new media & society
1–22

DOI: 10.1177/14614448231213267
journals.sagepub.com/home/nms

Keywords
Adtech, contextual integrity, critical data studies, digital advertising, online tracking, platforms, privacy, surveillance

Introduction

Business models based on surveillance and permissive information flows face intensifying scrutiny from regulators, policymakers, and civil society groups (e.g. Federal Trade Commission (FTC), 2022; Mizarhi-Borohovich et al., 2023; Veale and Borgesius, 2022). Platform companies like Google, Meta, and Apple now promise that privacy will be a central design value in the reconstruction of online advertising (Apple, 2021; Bindra, 2021; Mudd, 2021). This sounds like news worth celebrating, turning the page on the personal-data free-for-all that accompanied the rise of advertising technology, or "adtech" (Crain, 2021; Turow, 2011; Zuboff, 2019). We should hold our applause, however, until we know what "privacy" means to these companies, and how those definitions may be inadequate and/or productive of self-advantageous relationships (Greene and Shilton, 2018; Kollnig et al., 2022; Scharlach et al., 2023).

This study assesses adtech's reformist rhetoric by examining proposals for "privacy-preserving" advertising attribution. Attribution is a process for measuring advertising effects by matching information about users' media and marketplace activities (Smith, 2019). It requires intermediaries to produce and join records of advertising exposure or engagement, on one hand, and subsequent purchases or other valued actions (e.g. app downloads), on the other. Attribution essentially assigns credit for marketing outcomes to specific advertising efforts; it thereby lets advertisers and their agencies determine and possibly improve their return on investment (ROI), and, in some cases, it allows revenue to be allocated to the publishers, apps, and intermediaries deemed responsible for "causing" certain consumer behaviors. Because its mechanics rely on persistent surveillance, advertising attribution has empowered companies that are well-positioned to monitor users at multiple touchpoints—such as Google, Meta, and, increasingly, Apple—and it the adtech sector conceptualizes privacy “problems” in general, and how the specific “solutions” promised by these companies reflect aspects of their reputations, market positions, and infrastructural or platform power.

Our study discerns and compares the meanings and mechanisms of privacy conveyed in these attribution proposals. This sort of clarification is of urgent importance. Regulators and policymakers around the world are seeking to codify privacy in digitally-mediated environments (e.g. European Commission, 2022; FTC, 2022); meanwhile, adtech companies are appropriating the term in public relations and using their dominant positions to encode strategic definitions of privacy into information and market infrastructures (Veale, 2022). New proposals for ad attribution services are political instruments that stake out the legitimate boundaries of privacy, surveillance, datafication, and corporate power. This is a critical moment to clarify the meanings, contradictions, influencing forces, and implications of “privacy-preserving” adtech.

Based on a critical discourse analysis of their attribution proposals, we argue that Google, Meta/Mozilla, and Apple are each promising reforms that leverage (1) long-standing but limited definitions of privacy and (2) elaborate but techno-solutionist computational mechanisms. Addressing multiple audiences in a vaguely technical idiom, these proposals frame a discursive space where each company’s solution can do the work of legitimizing corporate data governance and platform-imposed “privacy.” They make sense by inviting the policymakers and other publics interested in these documents to picture the world in terms of security threat models, individual harms, and the “creepy” indignities associated with furtive tracking and profiling. While these initiatives may make progress on some real problems, they fail to contend with the broader ecosystems of surveillance and data capitalism. They may also further normalize dubious information flows, dismissing the possibility that attribution’s features, to say nothing of its bugs, raise privacy (and other) problems that are not eradicated by technical fixes.

Building on the latter point, we consider how the very notion of privacy-preserving attribution implies an extension of economic priorities and platform power within the mediation of social life. These proposals assume that the use of PETs is sufficient to justify information flows that combine media and market behaviors. We contend, by contrast, that the legitimization of attribution reflects an effort to shift the expectations surrounding ad-supported media: from an arrangement wherein advertisers are entitled to measure audience attention at the site of media exposure, to one wherein advertisers get to measure advertising effects by observing both the site of media exposure and the sites of subsequent consumer behavior. Adtech companies may feel compelled to impress with cryptographic techniques and self-regulatory promises because a definition of privacy rooted in social relations could invalidate the entire enterprise of attribution.

