Framing Privacy: Analysing Technology Giants' Shaping of Privacy Discourse

Ine van Zeeland

Privacy Studies Journal
ISSN: 2794-3941

Vol. 4 (2025)

Abstract
This position paper argues that more attention should be accorded to analysing the discursive practices around privacy by dominant technology actors. People necessarily have different perspectives on what they want to keep private, depending on personality characteristics, who they are in which society, and where they stand in time. However, the infrastructure of the digital environment leaves little space for different perspectives, and frames privacy to suit the interests of the infrastructure provider. This paper argues for an analysis of the practices of such dominant actors as discursive practices: the communication about privacy by infrastructure providers is the social reality of privacy within their environments. The paper presents an example analysis of the discursive practices that make up Apple's App Tracking Transparency Framework. The position it argues is that bringing discursive practices to light is necessary to envision alternative approaches that respect different perspectives on privacy.

Keywords
Discursive practices – privacy – framing – social reality – consent

Introduction

The concept of privacy is infamously difficult to define, yet, as a topic it is increasingly discussed in our digitalizing societies. Privacy has been laid down as a human right in legislation around the world, but it means different things to different people.[1] Privacy protection can cover a variety of things people wish to keep private, from (parts of) their bodies to their correspondence, or the autonomy of their decision-making, with some jurisdictions making a sharp distinction between the right to a private life and the right to the protection of personal data.[2] The question is which interpretations are used for privacy protection in practice.[3]

In the battle of privacy interpretations, some control the field, while others must band together to stand a chance. The aim of this paper is not to provide a definitive answer to what should be understood as privacy, but instead to argue for the analysis of strategies by powerful players to push forward their interpretations of privacy. To that end, a strategy by a powerful entity is analysed, by way of an example, describing how to analyse its discursive practices. Foucault's concept of "discursive practices" originally referred to the production of knowledge through contingent practices.[4] It is used here to refer to practices that produce a specific knowledge within a social reality; in this case, Apple's (material and symbolic) discourse on privacy within its App Store platform.

Apple Inc. is one of the so-called Big Five global technology companies and designated a gatekeeper platform by the European Commission. The company presents itself as a privacy advocate, but how does it interpret privacy in its practices? To illustrate the salience of discursive practice analysis, this paper will dissect Apple's production of privacy within its App Tracking Transparency Framework. The analysis will shed a light on what purpose Apple has in establishing both the practical meaning of privacy and a social reality in which the responsibility for its protection lies with the platform users rather than the platform provider, even while the latter claims the award of privacy champion.

1 Patricia Brierley Newell, "Perspectives on Privacy," *Journal of Environmental Psychology* 15 (1995): 87–104; Daniel J. Solove, "Conceptualizing Privacy," *California Law Review* 90, no. 4 (2002): 1087–1156.

2 Irwin Altman, "Privacy. A Conceptual Analysis," *Environment and Behavior* 8, no. 1 (March 1, 1976): 7–29, https://doi.org/10.1177/001391657600800102; Bert-Jaap Koops et al., "A Typology of Privacy," *University of Pennsylvania Journal of International Law* 38, no. 2 (September 18, 2017); Beate Roessler, "Three Dimensions of Privacy," in *The Handbook of Privacy Studies: An Interdisciplinary Introduction,* ed. Bart Sloot and Aviva Groot (Amsterdam University Press, 2018), 137–41, https://doi.org/10.5117/9789462988095; Bart Van der Sloot, "Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data,'" *Utrecht Journal of International and European Law 31*, no. 80 (February 27, 2015): 25–50, https://doi.org/10.5334/ujiel.cp.

3 Daniel Greene and Katie Shilton, "Platform Privacies: Governance, Collaboration, and the Different Meanings of 'Privacy' in iOS and Android Development," *New Media & Society* 20, no. 4 (2018): 1640–57; Deirdre K. Mulligan, Colin Koopman, and Nick Doty, "Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374, no. 2083 (December 28, 2016): 20160118, https://doi.org/10.1098/rsta.2016.0118.

4 Carol Bacchi and Jennifer Bonham, "Reclaiming Discursive Practices as an Analytic Focus: Political Implications," *Foucault Studies*, (April 30, 2014): 179–92, https://doi.org/10.22439/fs.v0i17.4298.

This approach to discursive practice analysis follows in the footsteps of a specific strand within critical discourse analysis, based on Foucault's ideas about the use of language to exercise power and to enforce or reinforce a social reality. The analysis of discursive practices goes beyond a linguistic analysis, to focus on "the discursive effects of the material, and the material effects of the discursive".[5] It can be situated between framing analyses of political discourse and critical analyses within the fields of platform studies and infrastructure studies, in that it accords equal attention to the power effects of a certain use of terms and to material aspects.[6]

The purpose of analysing discursive practices is to expose hidden agendas and attempts at social control. From this critical perspective, presenting privacy – a contested concept *par excellence* – as a practical notion with clear boundaries, inherently suggests a hidden agenda. Bringing that agenda to light is a worthy academic as well as subversive endeavor in the pursuit of deeper understandings of power (infra)structures on the one hand, and the power of discourse on the other hand.

This position paper first briefly discusses why the concept of privacy is so difficult to pin down, and why it is particularly amenable to a discursive practice analysis in the digital age. The next section illustrates the analytical approach, with the case of Apple's App Tracking Transparency Framework. A discussion of the results of the analysis and the conclusion round off the thesis of this paper.

Background: Privacy and Power

Privacy theorists have long argued that privacy is a multi-faceted or multi-dimensional concept.[7] Consequently, definitions of privacy vary wildly, ranging from a focus on a human condition (e.g. being alone) or a location (e.g. a refuge) to an interaction (e.g. a lower tone of voice), or various other focal points.[8] The concept of privacy is affiliated and often conflated with the concepts of anonymity, secrecy, and solitude,[9] and connected with building intimacy.[10] Despite this variety in definitions, there is some overlap, par-

5 Derek Hook, *Foucault, Psychology and the Analytics of Power, Critical Theory and Practice in Psychology and the Human Sciences* (Palgrave Macmillan, 2007), 126, https://lanlib.alzahra.ac.ir/multiMediaFile/2231433-4-1.pdf.

6 Cynthia Hardy and Robyn Thomas, "Discourse in a Material World," *Journal of Management Studies* 52, no. 5 (2015): 680–96, https://doi.org/10.1111/joms.12113; Jean-Christophe Plantin et al., "Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook," *New Media & Society* 20, no. 1 (January 2018): 293–310, https://doi.org/10.1177/1461444816661553.

