsers via a browser extension. Eventually, if usage of the <ad> tag became ubiquitous, browser developers might be sufficiently motivated to add support for the tag to the browser core itself.

Garnering support for the technical standard in desktop and mobile apps is more challenging. Operating systems are responsible for rendering the user interface of apps. For example, apps communicating the <ad> tag to operating systems could take action by respecting user preferences for ad presentation. A privacy-conscious operating system developer like Apple might be willing to modify iOS and OSX to act on <ad> tags and offer users options for customizing how and when ads are presented. Other operating system developers — like Microsoft and Google, who also happen to run major ad networks — may be less forthcoming. As their operating systems are not easily extensible like web browsers, they could attempt to neuter the <ad> tag standard simply by ignoring it. For the <ad> tag standard to succeed, lawmakers and regulators would need to be willing to press major operating system developers to comply with the standard in good faith.

A secondary technical issue with my proposal is backward compatibility: what happens when an old web browser encounters a web page with the <ad> tag, or an old smartphone executes a new app that includes the <ad> tag? I do not foresee this being a significant issue in practice. Web developers routinely release web pages with incorrect HTML tags, so web browsers are designed to be resilient[78] — they simply ignore tags they do not understand. On platforms that are more sensitive to the correctness of tags, the machine-readable disclosures could be placed in XML attributes, which are permissive of arbitrary, developer-defined data.

---

77. *See* Andrey Simonov & Shawndra Hill, *Competitive Advertising on Brand Search: Traffic Stealing and Click Quality*, 40 MKTG. SCI. 923, 924–25 (2021).

78. *Cf. Tools and Testing*, MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Tools_and_testing [https://perma.cc/63GM-ETR8].

The language of a law mandating use of the <ad> tag would need to be carefully crafted to exclude contexts where machine-readable disclosures are impossible or the affordances of disclosure are not obvious. For example, it is not immediately clear how machine-readable ad disclosures would be implemented for podcasts: would they be embedded directly into the audio stream, or communicated via metadata? Another complex case is video games. There is no standard for how video games are rendered, so it is not clear how to mandate a specific structure for machine-readable disclosures, or how such disclosures would be presented in real-time environments in video games. That said, the existence of scenarios where <ad> tags are not feasible does not detract from the many other scenarios where they would be feasible and useful.

IV. CONCLUSION

The digital advertising marketplace is enormous, growing, and integral to many businesses. There are many justified criticisms of the industry, and reform is desperately needed. Nonetheless, digital advertising is here to stay for the foreseeable future. Digital ads are not going anywhere, and neither is the need for tracking data that underlies ad targeting, rate limiting, conversion measurement, and other processes that the industry views as sacrosanct.

I argue that the failure to grapple with this reality has led to attempts at reform that miss the mark. Beneficial as the GDPR has been, its lack of accompanying technical standards has permitted a range of bad practices to flourish.[79] The digital advertising industry's own attempts at self-regulation have also been lackluster. For example, Google's Privacy Sandbox initiative is moving at a glacial pace,[80] and current evidence suggests that the results may not improve people's privacy at all.[81] Even if Privacy Sandbox is eventually rolled out, digital advertisers are already adopting privacy-violating and non-transparent workarounds, like UID 2.0 and greater reliance on fingerprinting.[82]

In contrast to existing governance efforts, I argue that systemic governance — a convergence of complementary technical and legal standards — is a viable approach for achieving lasting reform of digital

79. Matte et al., *supra* note 12, at 2; *see* Cristiana Santos, Nataliia Bielova & Célestin Matte, *Are Cookie Banners Indeed Compliant with the Law?*, TECH. & REGUL. 91, 91–92 (2020).

80. *See generally The Privacy Sandbox Timeline for the Web*, PRIV. SANDBOX, https://privacysandbox.com/open-web/#the-privacy-sandbox-timeline [https://perma.cc/VP5M-77LQ].

81. Alex Berke & Dan Calacci, *Privacy Limitations of Interest-Based Advertising on The Web: A Post-Mortem Empirical Analysis of Google's FLoC*, PROC. 2022 ACM SIGSAC CONF. ON COMPUT. & COMMC'NS SEC. 337, 342 (2022).

82. Ronan Shields, *How to Pick an Identifier to Navigate the Ad Industry's Cookieless Future*, DIGIDAY (Jan. 12, 2023), https://digiday.com/media-buying/how-to-pick-an-identifier-to-navigate-the-ad-industrys-cookieless-future [https://perma.cc/RE4R-MUAZ].

advertising practices. This approach can be roughly summarized as follows: identify a concrete problem faced by people due to current digital advertising practices, develop a user-centered technical standard that addresses the issue or precludes the problematic behavior, and then mandate that the technical standard be followed. I rely on the ability of software platforms (e.g., web browsers and operating systems) to offer user-facing tools and intermediate interactions with client software (e.g., web pages and apps) as a fulcrum for deploying these complementary technical and legal standards. Through two case studies, I demonstrate how this approach could solve real-world problems without requiring deeply complex and brittle technical standards or complex legal language.

The ideas I present in these case studies are pro-competition, in that they level the playing field between all participants in the digital advertising space. In the current landscape, digital advertisers willing to adopt aggressive tactics may outcompete digital advertisers who voluntarily adopt robust privacy safeguards and prominent disclosures, creating a race-to-the-bottom. Establishing standards and mandating their use creates conditions where compliance can be rapidly and automatically assessed at scale, heavily penalizing dissenting digital advertisers.

The technical and regulatory interventions I propose here do not and cannot solve all the myriad problems that plague digital advertising. Rather than proposing a comprehensive solution, my aim is to motivate systemic governance as an approach to navigating sociotechnical challenges, and to demonstrate how we may be able to make substantive, incremental progress towards a more private and more transparent digital advertising ecosystem in the short term.

Neither standard is an ironclad technical solution: lazy or malicious digital advertisers may still attempt to use contraband identifiers to track people or fail to label ads properly. However, a world in which these interventions exist is no worse than the world today. In the best case, these proposals would bring increased privacy, transparency around ads and collected data, and more direct access to recourse if tracking or ad labeling standards are violated.

Another challenge is pernicious behavior by platform owners. If APIs for unique tracking identifiers were imbued with legal power, there might be an incentive for conflicted platform owners to defect. For example, Apple has made strong commitments to privacy and might welcome the ability to police apps on their platforms with stricter rules. However, Google might balk: they could respond by removing the tracking identifier APIs from Android entirely, freeing digital advertisers to track with impunity since the platform would no longer contain the prerequisite capabilities.

Similar issues exist with respect to machine-readable ad labels. The Web is fundamentally open source, so there would be no way to unilaterally prevent web browsers from checking ad labels in web pages. But on desktop and mobile, operating systems would need to be modified to surface ad labels in apps to users. Of course, Microsoft and Google could simply refuse to build this functionality, effectively dooming the ad labels to obscurity. Lawmakers and regulators could solve this issue by demanding that major platforms incorporate substantive support for ad labels, but this would be a much more complex — and likely litigious — problem than mandating that advertisers label their ads in the first place.

The technical standards I propose will be dead on arrival if they are not backed up by legal mandates. The most robust path forward would be legislative, possibly at the state level to avoid congressional gridlock (although this would potentially constrain their real-world impact). It is also possible that a regulator like the FTC could attempt to mandate these standards, as they already do with other facets of advertising like human-readable disclosures.