“Privacy-preserving” attribution: background and literature review

Adtech, surveillance, data capitalism

Digital economies depend on forms of data processing and analytics that create well-documented tensions with privacy, as well as related concerns about discrimination and corporate and state power (Binns, 2022; Gandy, 2021; McNealy, 2022; West, 2019). Proponents of data capitalism, by contrast, argue that privacy impedes the social and among the professionals using these measures. Nevertheless, the goal of attributing consumer behaviors to advertising events has motivated organizational and infrastructural investments in surveillance, data processing, and data sharing (McGuigan, 2023).

It follows that attribution raises privacy concerns. Mozilla even admits that “current attribution practices have terrible privacy properties” (Thomson, 2022). Companies now seek to maintain existing capabilities, which are still in demand, while complying with new rules and norms. We contend that attribution provides an interesting case study for examining the advertising industry’s privacy rhetoric. Attribution is a key functionality provided by adtech vendors, yet it has been understudied in critical literature on marketing, surveillance, and privacy (for an exception, see Smith, 2019). It is also particularly well-suited to an analysis informed by a theory of privacy as “contextual integrity” (CI) (Nissenbaum, 2009), since attribution requires the collection and matching of data gener ated across multiple sites of user behavior. Attribution’s core function is to join records created when users encounter advertisements embedded in media content, with records created when users make purchases or download apps on other sites. In short, it requires data flows that encompass both media usage and marketplace behavior.

This raises a key dilemma: What definition(s) of privacy can be reconciled with attribution’s basic processes?

Meanings and mechanisms of privacy

The meaning of privacy is subject to ongoing debate (e.g. Citron and Solove, 2022), varying across legal, philosophical, and technical disciplines (Nissenbaum, 2009). Privacy definitions, and the mechanisms for operationalizing them, are situated within political-economic contexts; as such, they both reflect and shape dynamics of power that structure the experiences of designers, workers, and consumers who develop or interact with socio-technical systems (Greene and Shilton, 2018). The privacy discourses circulated through corporate documentation also help companies position themselves in relation to regulators and other stakeholders by aligning with desirable principles (Scharlach et al., 2023). Some principles have been especially influential at defining what privacy will mean in policy and practice (Cohen, 2013; Epstein et al., 2014). We highlight some perspectives identified by Nissenbaum (2009) as key frameworks for theorizing privacy.

Privacy protections predominantly rely on an “informed consent” model, which puts the onus on the user to comprehend the associated benefits and harms and adjust controls around what information to share, with whom, and for what purpose (Solove, 2013). This paradigm understands privacy as control over personal information, and its proponents push for greater transparency in disclosing information handling practices. The main focus within this approach is identifying different information categories and purposes, often through recourse to dichotomies such as private versus public, personal versus non-personal, and sensitive versus non-sensitive information.

Another dominant perspective defines privacy as limiting access to individuals’ data (Nissenbaum, 2009: 69–71). The basic idea is that privacy increases as the amount of information disclosed about an individual, or the number of parties privy to it, decreases. This notion of privacy is strongly coupled with security mechanisms such as encryption,

companies and smuggling these issues out of the realms of collective action, strong public governance, and political debates about values and power. These conceptual tools

The privacy meanings we coded were defined as follows:

Anonymity: Any effort to prevent information from being associated with an identifiable person. This includes the initial anonymization of personal data, as well as subsequent defenses against adversaries trying to deanonymize that data. Common mechanisms for achieving anonymity include aggregation, obfuscation, MPC, and differential privacy.

Limiting access: Any effort to limit the information collected, processed, shared, or revealed about an individual. This includes references to secrecy and confidentiality, and it corresponds to mechanisms such as encryption and on-device data processing. Access can be limited along two dimensions: the amount of information about a user that is accessible; and the number of parties able to access information about a user.