7 Anita L. Allen, "Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm," *Connecticut Law Review* 32, no. 3 (2000): 861–76; Altman, "Privacy. A Conceptual Analysis"; Helen Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review* 79, no. 1 (2004): 119–58; Roessler, "Three Dimensions of Privacy"; Solove, "Conceptualizing Privacy"; Alan F. Westin, *Privacy And Freedom* (Atheneum, 1967), https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr.

8 Newell, "Perspectives on Privacy."

9 Westin, *Privacy And Freedom*.

10 Jeffrey H. Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future," *Santa Clara High Technology Law Journal*, (January

ticularly in elements of setting boundaries related to the self.[11] Privacy can therefore be understood as a set of associated concepts with "family resemblances".[12]

Automation and digitalization efforts have shifted attention away from other privacy issues towards the protection of personal information.[13] In privacy definitions that focus on information, a core element is the notion of control,[14] for example in Westin's definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[15] In 1983, a judgment of the German Constitutional Court established a fundamental right to informational self-determination. This right should enable individuals to develop their personalities, interact with other members of society on an equal footing, and participate freely and without fear of prosecution in a democratic society.[16]

Privacy definitions focused on individual control are criticized for ignoring the public interest in privacy. An example of the public interest in privacy is the need in democratic societies for unmonitored spheres, for political opposition and for minorities to express themselves without majority scrutiny.[17] In this instrumental sense, the right to privacy also shields scholars, scientists, and the press from government interference.[18]

To protect both the individual right and the public interest in privacy, human rights declarations and treaties, and constitutional and specific legislation contain privacy provisions. Similar to the definitional variety, those legal provisions reflect different beliefs in societies regarding what should be protected as private.[19] Basic types of privacy protected by laws include bodily, intellectual, spatial, decisional, communicational, associational, proprietary, behavioural, and informational privacy.[20] A distinction can be made between the objects of privacy (e.g. human dignity) and the things to be protected (e.g. bodies, spaces) on the one hand, and information about them on the other hand. In the European Union (EU), this is reflected in the distinction between the right to a private life (article 7 Charter of Fundamental Rights, CFR) and the right to the protection of personal information (article 8 CFR).

1995), 19; Beate Roessler and Dorota Mokrosinska, "Privacy and Social Interaction," *Philosophy & Social Criticism* 39, no. 8 (October 2013): 771–91, https://doi.org/10.1177/0191453713494968.

11 Sandra Petronio, *Boundaries of Privacy: Dialectics of Disclosure* (SUNY Press, 2002).

12 Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008).

13 Colin J. Bennett, "The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?," ed. Soon Ae Chun, Nabil R. Adam, and Beth Noveck, *Information Polity 23*, no. 2 (June 29, 2018): 239–46, https://doi.org/10.3233/IP-180002.

14 Claudia Diaz and Seda Gürses, "Understanding the Landscape of Privacy Technologies," in *Proceedings of the Information Security Summit 2012* (2012), 58–63.

15 Westin, *Privacy And Freedom*, 7.

16 BVerfGE 65, 1

17 Allen, "Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm"; Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (The University of North Carolina Press, 1995).

18 Westin, *Privacy And Freedom*.

19 Altman, "Privacy. A Conceptual Analysis."

20 Koops et al., "A Typology of Privacy."

Apart from cultural and jurisdictional particularities, there are also important differences in privacy perceptions along the lines of class, ethnicity, gender, social and group norms, and role-specific expectations.[21] This necessary variety in privacy conceptualizations and their contingency on context gives rise to a competition between different perspectives on what privacy is for, bringing to light different social values at play.[22] However, the competition between privacy interpretations in a given practical situation does not take place on a level playing field. What privacy means in practice is shaped by actors with differential power. For instance, a gatekeeper platform can design its own ideas about privacy into the reality of the platform environment.[23]

Platform providers produce privacy in doing.[24] The continuous construction of the platform environment, which is informed by how its users behave in it, is performative discourse: it is an ongoing discursive practice, a communication that constructs a social reality. Within that social reality, the privacy discourse/construction serves a role in reinforcing the larger discursive practices of the platform. What constitutes privacy constantly shifts in the platform environment, but continues to revolve around the core principle that its practical meaning should serve the platform owner.[25] This production of privacy in the platform environment, which is also the platform's discourse on privacy, is therefore also performative.

Users of a platform accommodate to its discursive practices regarding privacy. For instance, iOS app developers, a specific type of users of Apple's App Store platform, focus on App Store approval for their privacy-related practices, rather than on state regulation, end-user concerns, or the public interest – after all, Apple alone decides whether the time and money developers spend creating an app will be rewarded with acceptance to the platform.[26] In the everyday work practices of iOS app developers, privacy becomes what they believe Apple will sanction as privacy practice, and their privacy practices produce app privacy on the platform. Notably, developers and other users assign this power to platforms through their practices, co-constructing the social reality of platforms.

The operational definition of discursive practices of platform privacy used for this analysis is: platform constraints and affordances that shape and regulate in practical reality what is protected under the header of privacy. These practices can include policies, instructions, technical limitations, and user interfaces, among others, and they are mate-

21 Anita L. Allen, "What Must We Hide: The Ethics of Privacy and the Ethos of Disclosure," *St. Thomas Law Review* 25, no. 1 (2012): 1–18; Julie Cohen, "What Privacy Is For," *Harvard Law Review* 126, no. 7 (2013): 1904–33; Nissenbaum, "Privacy as Contextual Integrity."

22 Mulligan, Koopman, and Doty, "Privacy Is an Essentially Contested Concept."

23 Julia Black, "The Rise, Fall and Fate of Principles Based Regulation," *LSE Law, Society and Economy Working Papers* 17 (2010): 26; Greene and Shilton, "Platform Privacies: Governance, Collaboration, and the Different Meanings of 'Privacy' in iOS and Android Development."

24 Wanda J. Orlikowski and Susan V. Scott, "Exploring Material-Discursive Practices," *Journal of Management Studies* 52, no. 5 (2015): 697–705, https://doi.org/10.1111/joms.12114.

25 Tarleton Gillespie, "The Politics of 'Platforms,'" *New Media & Society* 12, no. 3 (May 2010): 347–64, https://doi.org/10.1177/1461444809342738.