Preventing third-party tracking and profiling: These documents often define privacy inversely, by referencing privacy violations. We coded instances in which the companies claim that their solutions are privacy-preserving because they prevent third-party tracking and profiling. This anti-tracking category is, in fact, a subset of Limiting Access; but it focuses particularly on third-parties and appeals directly to popular anxieties about “creepy” surveillance by unknown companies. We deter mined that it is important to capture the tendency among adtech companies to claim the prevention of third-party tracking as a privacy trump card.

Control: The ability of users to control information about themselves. This is typically related to consent mechanisms that let users opt-out of or opt-into commercial data collection and usage.

privacy's normative content (i.e. why it is important), apart from implied benefits of information security. Privacy is also treated in a "descriptive" sense (see Nissenbaum, 2009: 68–69), as a property that these attribution solutions will "enhance," "increase," or "protect." Across these normative and descriptive claims, though, almost none of the proposals expressly defines what privacy means. Instead, privacy meanings are implicit and often vague, evoked through reference to practices that violate privacy (e.g. "tracking") or mechanisms that protect against privacy harms. Furthermore, although all three companies align themselves with privacy as a value, they suggest that the extent of privacy must be balanced against economic priorities (which are themselves justified through normative appeals—namely, that advertising is an essential guarantor of the open Internet).

We find that the solutions all converge primarily around definitions of privacy as anonymity, as limiting access to individuals' data, and as the prevention of third-party tracking and profiling. The following sections describe each attribution solution and the privacy meanings and mechanisms encoded therein.

Meta/Mozilla's Interoperable Private Attribution

Meta (then Facebook) signaled its intention to use PETs for more "private" measurement of ad effectiveness at least as early as 2021, and, together with Mozilla, it published an overview of the Interoperable Private Attribution (IPA) system in January of 2022. The proposed solution uses local identifiers called "write-only match keys" to link "source events," such as viewed impressions, with "target events," such as purchases or app installations, from the same user. Match keys are set on a user's device or browser by designated "providers," such as Facebook, Google, and Twitter, when users log in to those platforms or apps. Any participating website can use those match keys to associate what happens on their site with an individual user, but the identity of the match key is only readable by the local device or operating system. Upon leaving the device, event records are matched in a confidential way via a MPC arrangement involving double encryption-decryption by "trusted helper" servers. The purpose of MPC is to collectively process data about source and target events without letting any single party access or reconstruct the behavioral records associated with each user. Finally, the system produces aggregated attribution reports for advertisers and publishers. Access to the reports is limited by a "privacy budget," imposed on each interested party, that gets depleted as they ask for information. The privacy budget prevents anyone from repeatedly querying the servers that process individual information so as to disaggregate and deanonymize conversion reports. User identity is further masked using differential privacy, a technique which adds a calibrated amount of distortion to a dataset so that insights may be derived about a population while concealing each individual's data.

The dominant privacy meanings applied in the IPA documentation are anonymity and limiting access. A key privacy promise is that the identifiers used to measure each individual's activities across sites, apps, and devices—"write-only match keys"—are not readable by third-parties, and so they "cannot be used for tracking or profiling" (Savage et al., n.d.). The attribution reports are considered "private" because advertisers and adtech vendors see aggregate data and are unable to re-identify individuals.

Meta comes close to articulating an explicit definition of privacy as limiting access, but with some discrepancies that bear noting. Documents predating the IPA proposal discuss how PETs will minimize the amount of data that the company collects or processes. “Ensuring privacy throughout our apps while reducing the data we collect is a long-term effort,” one text explains. It later alludes to the sophistication of this class of privacy mechanisms and their ability to satisfy advertisers’ business demands: “PETs involve advanced techniques drawn from the fields of cryptography and statistics. These techniques help minimize the data that’s processed while preserving critical functionality like ad measurement and personalization” (Facebook, 2021).

This initial position stands in subtle but critical contrast to Meta’s eventual proposal (with Mozilla) for IPA, which offers perhaps the clearest definition of privacy in the whole corpus: “Our privacy goal is to limit the total amount of information IPA releases about an individual over a given period of time” (Taubeneck et al., 2022a; emphasis added). One of the key questions motivating the IPA design is: “How can we make sure fewer companies have access to our personal data?” (Savage et al., n.d.: 20).