26 Greene and Shilton, "Platform Privacies: Governance, Collaboration, and the Different Meanings of 'Privacy' in iOS and Android Development."

rially effective, in that they constitute the truth of what privacy means in the social reality of the platform.

The step-by-step approach to the analysis consists of:

1. Delineating a social reality and a contestable concept for the analysis.

2. Selecting the discursive practices that shape and regulate the practical meaning of the concept within the social reality.

    a. An important selection criterion is whether a practice is materially effective, looking beyond linguistic aspects to, for instance, regulatory and technological practices that can delimit the concept.

    b. "Why" questions can help in the selection: why does the actor (in this case: infrastructure provider) interpret the concept in this way in the social reality at hand, and why choose these practices for that purpose?

3. Evaluating the material effects of the discursive practices regarding the concept, taking into account longer-term effects as well.

The following section illustrates the approach by analysing discursive practices regarding privacy in the case of Apple's App Tracking Transparency Framework (ATT). Conducting a thorough discursive practice analysis requires empirical research, studying the evolving everyday practices that construct a social reality.[27] Unfortunately, extensive empirical research is beyond the remit of this position paper. Instead, the analytical approach will be described for the example case using relevant academic literature and desk research.

A Case in Point: Apple's ATT Framework

The ATT strategy by Apple was chosen because the company conspicuously presents itself as a privacy champion in the consumer market.[28] It has aired advertising proclaiming "Privacy. That's iPhone".[29] Its CEO has delivered keynote speeches at prominent privacy-themed events, such as the 2018 International Data Protection and Privacy Commissioners' Conference,[30] the 2021 Computers, Privacy and Data Protection Conference,[31]

27 Wanda J. Orlikowski and Susan V. Scott, "What Happens When Evaluation Goes Online? Exploring Apparatuses of Valuation in the Travel Sector," *Organization Science* 25, no. 3 (June 2014): 868–91, https://doi.org/10.1287/orsc.2013.0877.

28 Lee McGuigan et al., "The after Party: Cynical Resignation in Adtech's Pivot to Privacy," *Big Data & Society* 10, no. 2 (July 1, 2023): 20539517231203665, https://doi.org/10.1177/20539517231203665.

29 "Privacy on iPhone | Data Auction," Apple, May 18, 2022, YouTube, 0:01:34, https://www.youtube.com/watch?v=NOXK4EVFmJY.

30 Tim Cook, "Keynote address from Tim Cook, CEO, Apple Inc," European Data Protection Supervisor, October 24, 2018, YouTube, 00:22:11, https://www.youtube.com/watch?v=kVhOLkIs20A

31 Tim Cook, "Tim Cook on Privacy," Apple, February 3, 2021, YouTube, 00:12:09, https://www.youtube.com/watch?v=OaLxTz1Yw7M

and the 2022 global summit of the International Association of Privacy Professionals (IAPP).[32]

The case dissected here revolves around a framework for "app tracking transparency" Apple introduced in 2020 for the operation system of its iPhone. The introduction of Apple's iPhone in 2007 was the start of the creation of a large market for smartphone hardware, software applications (apps), and user data. Apple's iPhone operating system, iOS, is one of two major operating systems for smartphones worldwide.[33] The App Store that comes with iOS facilitates downloading and installation of millions of apps, offered by both Apple and third parties (app vendors). Apple suggests several business models to monetize mobile apps in its App Store, but the most popular models include advertising, and sharing or selling of user data.[34]

These data go beyond the information provided knowingly by app users, such as names and payment details, by also including data about clicks and other in-app behaviour, usage statistics (e.g. times, duration, and frequency of use), and meta data such as network access and user locations. This type of collection and processing of user data is known as tracking.[35] App vendors mostly track users for marketing and product improvement purposes. Offering apps without monetary payment, they may sell advertising space in-app, or sell user data or insights to data brokers, marketeers, or others.[36] Although tracking is a common practice, users are often unaware of the extent of it or the associated risks.[37]

Such risks to individuals can be reputational, financial, intellectual, or legal.[38] There may also be risks at a societal level, such as group discrimination, political micro-targeting, and threats to open democratic debate.[39] Therefore, people's low awareness of tracking and its risks has been flagged as problematic, and lawmakers have attempted to require

32 International Association of Privacy Professionals, "LIVE IAPP Summit 2022 General Session with Tim Cook, Zahra Mosawi, Didier Reynders and Trevor Hughes", International Association of Privacy Professionals, April 12, 2022, YouTube, 00:58:45, https://www.youtube.com/watch?v=Dq0fcmmzfog

33 Global Stats | Statscounter, "Mobile Operating System Market Share Worldwide," StatCounter Global Stats, accessed January 10, 2025, https://gs.statcounter.com/os-market-share/mobile/.

34 Ilias Leontiadis et al., "Don't Kill My Ads!: Balancing Privacy in an Ad-Supported Mobile Application Market," in *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications - HotMobile '12* (ACM Press, 2012), 1, https://doi.org/10.1145/2162081.2162084.

35 Konrad Kollnig et al., "A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps," in *Proceedings of the Seventeenth Symposium on Usable Privacy and Security (SOUPS 21)* (2021), 181–96.

36 Chris Jay Hoofnagle and Jan Whittington, "Free: Accounting for the Costs of the Internet's Most Popular Price," *UCLA Law Review* 61, no. 3 (2014): 606–71; Leontiadis et al., "Don't Kill My Ads!"

37 Stephen Cory Robinson, "Self-Disclosure and Managing Privacy: Implications for Interpersonal and Online Communication for Consumers and Marketers," *Journal of Internet Commerce* 16, no. 4 (October 2, 2017): 385–404, https://doi.org/10.1080/15332861.2017.1402637.

38 Ine Van Zeeland and Jo Pierson, "Data Privacy," in *Handbook of Media and Communication Governance*, ed. Manuel Puppis, Robin Mansell, and Hilde Van Den Bulck (Edward Elgar Publishing, 2024), 384–96, https://www.elgaronline.com/edcollchap/book/9781800887206/book-part-9781800887206-40.xml.

39 Cohen, "What Privacy Is For"; Information Commissioner's Office, "Investigation into the Use of Data Analytics in Political Campaigns - A Report to Parliament" (Information Commissioner's Office, November 6, 2018).

transparency and active user consent for it. In the EU, the ePrivacy Directive (ePD)[40] requires explicit consent for tracking, but this provision appears to be widely violated.[41] A proposed update of the ePD, the ePrivacy Regulation, stalled due to intense lobbying exerted by, amongst others, Apple.[42] At a federal level in the US, no such legislation exists, although several states regulate online tracking to some extent. This lacuna has prompted a top politician investigating antitrust violations to remark about Apple's practices that "without a strong privacy law in the United States, platforms will exploit their role as de facto private regulators by placing a thumb on the scale in their own favor".[43]

In iOS, tracking had originally been allowed by default, although users could opt out by adjusting iPhone settings. These settings are found outside the App Store. As a matter of discourse, it is relevant to note the normalized use of the terms "store" and "vendors" for characteristics of software environments, while what a user interacts with are menus and actors listed on a smartphone screen. In terms of discursive practices, the iPhone settings materialize the conception of information privacy that Apple is imposing as the private regulator of its infrastructure: privacy for users means sharing less data gathered about them by the iOS and apps with technology and data companies (called app vendors), and to achieve such privacy practically, users need to find and click on pre-determined iOS settings.

In an update to iOS (iOS 14.5) in April 2021, Apple introduced the App Tracking Transparency (ATT) framework.[44] This update may have been inspired by expected regulatory action: in 2022, the French Data Protection Authority (CNIL) issued an €8 million fine to Apple under the ePD, for having the Personalized Advertising privacy setting turned on by default in iOS 14.6 and earlier versions.[45] Meanwhile, Apple had made an estimated $7 billion on advertising in 2022.[46]

The ATT framework consists of contractual and technical standards for App Store apps. The contractual standards require that apps disclose tracking practices, materialized in

40 Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37.

41 Ine Van Zeeland and Jo Pierson, "Data Privacy," in *Handbook of Media and Communication Governance*, ed. Manuel Puppis, Robin Mansell, and Hilde Van Den Bulck (Edward Elgar Publishing, 2024), 384–96, https://www.elgaronline.com/edcollchap/book/9781800887206/book-part-9781800887206-40.xml.

42 Corporate Europe Observatory, "Big Data Is Watching You," October 17, 2017, https://corporateeurope.org/en/power-lobbies/2017/10/big-data-watching-you.

43 Reed Albergotti, "Apple Says Recent Changes to Operating System Improve User Privacy, but Some Lawmakers See Them as an Effort to Edge out Its Rivals," Washington Post, November 26, 2019, https://www.washingtonpost.com/technology/2019/11/26/apple-emphasizes-user-privacy-lawmakers-see-it-an-effort-edge-out-its-rivals/.

44 The ATT framework was introduced for its operating systems of iPhones, iPads, and Apple televisions, but for reasons of brevity the analysis is restricted to the consequences for smartphone users.

45 CNIL, "Identifiant Publicitaire : Sanction de 8 Millions d'euros à l'encontre de APPLE DISTRIBUTION INTERNATIONAL," December 29, 2022, https://www.actualitesdudroit.fr/browse/affaires/immateriel/39546/identifiant-publicitaire-sanction-de-8-millions-d-euros-prononcee-par-la-cnil-a-l-encontre-de-apple-distribution-international.

46 Jeremy Goldman, "Why Apple Could Be 2023's Most Impactful Advertising Player," Insider Intelligence, December 28, 2022, https://www.insiderintelligence.com/content/apple-will-emerge-advertising-player-watch-2023.

"privacy nutrition labels", that require the vendor of an app to provide a list of the types of user data collected, along with the purposes for which they are processed. This information is displayed in the App Store in a user-friendly overview. However, the information is not verified by Apple, and research has found "notable discrepancies between apps' disclosed and actual data practices".[47]

The ATT framework's technical standards force app vendors to obtain user consent for tracking by blocking access to Apple's Identifier for Advertisers (IDFA) for vendors if users have not consented. The IDFA code uniquely identifies iPhone users, which allows for tracking across different apps and services. However, there are other ways to uniquely identify users, for example by combining other data types into a self-made unique code (a practice known as fingerprinting). These data types can be obtained by requesting permissions for an app when it is installed, for instance for access to the user location, the iPhone name, or the unique International Mobile Equipment Identity (IMEI) of the device.[48] Faced with such permission requests, users can either accept or not install the app. Due to the ubiquity of consent requests, consent fatigue is a common response by users who simply click 'accept' to get on with their lives.[49] Apps' use of permissions and fingerprinting increased after the introduction of the ATT framework, in violation of Apple's Developer Program License Agreement.[50] From late 2023 onwards, Apple has required vendors to declare reasons for permissions, but again, this self-declared information does not appear to be verified.

In another work-around, large vendors can combine data types to create their own identifiers because they offer more apps, or services embedded in other vendors' apps. Examples are social media integration for seamless access ("Sign in with Gmail") and authentication and analytics services, such as the Facebook software development kit used in other vendors' apps.[51]

What the ATT framework does not provide transparency on is Apple's own practices. As the gatekeeper to the entire iOS infrastructure, Apple can and does track users throughout. A comparison between Apple's definition of tracking and the definition of the World Wide Web Consortium (W3C) is telling (table 1).

47 Konrad Kollnig et al., "Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels," in *2022 ACM Conference on Fairness, Accountability, and Transparency, FAccT '22* (Association for Computing Machinery, 2022), 508–20, https://doi.org/10.1145/3531146.3533116. Kollnig et al. (2022) note app developers are often unaware of tracking elements in software development kits and third-party libraries they use in their code. Naturally, they will not report tracking practices of which they are unaware.

48 Leontiadis et al., "Don't Kill My Ads!"

49 Leontiadis et al., "Don't Kill My Ads!"

50 Kollnig et al., "Goodbye Tracking?"

51 Robert Burnson, "Meta Sued for Skirting Apple Privacy Rules to Snoop on Users," Bloomberg.Com, September 22, 2022, https://www.bloomberg.com/news/articles/2022-09-22/meta-sued-for-skirting-apple-privacy-rules-to-snoop-on-users.