Our findings thus document a shift from the promise of data minimization—reducing the amount of data collected and processed—to the promise of limiting the amount of data that is released or shared and the number of parties involved. This is a much more permissive approach to privacy than preventing personal data from being generated and stored in the first place. It sidesteps questions about the legitimacy of the information flow and instead purports to make that flow “more private” by limiting access.

Despite this hedge on data minimization, IPA is the most ambitious of the attribution solutions we examined. Compared with the others, Meta/Mozilla make the boldest privacy claims and propose the most demanding computational and cryptographic mechanisms. That said, this proposal is also the most prospective. Key details remain indefinite—such as whether or how data from attribution reports are fed back into the optimization of ad targeting, and who will operate the “trusted” servers. Since Meta/Mozilla begin one document by stating (as if a matter of fact), “Advertisers need accurate reporting about how their ad campaigns are performing” (Savage et al., n.d.: 3), we should expect tensions and compromises to arise as IPA enters the messy politics of implementation.

Google’s attribution reporting API

Google’s solution has been in use since 2021. The documentation and publicity sur rounding it also portray privacy mainly as limiting access and anonymity. Like IPA, Google’s Attribution Reporting API links source and target events while “minimizing” information sharing and adding noise to the produced reports. Implicit here is the notion that cross-context measurement (i.e. the joining of ad exposure or clicking events with conversion behaviors by a unique user) does not constitute tracking if it is executed locally on the user’s device or browser. “No cross-site identifier is used and no detailed cross-site browsing activity leaves the device,” Google explains. “A small amount of information is joined across sites—enough to measure conversions, but not enough to track [a user’s] activity across sites in detail” (Nalpas et al., 2023).

solution that promotes privacy as limiting access, linking source and target events locally, on users' browsers, up to 1 week from ad impression to conversion. Only the browser on the user's device can match source and target events to actual users, and that data, according to Apple, never leaves the local device. To ensure anonymity and confidentiality, the reports are encrypted and signed to prevent fraud, provided to both ad impression and conversion outlets, and are delayed by 24–48 hours to further obfuscate user identity (Apple, n.d.). Conversion destinations are only registered at the top-level domain to prevent tracking users through a chain of subdomains that can reveal information about the attribution source.

For "app-to-app" and "web-to-app" attribution, Apple deploys SKAdNetwork 4.0, a solution for measuring the impact of advertising on app downloads and engagement. Any click on an ad for an app generates a report that is stored locally; the report includes the unique IDs of the publisher, advertiser, and ad network involved and a "hierarchical id"—a 4-digit number that can include information on the campaign, approximate user location, and the type of ad served (Apple, 2021). Once the user engages with the app, the latter point, all solutions boast that they limit the information revealed about individuals through technical restrictions, but they do not acknowledge the flexibility– advertisers still have to specify characteristics for targeting on the “line-item” level. A line item is a string of taxonomic descriptors that an advertiser or demand-side platform uses to define certain features about the delivery and targeting of an ad campaign, such as publisher site, geography, demographic details, and creative content. It is possible that clever manipulation of line items will let advertisers evaluate ad performance in granular detail, regardless of the technical restrictions imposed through an attribution system. For example, Google Summary Reports allow advertisers to see conversion counts and campaign spending broken down by targeting categories. This privacy feature promises to protect users by only sharing campaign level IDs, rather than user IDs; however, by applying targeting categories at the line-item level before interacting with the platform, advertisers could potentially compromise de-identification efforts through permutations of line-item targeting. They could, in effect, turn the campaign ID into something that works more like a pseudonymous user or cohort ID.