Table 1 Comparison between the W3C's definition of tracking and Apple's definition

World Wide Web Consortium (W3C)	Apple App Store: User privacy and data use
"the collection of data regarding a particular user's activity across multiple distinct contexts, and the retention, use, or sharing of data derived from that activity outside the context in which it occurred."[52]	"the act of linking user or device data collected from your app with user or device data collected from other companies' apps, websites, or offline properties for targeted advertising or advertising measurement purposes. Tracking also refers to sharing user or device data with data brokers."[53]

"First-party tracking", in which data are collected by the platform provider, is not tracking in Apple's definition, in contrast to the W3C definition that emphasises "across multiple distinct contexts". Apple does track users across multiple contexts (different services and devices), using the Apple ID, hardware identifiers, and device permissions to which it has privileged access. This could be argued to rest on different interpretations of "context", which Apple interprets in its own interest; the App Store may not be a different context than the device settings after all, when that framing does not serve Apple's interests in tracking users. As Apple may argue, based on its definition of tracking, it is the same company that follows users between apps and across different iPhone services (and other Apple devices) for targeted advertising purposes, therefore it is not tracking. Incidentally, Apple also collects data about advertising in other vendors' apps for its own purposes.[54] Moreover, after the introduction of iOS 14.6, Apple appears to have tracked its users even more even when they turned off sharing device data.[55]

The ATT framework did have a large impact on user data processing by other companies presenting as vendors in the App Store. In the first year after its introduction, a majority of iPhone users (up to 70 percent) did not consent to tracking.[56] This indicates that most iPhone users are not fond of tracking. It remains unclear to what extent they are aware of tracking by Apple and whether they would consent to its tracking practices, since they have no options to accept or refuse tracking by Apple except to buy a smartphone with another operating system. In the debate around the EU's proposal for the Digital Services Act, an important piece of platform regulation, privacy activists used the high tracking

52 "Tracking Compliance and Scope," W3C.org, retrieved April 28, 2025, from https://www.w3.org/TR/tracking-compliance/#tracking

53 "User Privacy and Data Use—App Store," Apple Developer, retrieved April 28, 2025, from https://developer.apple.com/app-store/user-privacy-and-data-use/

54 Kollnig et al., "Goodbye Tracking?"

55 Thomas Germain, "Apple Tracks You Even With Its Own Privacy Protections on, Study Says," Gizmodo, November 8, 2022, https://gizmodo.com/apple-iphone-analytics-tracking-even-when-off-app-store-1849757558.

56 Statista, "iOS ATT Opt-in Rate by App Category 2022," Statista, accessed January 10, 2025, https://www.statista.com/statistics/1281345/apple-att-opt-in-rate-by-app-category/.

refusal rates in their argumentation for a ban on targeted advertising, but they did not sufficiently convince lawmakers.[57]

Since this analysis focuses on the practices of the infrastructure provider, we have no insight into the acceptance of Apple's construction of privacy and responsibility by users. Possibly, a refusal to be tracked by Apple could explain the popularity of the other major OS, Android, but since Android's track record is in many ways similar in its practical effects for users, that is an unlikely scenario. The reason why users cannot simply switch to other operating systems, is because they would effectively opt out of many aspects of our digitalizing society: digital platforms such as Apple's and Google's have become essential social infrastructures.[58] Forswearing smartphones or using a smartphone with an OS that is incompatible with most other people's may disrupt communications with family and friends, authorities and service providers.

With users having few options but to accept tracking by the infrastructure provider, the ATT framework mostly affected advertising revenue distribution. The share of advertising on the iOS for Apple's own advertising network increased from 17 to 58 percent in the same year.[59] Search advertising in its App Store turned out to be most profitable for Apple, while it also brought advertising to other parts of its infrastructure.[60]

Associations representing App Store vendors have filed competition complaints at market supervisory authorities.[61] The German market authority Bundeskartellamt announced proceedings against Apple over the ATT framework in June 2022, to investigate suspicions of self-preferencing or impediment of competitors. In the announcement, the Bundeskartellamt president stated: "A corporation like Apple which is in a position to unilaterally set rules for its ecosystem, in particular for its app store, should make pro-competitive rules. We have reason to doubt that this is the case when we see that Apple's rules apply to third parties, but not to Apple itself".[62]

Discussion

Through the analysis of the ATT case, several discursive practices have been identified that construct a privacy reality on the App Store platform: lobbying, tracking and

57 Johann Laux, Sandra Wachter, and Brent Mittelstadt, "Taming the Few: Platform Regulation, Independent Audits, and the Risks of Capture Created by the DMA and DSA," *Computer Law & Security Review* 43 (November 2021): 105613, https://doi.org/10.1016/j.clsr.2021.105613.

58 Jo Pierson, "Digital Platforms as Entangled Infrastructures: Addressing Public Values and Trust in Messaging Apps," *European Journal of Communication* 36, no. 4 (August 2021): 349–61, https://doi.org/10.1177/02673231211028374.

59 FT.com, "Apple's Privacy Changes Create Windfall for Its Own Advertising Business," October 17, 2021, https://www.ft.com/content/074b881f-a931-4986-888e-2ac53e286b9d.

60 Goldman, "Why Apple Could Be 2023's Most Impactful Advertising Player."

61 Autorité de la concurrence, "Publicité sur applications mobiles iOS : le rapporteur général indique voir notifié un grief au groupe Apple," Autorité de la concurrence, July 25, 2023, https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/publicite-sur-applications-mobiles-ios-le-rapporteur-general-indique-avoir.

62 Bundeskartellamt, "Bundeskartellamt - Homepage - Bundeskartellamt Reviews Apple's Tracking Rules for Third-Party Apps," June 14, 2022, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/14_06_2022_Apple.html.

a restrictive definition of tracking, (default) operating system settings, contractual standards including privacy nutrition labels, technical standards including permissions and access to an identifying code, fingerprinting, the license agreement for app vendors, and consenting. With regard to the operational definition of discursive practices used in this analysis, the platform affordances and constraints that shape and regulate what is protected under the header of privacy consist of

- linguistic elements (framing; a definition; unverified declarations of data use),
- technological-material elements (access to codes, settings and data; tracking and fingerprinting),
- regulatory elements (a license agreement; contractual standards) and
- political elements (lobbying; public posturing).

The 'why' can be found in the profits made from targeted advertising on the platform, but to some extent, also in interventions by (supra)national regulators. Potential but excluded privacy-oriented practices are: providing transparency on tracking by Apple itself and asking consent for it; asking end users to express their own nuanced preferences in sharing personal information; or prohibiting tracking by anyone.

Apple's attempt to impose its interpretations of privacy and tracking within its infrastructure is contested by regulatory investigations and EU digital regulation, but these contestations do not explicitly or fundamentally challenge Apple's privacy discourse. Another form of opposition comes from circumventive maneuvers of other companies in the "battle for interpretive control" around users' information privacy.[63] Over time, these contestations may lead to incremental changes to the gatekeeper platform's discursive practices, but for at least a few years its hegemonic strategy to frame privacy in its interest has been impressively profitable.

There may be long-term effects on the acceptability of Apple's interpretation of privacy. App developers learn what privacy means through practices focused on acceptance into the App Store, as well as through training and documentation from Apple or similar platforms.[64] Through their everyday interaction with smartphones, users become habituated to the (even within the privacy-as-control paradigm)[65] severely restrictive interpretation of privacy as limited user control over device settings and app data-sharing practices. The restrictive interpretation of privacy enacted by Big Tech platform providers fits into a wider liberal view in which the value of privacy lies in individual interests and rights. Apple's construction of privacy may thus also reinforce a wider discourse of individual choice and responsibility.

63 Black, "The Rise, Fall and Fate of Principles Based Regulation."

64 Greene and Shilton, "Platform Privacies: Governance, Collaboration, and the Different Meanings of 'Privacy' in iOS and Android Development"; Ari Ezra Waldman, "Habit and Performative Privacy," *Social Epistemology Review and Reply Collective* 10, no. 10 (2021): 43–50.

65 Diaz and Gürses, "Understanding the Landscape of Privacy Technologies."

The privacy-as-control paradigm is akin to the privacy-as-security paradigm, in which the main privacy risks are considered to be access, copying, or modification of data by third-party threats.[66] A naive analysis of Apple's practices might conclude the ATT framework aligns with that privacy paradigm, but a critical inspection reveals its practices to be strategic, as evidenced by its lobbying against legal interventions to mitigate such threats, and the highly profitable, anti-competitive effects of the ATT framework on its market position. Other alternative privacy paradigms that emphasise societal interests, such as maintaining intersubjective or context-specific standards of appropriate role behaviour and information sharing, are entirely ignored by the ATT framework.[67]

Compared to classical discourse analysis, the analysis of discursive practices goes beyond the focus on how language reflects and reinforces power structures (while power is also constructed within discourse),[68] to examine technological-material aspects – not merely *effects*, but how materiality and discourse are different sides of the same coin.[69] In the case of a dominant infrastructural actor like Apple, this means more than "code is law" and vice versa, it implies that the dominant discourse participant literally produces the material reality through its discourse, and at the same time the material practice is the discourse. The ATT framework, with its contractual and technical standards, materializes the only possible truth of transparency, tracking, and privacy within Apple's walled - or rather, its framed - garden. In this meticulously framed garden, users on all sides of Apple's multi-sided platform (app developers, advertisers, end-users) get to perceive privacy only in the way the platform allows, as the infrastructural frame sets the boundaries of what privacy is and how it can be achieved.

The analytical approach presented here can provide answers to why questions, but it is not suitable for finding causal explanations. The kinds of why questions it can answer are questions about reasons, not about causes. Another limitation is that the analysis of discursive practices in this approach is one-sided, not taking into account the acceptance of Apple's privacy discourse by users, although the high rates of tracking refusal do provide some indication. Furthermore, the selection and availability of resources, and the amount of access researchers have to them, may influence the analysis, although it must be pointed out that while this example analysis relied on previous research and public documentation, ideally the analysis is based on ethnographic methods studying practices as they evolve inside organisations, providing richer detail.

A basic assumption of this approach is that reality is constructed, made of understandings acted out. The value of this approach lies in the idea that we can also construct our social realities differently and that we can reopen the discussion on what, in this case, privacy can be.

66 Irit Hadar et al., "Privacy by Designers: Software Developers' Privacy Mindset," *Empirical Software Engineering* 23, no. 1 (February 2018): 259–89, https://doi.org/10.1007/s10664-017-9517-1.

67 Nissenbaum, "Privacy as Contextual Integrity"; Roessler and Mokrosinska, "Privacy and Social Interaction."

68 Hook, *Foucault, Psychology and the Analytics of Power.*

69 Orlikowski and Scott, "Exploring Material-Discursive Practices."

Conclusion

In his speech at the 2022 IAPP summit, Apple CEO Tim Cook warned that European lawmakers' plans to force Apple to allow installation of apps outside the iOS App Store (under the EU's proposed Digital Markets Act) would entail that "data-hungry companies would be able to avoid our privacy rules, and once again track our users against their will".[70] The references to "our privacy rules" and "our users" are telling.

The analysis proposed in this paper does not include the reception-side of the discursive practices, i.e. acceptance by users. Infrastructural coercion may not be sufficient to dominate a discourse. For example, the platform provider Meta's discourse on privacy may be taken with a grain of salt by users since its platforms have been repeatedly embroiled in privacy scandals. For a discourse to take hold, its proponent must be seen as legitimate. Apple's consistent virtue signalling may have provided it an excess of credibility regarding privacy protection. In addition, its users may attribute "pragmatic legitimacy" to the platform provider because the alternatives are no better, they like the brand for other reasons, or they believe that Apple is a decent company.[71] These would certainly be interesting topics for further research into Apple's discursive practices around privacy.

As this paper sets out, privacy is a necessarily contested concept and therefore, attempts to materialize it in essential communication infrastructure should be approached with caution. Importantly, the analysis has shown that the concept of privacy is not an abstract sensitivity; its interpretation has material and experiential consequences. Through analysing the discursive practices of the infrastructure providers, it becomes clear which practices enact their interests and which interests are subdued by excluding other practices. Analysing discursive practices is therefore an active intervention, as exposure of potentially hidden agendas and power moves in itself make a difference in the construction of social reality.[72]

The example analysis in this paper concluded that privacy was constructed in a severely restricted manner. Does this lead to the conclusion that the term privacy should not be used to refer to device settings or organisational policies around personal data? While a discursive practices analysis explores norms as practices and its critical approach questions them, it does not push alternative narratives, although it asks why they are excluded. That does imply that the analysis itself is a discursive practice, and a necessary one in a digital social reality that is increasingly dominated by a selective few.

70 International Association of Privacy Professionals. "LIVE IAPP Summit 2022 General Session with Tim Cook, Zahra Mosawi, Didier Reynders and Trevor Hughes," at 00:22:18-28.