At a broader level, platforms’ privacy perspectives appear to be inspired by cybersecurity threat models. Consequently, many of the touted features are designed to be robust against malicious activity. Implicit here is the claim that privacy violations are, almost by definition, associated with unsanctioned actions. Attribution, in and of itself, raises no concerns in this account, and the record-keeping required for attribution is justified by business needs. This orientation lends itself toward discrete (if highly creative) solutions, wherein privacy becomes an objective property that can be “increased” with cryptographic techniques. Preventing abuse is beneficial, of course; but coming to terms with adtech’s privacy problems requires a more holistic approach. Privacy is not just about preventing data breaches or identity theft. To be useful in thinking critically about soci-r/ions

It appears that the principle heuristic for defining appropriate information norms in adtech is the proximity relationship between parties (or, to put it another way, the owner ship of the sites where data extraction and usage occurs). In this formulation, a first-party relationship assures the integrity of a context, while a third-party relationship is a de facto violation. Surely, third-party tracking activates problematic information flows. But, the legitimacy of the information flows here called "measurement" is not secured simply by being conducted within a first-party relationship; per CI theory, that determination must be rooted in considerations of social values and purposes. Attention to the political economy of media, platforms, and data further enhances those considerations.

We suggest that the industry's treatment of "contexts" does important political work. The legitimization of attribution represents a silent extension of media marketization and the platform enclosure of social life (Wu and Taneja, 2021). The embedding of attribution processes in digital media effectively renegotiates the implied transaction between audiences, publishers, and advertisers: from an exchange based on attention, to one based on buying behavior. Attribution implies that marketers are not just entitled to measure "audience attention," to confirm that their ads are distributed properly; rather, marketers are entitled to measure the effects of advertisements, by following audiences beyond the sites of ad exposure and into the marketplaces where those audiences become active consumers. This is a corporate-imposed shift in relationships that requires scrutiny. For attribution to be "privacy-preserving," in the sense of comprising legitimate information flows, we would have to accept that media and marketplaces are coterminous—that a prevailing purpose of news, entertainment, and social media is to produce not just audiences but consumers. The industrial logic of commercial media in the United States has always centered around bona fide consumers (Meehan, 2005), but its implementation is a site of social struggle, as people resist commodification of their leisure time and attention (Smythe, 1981). Justification for this emergent attribution arrangement is not assured by techno-solutions that configure privacy as anonymity or limiting access, and its normalization should be considered part of the corporate cultivation of resignation to commercial surveillance (Draper and Turow, 2019; McGuigan et al., 2023). CI and CPE are useful analytics—and troublesome ones from adtech's perspective—because they demand an account of the assumption at the core of all these solutions: Why is the measurement of advertising effects, and the relationships necessary for joining media and marketplace data, integral to the socio-technical systems that mediate our social and personal lives and our access to news and culture? The rhetoric in the documents we analyzed does not answer this question. Accepting that attribution can be private requires an admission that the production of consumers deserves pride of place among the values and priorities commonly attached to media systems in a democracy (see, for example, Napoli, 2019; Pickard, 2019).

Conclusion

Google, Meta, and (to a lesser extent) Apple are advertising giants. They have benefited from perverse data collection practices for years. Their executives declared the death of privacy and invested heavily in data-extractive technologies and commercial relations. While we welcome initiatives to reverse this trend, our examination shows that what

“fixes” to the “privacy problem,” and it diverts attention toward the configuration of internal details rather than the values, social relations, and power dynamics congealed within adtech infrastructures. The frameworks of CI and CPE collectively force these issues into the open, making the purposes and priorities at the root of attribution systems into matters of concern and collective political action. By accepting these proposals on their own terms (however well-meaning their proponents may be), we risk further normalizing the platform enclosure of personal and population-level data and deepening ad-supported media’s highly contestable relations of commodification, discrimination, and exploitation. Challenging adtech’s privacy meanings is a critical step for denying platform companies’ claims of ownership over a privatized—but not privacy-preserving—digital sphere, where social mediation and cultural production are collapsed into an encompassing commercial context.

Limitations and future directions

There is much more to know, and our study has limitations. Some of the texts in our corpus are fairly technical. They are also quite vague, both in that they are written for developers who may be implementing these systems across different software configurations and use cases, and in that some elements of these systems remain prospective or experimental. We tried to compensate by assembling an interdisciplinary research team

Gehl RW (2014) Reverse Engineering Social Media: Software, Culture, and Political Economy in New Media Capitalism. Philadelphia, PA: Temple University Press.

Gillespie T (2010) The politics of “platforms.” New Media & Society 12(3): 347–364.

Graham M (2022) More changes loom for online marketers. Wall Street Journal, 25 January. Available at: https://www.wsj.com/articles/more-changes-loom-for-online-marketers-11643150679

Greene D and Shilton K (2018) Platform privacies: governance, collaboration, and the different meanings of “privacy” in iOS and Android development. New Media & Society 20(4): 1640–1657.

Haggerty KD and Ericson RV (2000) The surveillant assemblage. The British Journal of Sociology 51(4): 605–622.

Hercher J (2022) Mozilla and meta submit (yet another) privacy ad tech proposal in new W3C group. AdExchanger. Available at: https://www.adexchanger.com/online-advertising/mozilla-and-facebook-submit-yet-another-privacy-ad-tech-proposal-to-new-w3c-group/

Hwang T (2020) Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet. New York: FSG/Logic.

Kak A and West SM (2023) AI now 2023 landscape: confronting tech power. AI Now Institute, 11 April. Available at: https://ainowinstitute.org/2023-landscape

Kollnig K, Shuba A, Van Kleek M, et al. (2022) Goodbye tracking? Impact of iOS app tracking transparency and privacy labels. In: ACM conference on fairness, accountability, and transparency, Seoul, Republic of Korea, 21–24 June, pp. 508–520. New York: ACM.

MacKenzie D (2021) Cookies, pixels and fingerprints. London Review of Books, 1 April. Available at: https://www.lrb.co.uk/the-paper/v43/n07/donald-mackenzie/cookies-pixels-and-fingerprints

Maréchal N (2018) Targeted advertising is ruining the internet and breaking the world. Motherboard,16 November. Available at: https://www.vice.com/en/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world

, 1 April. Availab20 Januar2/.k/ts 2 -51.222 337 Internet

Napoli PM (2019) Social Media and the Public Interest. New York: Columbia University Press.

Nieborg DB and Poell T (2018) The platformization of cultural production: theorizing the contingent cultural commodity. New Media & Society 20(11): 4275–4292.

Nissenbaum H (2009) Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press.

Pickard V (2019) Democracy Without Journalism? Confronting the Misinformation Society. New York: Oxford University Press.

Savage B, Taubeneck E and Thomson M (n.d.) A non-technical introduction to Interoperable Private Attribution (IPA). Available at: https://docs.google.com/presentation/d/1NpQz0Wm73eEKw24V7B0yCjq4Tw2qPgeezhMfS0-P-TY/edit#slide=id.gf172a1733b_0_251

Scharlach R, Hallinan B and Shifman L (2023) Governing principles: articulating values in social media platform policies. New Media & Society. Epub ahead of print 7 March. DOI:

Author biographies

Lee McGuigan is an Assistant Professor in the Hussman School of Journalism and Media at the University of North Carolina at Chapel Hill. He is the author of Selling the American People: Advertising, Optimization, and the Origins of Adtech (MIT Press, 2023).

Ido Sivan-Sevilla is an Assistant Professor of information studies at the University Maryland, where he bridges computer science and public policy by developing measurements and theories of policy implementation across a range of cybersecurity, privacy, and machine learning issues.

Patrick Parham is a Ph.D. student at the College of Information Studies, University of Maryland. He has been studying advertising and media technology, and proposals addressing the deprecation of third-party cookies. Patrick previously worked in the programmatic advertising industry.

Yan Shvartzshnaider is an Assistant Professor and the director of the Privacy Rhythm research lab in the Department of Electrical Engineering and Computer Science, Lassonde School of Engineering at York University. His research focuses on sociotechnical systems that incorporate a socially meaningful conception of privacy which meets peoples' expectations and is ethically defensible. His work addresses the fundamental mismatch between programmable privacy frameworks and the ever-shifting privacy expectations of computer system users.