71 Mark C. Suchman, "Managing Legitimacy: Strategic and Institutional Approaches," *The Academy of Management Review* 20, no. 3 (1995): 571–610. Suchman (1995) notes that advertising is a common strategy to manipulate pragmatic legitimacy, which may explain Apple's "Your data are $old" ads.

72 Orlikowski and Scott, "Exploring Material-Discursive Practices."

References

Albergotti, Reed. "Apple Says Recent Changes to Operating System Improve User Privacy, but Some Lawmakers See Them as an Effort to Edge out Its Rivals." *Washington Post*, November 26, 2019, https://www.washingtonpost.com/technology/2019/11/26/apple-emphasizes-user-privacy-lawmakers-see-it-an-effort-edge-out-its-rivals/.

Allen, Anita L. "Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm." *Connecticut Law Review* 32, no. 3 (2000): 861–76.

———. "What Must We Hide: The Ethics of Privacy and the Ethos of Disclosure." *St. Thomas Law Review* 25, no. 1 (2012): 1–18.

Altman, Irwin. "Privacy. A Conceptual Analysis." *Environment and Behavior* 8, no. 1 (March 1, 1976): 7–29. https://doi.org/10.1177/001391657600800102.

Apple, "Privacy on iPhone | Data Auction." Apple, May 18, 2022, YouTube video, 1 min., 34 sec. https://www.youtube.com/watch?v=NOXK4EVFmJY.

Autorité de la concurrence. "Publicité sur applications mobiles iOS : le rapporteur général indique avoir notifié un grief au groupe Apple." Autorité de la concurrence, July 25, 2023, https://www.autoritedelaconcurrence.fr/fr/communiques-de-presse/publicite-sur-applications-mobiles-ios-le-rapporteur-general-indique-avoir.

Bacchi, Carol, and Jennifer Bonham. "Reclaiming Discursive Practices as an Analytic Focus: Political Implications." *Foucault Studies*, (April 30, 2014): 179–92, https://doi.org/10.22439/fs.v0i17.4298.

Bennett, Colin J. "The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?" Edited by Soon Ae Chun, Nabil R. Adam, and Beth Noveck, *Information Polity* 23, no. 2 (June 29, 2018): 239–46, https://doi.org/10.3233/IP-180002.

Black, Julia. "The Rise, Fall and Fate of Principles Based Regulation." *LSE Law, Society and Economy Working Papers*, 17 (2010): 26.

Bundeskartellamt. "Bundeskartellamt Reviews Apple's Tracking Rules for Third-Party Apps." Last modified June 14, 2022. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2022/14_06_2022_Apple.html.

Burnson, Robert. "Meta Sued for Skirting Apple Privacy Rules to Snoop on Users." *Bloomberg.Com*, September 22, 2022, https://www.bloomberg.com/news/articles/2022-09-22/meta-sued-for-skirting-apple-privacy-rules-to-snoop-on-users.

CNIL. "Identifiant Publicitaire : Sanction de 8 Millions d'euros à l'encontre de APPLE DISTRIBUTION INTERNATIONAL." Last modified December 29, 2022. https://www.actualitesdudroit.fr/browse/affaires/immateriel/39546/identifiant-publicitaire-sanction-de-8-millions-d-euros-prononcee-par-la-cnil-a-l-encontre-de-apple-distribution-international.

Cohen, Julie. "What Privacy Is For." *Harvard Law Review* 126, no. 7 (2013): 1904–33.

Cook, Tim. "Keynote address from Tim Cook, CEO, Apple Inc." European Data Protection Supervisor, October 24, 2018, YouTube video, 22 min., 11 sec. https://www.youtube.com/watch?v=kVhOLkIs20A

Cook, Tim. "Tim Cook on Privacy." Apple, February 3, 2021, YouTube video, 12 min., 9 sec. https://www.youtube.com/watch?v=OaLxTz1Yw7M

Corporate Europe Observatory. "Big Data Is Watching You." Last modified October 17, 2017. https://corporateeurope.org/en/power-lobbies/2017/10/big-data-watching-you.

Diaz, Claudia, and Seda Gürses. "Understanding the Landscape of Privacy Technologies." In *Proceedings of the Information Security Summit 2012*, 58–63, 2012.

FT.com. "Apple's Privacy Changes Create Windfall for Its Own Advertising Business." Last modified October 17, 2021. https://www.ft.com/content/074b881f-a931-4986-888e-2ac53e286b9d.

Germain, Thomas. "Apple Tracks You Even With Its Own Privacy Protections on, Study Says." Gizmodo, November 8, 2022. https://gizmodo.com/apple-iphone-analytics-tracking-even-when-off-app-store-1849757558.

Gillespie, Tarleton. "The Politics of 'Platforms.'" *New Media & Society* 12, no. 3 (May 2010): 347–64. https://doi.org/10.1177/1461444809342738.

Global Stats | Statscounter. "Mobile Operating System Market Share Worldwide." StatCounter Global Stats. Accessed January 10, 2025. https://gs.statcounter.com/os-market-share/mobile/.

Goldman, Jeremy. "Why Apple Could Be 2023's Most Impactful Advertising Player." *Insider Intelligence*, (December 28, 2022). https://www.insiderintelligence.com/content/apple-will-emerge-advertising-player-watch-2023.

Greene, Daniel, and Katie Shilton. "Platform Privacies: Governance, Collaboration, and the Different Meanings of 'Privacy' in iOS and Android Development." *New Media & Society* 20, no. 4 (2018): 1640–57.

Hadar, Irit, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. "Privacy by Designers: Software Developers' Privacy Mindset." *Empirical Software Engineering* 23, no. 1 (February 2018): 259–89. https://doi.org/10.1007/s10664-017-9517-1.

Hardy, Cynthia, and Robyn Thomas. "Discourse in a Material World." *Journal of Management Studies* 52, no. 5 (2015): 680–96. https://doi.org/10.1111/joms.12113.

Hoofnagle, Chris Jay, and Jan Whittington. "Free: Accounting for the Costs of the Internet's Most Popular Price." *UCLA Law Review* 61, no. 3 (2014): 606–71.

Hook, Derek. *Foucault, Psychology and the Analytics of Power. Critical Theory and Practice in Psychology and the Human Sciences.* Palgrave Macmillan, 2007, https://lanlib.alzahra.ac.ir/multiMediaFile/2231433-4-1.pdf.

Information Commissioner's Office. "Investigation into the Use of Data Analytics in Political Campaigns - A Report to Parliament." Information Commissioner's Office, November 6, 2018.

International Association of Privacy Professionals. "LIVE IAPP Summit 2022 General Session with Tim Cook, Zahra Mosawi, Didier Reynders and Trevor Hughes." International Association of Privacy Professionals, April 12, 2022, YouTube video, 58 min., 45 sec. https://www.youtube.com/watch?v=Dq0fcmmzfog

Kollnig, Konrad, Reuben Binns, Pierre Dewitte, Max Van Kleek, Ge Wang, Daniel Omeiza, Helena Webb, and Nigel Shadbolt. "A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps." In *Proceedings of the Seventeenth Symposium on Usable Privacy and Security (SOUPS 21)*, 181–96, 2021.

Kollnig, Konrad, Anastasia Shuba, Max Van Kleek, Reuben Binns, and Nigel Shadbolt. "Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels." In *2022 ACM Conference on Fairness, Accountability, and Transparency*, 508–20. FAccT '22. New York, NY, USA: Association for Computing Machinery, 2022, https://doi.org/10.1145/3531146.3533116.

Koops, Bert-Jaap, Bryce Newell, Tjerk Timan, Ivan Škorvánek, Tom Chokrevski, and Galič Maša. "A Typology of Privacy." *University of Pennsylvania Journal of International Law* 38, no. 2 (September 18, 2017).

Laux, Johann, Sandra Wachter, and Brent Mittelstadt. "Taming the Few: Platform Regulation, Independent Audits, and the Risks of Capture Created by the DMA and DSA." *Computer Law & Security Review* 43 (November 2021): 105613. https://doi.org/10.1016/j.clsr.2021.105613.

Leontiadis, Ilias, Christos Efstratiou, Marco Picone, and Cecilia Mascolo. "Don't Kill My Ads!: Balancing Privacy in an Ad-Supported Mobile Application Market." In *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications - HotMobile '12*, 1. ACM Press, 2012. https://doi.org/10.1145/2162081.2162084.

McGuigan, Lee, Sarah Myers West, Ido Sivan-Sevilla, and Patrick Parham. "The after Party: Cynical Resignation in Adtech's Pivot to Privacy." *Big Data & Society* 10, no. 2 (July 1, 2023): 20539517231203665. https://doi.org/10.1177/20539517231203665.

Mulligan, Deirdre K., Colin Koopman, and Nick Doty. "Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374, no. 2083 (December 28, 2016): 20160118. https://doi.org/10.1098/rsta.2016.0118.

Newell, Patricia Brierley. "Perspectives on Privacy." *Journal of Environmental Psychology* 15 (1995): 87–104.

Nissenbaum, Helen. "Privacy as Contextual Integrity." *Washington Law Review* 79, no. 1 (2004): 119–58.

Orlikowski, Wanda J., and Susan V. Scott. "Exploring Material-Discursive Practices." *Journal of Management Studies* 52, no. 5 (2015): 697–705. https://doi.org/10.1111/joms.12114.

———. "What Happens When Evaluation Goes Online? Exploring Apparatuses of Valuation in the Travel Sector." *Organization Science* 25, no. 3 (June 2014): 868–91. https://doi.org/10.1287/orsc.2013.0877.

Petronio, Sandra. *Boundaries of Privacy: Dialectics of Disclosure*. SUNY Press, 2002.

Pierson, Jo. "Digital Platforms as Entangled Infrastructures: Addressing Public Values and Trust in Messaging Apps." *European Journal of Communication* 36, no. 4 (August 2021): 349–61. https://doi.org/10.1177/02673231211028374.

Plantin, Jean-Christophe, Carl Lagoze, Paul N Edwards, and Christian Sandvig. "Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook." *New Media & Society* 20, no. 1 (January 2018): 293–310. https://doi.org/10.1177/1461444816661553.

Regan, Priscilla M. *Legislating Privacy: Technology, Social Values, and Public Policy*. The University of North Carolina Press, 1995.

Reiman, Jeffrey H. "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future." *Santa Clara High Technology Law Journal*, (January 1995): 19.

Robinson, Stephen Cory. "Self-Disclosure and Managing Privacy: Implications for Interpersonal and Online Communication for Consumers and Marketers." *Journal of Internet Commerce* 16, no. 4 (October 2, 2017): 385–404. https://doi.org/10.1080/15332861.2017.1402637.

Roessler, Beate. "Three Dimensions of Privacy." In *The Handbook of Privacy Studies: An Interdisciplinary Introduction*, edited by Bart Sloot and Aviva Groot, 137–41. Amsterdam University Press, 2018. https://doi.org/10.5117/9789462988095.

Roessler, Beate, and Dorota Mokrosinska. "Privacy and Social Interaction." *Philosophy & Social Criticism* 39, no. 8 (October 2013): 771–91. https://doi.org/10.1177/0191453713494968.

Solove, Daniel J. "Conceptualizing Privacy." *California Law Review* 90, no. 4 (2002): 1087–1156.

———. *Understanding Privacy*. Harvard University Press, 2008.

Statista. "iOS ATT Opt-in Rate by App Category 2022." Statista. Accessed January 10, 2025. https://www.statista.com/statistics/1281345/apple-att-opt-in-rate-by-app-category/.

Suchman, Mark C. "Managing Legitimacy: Strategic and Institutional Approaches." *The Academy of Management Review* 20, no. 3 (1995): 571–610.

Van der Sloot, Bart. "Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data.'" *Utrecht Journal of International and European Law* 31, no. 80 (February 27, 2015): 25–50. https://doi.org/10.5334/ujiel.cp.

Van Zeeland, Ine, and Jo Pierson. "Data Privacy." In *Handbook of Media and Communication Governance*, edited by Manuel Puppis, Robin Mansell, and Hilde Van Den Bulck, 384–96. Edward Elgar Publishing, 2024. https://www.elgaronline.com/edcollchap/book/9781800887206/book-part-9781800887206-40.xml.

W3C. (n.d.). "Tracking Compliance and Scope." W3C.org. Retrieved April 28, 2025, from https://www.w3.org/TR/tracking-compliance/#tracking

Waldman, Ari Ezra. "Habit and Performative Privacy." *Social Epistemology Review and Reply Collective* 10, no. 10 (2021): 43–50.

Westin, Alan F. *Privacy And Freedom*. Atheneum, 1967. https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr.