COMPUTER LAW & SECURITY REVIEW 41 (2021) 105557

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Smartphone platforms as privacy regulators

Joris van Hoboken[a], *R Ó Fathaigh*[b,#,*]

[a] *Institute for Information Law, University of Amsterdam; Professor of Law, Chair 'Fundamental Rights and Digital Transformation', Vrije Universiteit Brussel (VUB). The Chair at VUB is established at the Interdisciplinary Research Group on Law Science Technology & Society, with the support of Microsoft*

[b] *Institute for Information Law, University of Amsterdam*

ARTICLE INFO

Keywords:
Online platforms
Smartphones
Data protection
Privacy
Regulation
Disclosures

ABSTRACT

A series of recent developments highlight the increasingly important role of online platforms in impacting data privacy in today's digital economy. Revelations and parliamentary hearings about privacy violations in Facebook's app and service partner ecosystem, EU Court of Justice judgments on joint responsibility of platforms and platform users, and the rise of smartphone app ecosystems where app behaviour is governed by app distribution platforms and operating systems, all show that platform policies can make or break the enjoyment of privacy by users. In this article, we examine these developments and explore the question of what can and should be the role of platforms in protecting data privacy of their users.

The article first distinguishes the different roles that platforms can have in ensuring respect for data privacy in relevant ecosystems. These roles include governing access to data, design of relevant interfaces and privacy mechanisms, setting of legal and technical standards, policing behaviour of the platform's (business) users, coordinating responsibility for privacy issues between platform users and the platform, and direct and indirect enforcement of a platform's data privacy standards on relevant players. At a higher level, platforms can also perform a role by translating different international regulatory requirements into platform policies, thereby facilitating compliance of apps in different regulatory environments. And in all of this, platforms are striking a balance between ensuring the respect for data privacy in data-driven environments on the one hand and optimization of the value and business opportunities connected to the platform and underlying data for users of the platform on the other hand.

After this analysis of platforms' roles in protecting privacy, the article turns to the question of what should this role be and how to better integrate platforms in the current legal frameworks for data privacy in Europe and the US. The article will argue for a compromise between direct regulation of platforms and mere self-regulation, in arguing that platforms should be required to make official disclosures about their privacy-related policies and practices for their respective ecosystems. These disclosures should include statements about relevant conditions for access to data and the platform, the platform's standards with respect to privacy and the way in which these standards ensure or facilitate compliance with

* Corresponding author: Ronan Ó Fathaigh, Institute for Information Law, University of Amsterdam, Nieuwe Achtergracht 166, 1018 WV Amsterdam, The Netherlands.

E-mail addresses: j.v.j.vanHoboken@uva.nl (J. van Hoboken), r.f.fahy@uva.nl (R.Ó. Fathaigh).

# Authors have contributed equally to this article.

https://doi.org/10.1016/j.clsr.2021.105557

existing legal frameworks by platform users, and statements with respect to the risks of abuse of different data sources and platform tools and actions taken to prevent or police such abuses. We argue that such integration of platforms in current regulatory frameworks is both feasible and desirable. It would make the role that platforms already have in practice more explicit. This would help to highlight best practices, create more accountability and could save significant regulatory and compliance resources in bringing relevant information together in one place. In addition, it could provide clarity for business users of platforms, who are now sometimes confronted with restrictive decisions by platforms in ways that lack transparency and oversight.

1. Introduction

Facebook's Cambridge Analytica scandal has been privacy's most recent watershed moment. It has created an awareness across the political spectrum in the United States that privacy laws may need an update for the digital age. In Europe, it has strengthened the resolve of policy makers and privacy regulators to proceed on the basis of the strong data privacy standards adopted with the General Data Protection Regulation (GDPR).[1] Following an investigation by the Federal Trade Commission (FTC) into the scandal, Facebook agreed to pay a record-breaking $5 billion penalty to settle charges that it deceived its users about its privacy practices.[2] In summary, the Cambridge Analytica scandal not only brought to light problematic personal data gathering, profiling and micro-targeting practices, it more broadly highlighted the extent to which platforms, such a Facebook, have turned into the central new data brokers of the digital age, leveraging unprecedented quantities of personal data shared by their users for profit, through innovations in platform tools for advertisers and data management strategies.[3]

The Cambridge Analytica scandal and other data broker-like activity involving Facebook apps highlight how much of Facebook's business model revolves around direct access to Facebook users' data.[4] Investigative reporting has now uncovered Facebook strategically offering privileged access to data for certain business partners.[5] In leaked Facebook documents, Facebook discussed 'cutting off access to user data' for an app that had 'grown too popular and was viewed as a competitor', and Facebook was 'formulating a strategy to publicly frame these moves as a way of protecting user privacy'.[6] As such, the discussions around Cambridge Analytica brought to the fore the question of how platforms (mis)manage the trade-offs between the opportunities related to pervasive legibility of citizens and consumers and the protection of privacy interests of the same.[7] More generally, this role in managing complicated trade-offs highlights the role that platforms nowadays find themselves in: a role as privacy regulators.[8]

In another high-profile example of a platform striking this balance in ways that have caused debate, Apple is alleged to use privacy protection of its users anti-competitively in relation to app providers relying on Apple's mobile platform iOS. For example, the *New York Times* recently reported that screen-time apps were removed from the App Store over supposed privacy and security concerns, but with app developers alleging they were 'being targeted because their apps could hurt

[1] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1.

[2] *In the Matter of Facebook, Inc.* (Case No. 19-cv-2184) Federal Trade Commission File No. C-4365 (24 July 2019).

[3] On the rise of platforms more generally, see Annabelle Gawer (ed), *Platforms, markets and innovation* (Edward Elgar Publishing 2011); Geoffrey G. Parker, Marshall W. Van Alstyne, and Sangeet Paul Choudary, *Platform revolution: How networked markets are transforming the economy and how to make them work for you* (WW Norton & Company 2016); David S. Evans and Richard Schmalensee, *The industrial organization of markets with two-sided platforms* (National Bureau of Economic Research 2005); and José Van Dijck, Thomas Poell and Martijn De Waal, *The platform society: Public values in a connective world* (OUP 2018).

[4] Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, 'How Trump Consultants Exploited the Facebook Data of Millions' *The New York Times* (17 March 2018) <www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> (all links last accessed 24 February 2020). See also, Information Commissioner's Office, *Investigation into the use of data analytics in political campaigns: A report to Parliament 6 November 2018* (ICO 2018); and *Facebook Ireland Ltd.* (Monetary Penalty Notice) Information Commissioner's Office (24 October 2018).

[5] Gabriel J.X. Dance, Nicholas Confessore and Michael LaForgia, 'Facebook Gave Device Makers Deep Access to Data on Users and Friends' *The New York Times* (3 June 2018) <www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html>. See also, Michael LaForgia, Matthew Rosenberg and Gabriel J.X. Dance, 'Facebook's Data Deals Are Under Criminal Investigation' *The New York Times* (13 March 2019) <www.nytimes.com/2019/03/13/technology/facebook-data-deals-investigation.html>.

[6] Olivia Solon and Cyrus Farivar, 'Mark Zuckerberg leveraged Facebook user data to fight rivals and help friends, leaked documents show' *NBC News* (16 April 2019) <www.nbcnews.com/tech/social-media/mark-zuckerberg-leveraged-facebook-user-data-fight-rivals-help-friends-n994706>.

[7] On the role of platforms in constructing access to and legibility of populations, see Julie E Cohen, 'Law for the Platform Economy' (2017) 51 *UC Davis Law Review* 133.

[8] See Tarleton Gillespie, 'Governance of and by platforms' in Jean Burgess, Alica Marwick and Thomas Poell, *The SAGE Handbook of Social Media* (SAGE 2017), 254 - 278. See also, Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, *Competition policy for the digital era* (European Commission 2019).

Apple's business'.[9] Apple's response was that it 'isn't a matter of competition. It's a matter of security'.[10] The chairman of the US House Judiciary antitrust subcommittee has also voiced concerned over platforms using privacy as 'a shield for anti-competitive conduct', and exploiting their roles as 'de facto private regulators'.[11] And over the last decade, smartphone ecosystems providers, such as Apple and Google have become stricter in policing their platforms for the privacy and security relevant behaviour of apps.

Indeed, this role as regulator came to a head in 2020 during the Covid-19 pandemic, when platforms were centrally involved in shaping government responses to the pandemic, by setting the technical standards for Bluetooth-powered contact-tracing by mobile apps, and the associated collection of data.[12] For the first time, Google and Apple collaborated on a Bluetooth-based contact-tracing platform for building this functionality into their underlying operating systems. And in another first, both companies released application programming interfaces (APIs) that enable interoperability between Android and iOS devices using apps from public health authorities.[13] Apple and Google have been able to frame their collaborative efforts as based on 'user privacy and security' being 'central to the design'.[14] But this raised a larger question of how it is that Google and Apple largely decide upon privacy standards for public health apps, while governments look on from the side-lines.[15] Indeed, the French government had tried to publicly pressure Apple to change its iOS technical standards, which Apple refused, and even led to a government minister warning that '[w]e will remember that when time comes'.[16]

Whereas the platform providers may be applauded for taking the privacy of their users more seriously by the year and stepping up as de facto regulators in this regard, this raises a number of questions. First, how to reconcile a protective function for privacy with the reality that platforms have been at the forefront of eroding privacy in constructing data-intensive service ecosystems? Could mobile platforms end up weaponising their privacy governance function for anti-competitive purposes, thereby turning privacy and security into a foundation of their already dominant positions?[17] And what does the rise of platforms as privacy regulators mean for privacy law and policy more generally, including internationally?

Online platforms tend to have their own (first-party) personal data-intensive relations with users of their services. In this article, we build upon this reality, and examine the question of platforms as potential (privacy) regulators between other services and end-users, and the role of platforms (and ecosystems) in enforcing existing regulatory standards with respect to privacy in this relationship. We are in particular interested in the role of platforms of shaping (and disciplining) the privacy relevant behaviour of data-driven services and activity that are running on the platform, using the platform to engage with end-users.[18] Nooren et al. have described platforms such as Apple and Google as 'platforms of platforms', being platforms (or ecosystems) on which other platforms work,[19] or as Schwarz describes, panoplies of interconnected platforms.[20] They act as gatekeepers controlling vital assets for the functioning of other platforms. Van Loo describes this increased gatekeeper function as the rise of the enforcer-firm, that exist beyond the platform economy, to industries such as banking, oil, and pharmaceuticals.[21]

While we aim to contribute to the more general discussion about privacy and platforms, we concentrate our discussion and examples on the smartphone context, in which Apple and Google combine a technological platform (mobile operating systems) with a transaction platform (app markets), leading to the ecosystems of Apple (iOS-App Store), and Google (Android-Google Play). We also discuss the Facebook platform, given all of the legal and regulatory attention it has re-

[9] Jack Nicas, 'Apple Cracks Down on Apps That Fight iPhone Addiction' *The New York Times* (27 April 2019) < https://www.nytimes.com/2019/04/27/technology/apple-screen-time-trackers.html>.

[10] 'The facts about parental control apps' (*Apple*, 28 April 2019) <www.apple.com/newsroom/2019/04/the-facts-about-parental-control-apps/>.

[11] 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' *The Washington Post* (26 November 2019) <www.washingtonpost.com/technology/2019/11/26/apple-emphasizes-user-privacy-lawmakers-see-it-an-effort-edge-out-its-rivals>.

[12] See Reed Albergotti and Drew Harwell, 'Apple and Google are building a virus-tracking system. Health officials say it will be practically useless' *The Washington Post* (15 May 2020) <www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus/>.

[13] 'Apple and Google partner on COVID-19 contact tracing technology' (*Apple*, 10 April 2020) <www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>.

[14] 'Apple makes mobility data available to aid COVID-19 efforts' (*Apple*, 14 April 2020) <www.apple.com/newsroom/2020/04/apple-makes-mobility-data-available-to-aid-covid-19-efforts/>.

[15] An in-depth examination of the compatibility of Covid-19 contact-tracing apps and the right to privacy and data protection are outside the scope of this article. For an excellent discussion, see Hannah van Kolfschooten and Anniek de Ruijter, 'COVID-19 and privacy in the European Union: A legal perspective on contact tracing' (2020) 41 *Contemporary Security Policy* 278.

[16] Sudip Kar-Gupta and Michel Rose, 'France accuses Apple of refusing help with 'StopCovid' app' *Reuters* (5 May 2020) <www.reuters.com/article/us-health-coronavirus-france-tech/france-accuses-apple-of-refusing-help-with-stopcovid-app-idUSKBN22H0LX>.

[17] See Editorial, 'Why Does Apple Control Its Competitors?' *The New York Times* (2 May 2019) <www.nytimes.com/2019/05/02/opinion/apple-app-store-iphone.html> and Ronan Ó Fathaigh and Joris van Hoboken, 'European Regulation of Smartphone Ecosystems' (2019) 5 *European Data Protection Law Review* 476.

[18] Pieter Nooren, Nicolai van Gorp, Nico van Eijk, and Ronan Ó Fathaigh, 'Should We Regulate Digital Platforms? A New Framework for Evaluating Policy Options' (2018) 10 *Policy & Internet* 264, 272.

[19] Ibid., 275.

[20] Andersson Schwarz, 'Platform Logic: An Interdisciplinary Approach to the Platform-Based Economy' (2017) 9 *Policy & Internet* 374, 380.

[21] Rory Van Loo, 'The New Gatekeepers: Private Firms as Public Enforcers' (2020) 106 *Virginia Law Review* 467. See also, José Van Dijck, 'Seeing the forest for the trees: Visualizing platformization and its governance' (2020) *New Media & Society* 1, which proposes a helpful tree metaphor to understand the hierarchical and interdependent structures of platform ecosystems.

ceived, and Facebook's mobile tracking software (called Facebook SDK) being embedded in many of the most popular apps available for iOS and Android.[22]

One of the starting points for this article is that the position of platforms in current privacy law and policy is not well-developed. Our first goal is to address this gap and document the rise of platforms as privacy regulators. How do platforms fit into current privacy law and policy? What are the ways in which platforms act as privacy regulators, which functions do they exercise and on what basis? Our second question is how should privacy law and policy respond to the rise of platforms as privacy regulators? And how can and should platforms be incorporated in existing and upcoming regulatory frameworks?

Certainly, privacy is not the first or only regulatory interest that platforms have been asked, required or incentivised to assume a role in regulating.[23] Most notably, legal frameworks for the policing of illegal and harmful content online (copyright, hate speech, indecency, etc.) have relied on online intermediaries for more than two decades.[24] While intermediary liability laws put some limits on enforcement of the law, a combination of market incentives, reputational pressure, and threats to regulate have turned online platforms into increasingly dominant regulators of speech.[25] Indeed, the European Commission's recently-proposed Digital Services Act (DSA) is premised upon the immense power platforms have over online speech, and thus proposes new responsibilities for platforms in regulating speech on their platforms (such as obligations to provide reasons to users for removing content).[26] Further, a recent report from the European Commission concluded that dominant platforms have a 'responsibility to ensure that their rules do not impede free, undistorted, and vigorous competition without objective justification'.[27] Together with the DSA, the Commission also recently proposed a Digital Markets Act (DMA), which is aimed at ensuring contestable and fair markets in the digital sector.[28] It includes new obligations for so-called 'gatekeeper' platforms, including prohibitions on treating their own products more favourably in ranking services;[29] and allowing the installation and use of third party software apps or apps stores using, or interoperating with, the operating systems of these gatekeepers.[30] In line with the rise of platform power, political pressure from the media and by civil society actors is aimed directly at platform policies as well.[31]

In the next section (Section 2), we review the current position of platforms (smartphone platforms in particular) in privacy law and policy in the EU and US. In Section 3, we analyse the privacy governance functions of platforms in more depth. After discussing how platforms create and govern infrastructures for access to personal data, we distinguish and discuss the three layers of privacy governance by platforms: technical standards, contractual standards, and enforcement. In Section 4, we move to discuss higher-level privacy governance functions. After highlighting the connection between platforms and the creation of trust, we discuss their potential role in (a) bridging transnational regulatory requirements, (b) engaging as stakeholders in regulatory discussions and as sources of policy-relevant information about the functioning of the relevant ecosystems, and (c) striking a balance between respect for data privacy in data-driven environments and the optimization of business opportunities connected to the platform and underlying data. Section 5 discusses the potential value of disclosure requirements on platforms with respect to their regulatory privacy function. Finally, Section 6 concludes.

2. Platforms (as platforms) under existing privacy law

One of the starting points for this article is that the position of platforms in current privacy law and policy is not well-developed. In the following, we briefly review the state of play in Europe and the United States. Notably, the GDPR does not contain any platform-specific provisions. It imposes its main set of obligations on so-called data controllers. These are the entities that determine the purposes and means of personal

[22] Nick Statt, 'Why a small Facebook bug wreaked havoc on some of the most popular iOS apps' (*The Verge*, 7 May 2020) <www.theverge.com/2020/5/7/21250689/facebook-sdk-bug-ios-app-crash-apple-spotify-venmo-tiktok-tinder>.

[23] For a discussion see, Orly Lobel, 'The Law of the Platform' (2016) 101 *Minnesota Law Review* 87, 153. See also Cohen (n 7); Natali Helberger, Jo Pierson and Thomas Poell, 'Governing online platforms: From contested to cooperative responsibility' (2018) 34 *The Information Society* 1; and Robert Gorwa, 'What is platform governance?' (2019) 22 *Information, Communication & Society* 854.

[24] See Gillespie (n 8) 254-278; Jack M. Balkin, 'Free Speech Is a Triangle' (2018) 118 *Columbia Law Review* 2011; Jonathan Zittrain and John G. Palfrey, *Access Denied: The Practice and Policy of Global Internet Filtering* (Oxford Internet Institute Research Report No. 14, 2007); and Christina Angelopoulos et al., *Study of fundamental rights limitations for online enforcement through self-regulation* (Institute for Information Law, University of Amsterdam 2016).

[25] See recently, 'Christchurch Call to Eliminate Terrorist & Violent Extremist Content Online' (New Zealand Ministry of Foreign Affairs and Trade, 2020) <www.christchurchcall.com/call.html>. See Jack Nicas and Davey Alba, 'Amazon, Apple and Google Cut Off Parler, an App That Drew Trump Supporters' *The New York Times* (13 January 2021 <www.nytimes.com/2021/01/09/technology/apple-google-parler.html> (detailing how Apple and Google removed the Parler social network app from both the App Store and Play Store for not sufficiently policing users' content).

[26] Commission, 'Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM(2020) 825 final, Article 15.

[27] See Crémer, de Montjoye and Schweitzer (n 8).

[28] Commission, 'Proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act)' COM/2020/842 final.

[29] Ibid. art 6(d).

[30] Ibid. art 6(c). However, a gatekeeper 'shall not be prevented from taking proportionate measures to ensure that third party software applications or software application stores do not endanger the integrity of the hardware or operating system provided by the gatekeeper' (art 6(c)).

[31] See Dhruv Mehrotra and Kashmir Hill, 'Airbnb Doesn't Want White Nationalists On Its Platform—But How Hard Is It Looking for Them?' (*Gizmodo*, 5 April 2019) <https://gizmodo.com/airbnb-doesnt-want-extremists-on-its-platform-but-how-h-1833844785>.

data processing operations.[32] Platforms (as platforms) would typically not be the primary entity in the networked-service environment to determine the purposes and means of the processing of personal data by business users. They offer the possibility for services to process personal data of the platform's end-users. On the other hand, data processors process personal data on behalf of a controller,[33] and as Mahieu, van Hoboken and Asghari point out, processors are secondary actors (relative to controllers) under the GDPR.[34]

Mahieu, van Hoboken and Asghari also remark that the basic elements of the data protection legal framework – processors and controllers – have been 'carried forward without substantial changes' from the previous Data Protection Directive.[35] The European Data Protection Board (EDPB) similarly stated in 2020 that the concepts of controller and processor under the GDPR 'have not changed compared' to the DPD, and 'overall, the criteria for how to attribute the different roles remain the same'.[36] However, it must be recognised that processors do have new obligations under the GDPR, and the EDPB considers that the GDPR imposes 'obligations directly upon processors'.[37] These include processors ensuring that 'persons authorised to process the personal data have committed themselves to confidentiality';[38] processors required to 'maintain a record of all categories of processing activities carried out on behalf of a controller';[39] and processors required to implement 'appropriate technical and organisational measures' to ensure security of processing under Article 32.[40] Further, as Russo et al. have examined, the GDPR may also be applicable to cloud service providers, and certain platforms could be classified as a type of cloud service provider, such as platform-as-a-service (PaaS) or software-as-a-service (SaaS).[41]

Notably, two particular aspects of the GDPR are worth highlighting here. First, the provisions on data protection by design and default (Article 25), and the implications of these provisions for producers of information systems, in contrast to users. Second, recent case law on joint responsibility may bring platforms more directly under the scope of the GDPR's primary obligations on data controllers to ensure lawful, fair and transparent processing of personal data. The obligation of data protection by design and default applies to data controllers under Article 25 GDPR. As noted by regulators and commentators, this focus on controllers means that it does not speak directly to the developers and producers of technologies and services for the processing of personal data.[42] The European Data Protection Supervisor, for example, in its opinion on Article 25, acknowledges that the 'serious limitation' of the obligations under Article 25, in that 'they apply only to impose an obligation on controllers and not to the developers of those products and technology used to process personal data'.[43] What remains is the non-binding encouragement on producers and developers of relevant technologies to take the necessary steps and make the relevant design decisions to facilitate compliance by the actual controllers. Specifically, Recital 78 GDPR provides that '[*w*]hen developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations'.[44]

Recent case law by the EU Court of Justice (CJEU) on joint responsibility under the GDPR complicates the legal analysis of responsibility for platforms under European data protection law. Informed by its principle of effective and complete protection, the CJEU adopts an expansive notion of 'joint responsibility' between platforms and their business users.[45] Specifically, the CJEU concludes that the operator of a Facebook fan page is jointly responsible for the processing of personal data of visitors of the fan page by Facebook, even though the fan page does not have access to the personal data itself.[46] Similarly, in the related *Fashion ID* case, the CJEU held that a website that embeds a social plugin (such as a Facebook like button) for the processing of personal data by a third-party service, can be considered to be a joint controller under the GDPR.[47] To sum-

[32] For a recent discussion of the concept of controller and how to apply it in networked service-settings, see René Mahieu, Joris van Hoboken, and Hadi Asghari, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe' (2019) 10 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 84.

[33] GDPR, art 28.

[34] Mahieu, van Hoboken, and Asghari (n 32), 88.

[35] Ibid.

[36] European Data Protection Board, *Guidelines on the concepts of controller and processor in the GDPR* (EDPS Guidelines 7/2020), para 11.

[37] Ibid. para 91.

[38] GDPR, art 28(3)(b).

[39] GDPR, art 30(2).

[40] GDPR, art 32.

[41] See Barbara Russo et al., 'Cloud Computing and the New EU General Data Protection Regulation' (2018) 5 *IEEE Cloud Computing* 58. See also Seda Gürses and Joris van Hoboken, 'Privacy after the Agile Turn' in Evan Selinger, Jules Polonetsky and Omer Tene (eds) *The Cambridge Handbook of Consumer Privacy* (CUP 2018); Christopher Millard, *Cloud Computing Law* (OUP 2013); and Art 29 WP, 'Opinion 05/2012 on Cloud Computing' WP 196.

[42] See Lee Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 *Oslo Law Review* 105.

[43] See European Data Protection Supervisor, *Preliminary Opinion on privacy by design* (EDPS Opinion 5/2018) para 37. See also European Union Agency for Network and Information Security, *Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR* (ENISA 2017).

[44] GDPR, recital 78.

[45] Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein*, EU:C:2018:388, Judgment of 5 June 2018.

[46] For a detailed discussion, see Mahieu, van Hoboken, and Asghari (n 32). See also Charlotte Ducuing, Jessica Schroers, and Els Kindt, 'The Wirtschaftsakademie Fan Page Decision: A Landmark on Joint Controllership – A Challenge for Supervisory Authorities Competences' (2018) 4 *European Data Protection Law Review* 547.

[47] Case C-40/17, *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*, ECLI:EU:C:2019:629, Judgment of 29 July 2019. See René Mahieu and Joris van Hoboken, 'Fashion-ID: Introducing a phase-oriented approach to data protection?' (*European Law Blog*, 30 September 2019 <https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/>.

marise, platforms may be sufficiently involved, through the design and governance of personal data processing opportunities and tools, to be held jointly responsible for the processing of (certain) personal data by their business users.

In terms of regulatory guidance in Europe concerning the smartphone ecosystem in particular, the previous Article 29 Data Protection Working Party (Art 29 WP), now superseded by the European Data Protection Board (EDPB), issued guidance on mobile apps.[48] Notably, in addition to guidance for app developers, it included some guidance for operating system (OS) providers, device manufacturers, and app stores. The Art 29 WP recognised that OS providers, device manufacturers, and app stores, have an 'important responsibility' to provide safeguards for protecting the privacy of app users, including 'appropriate mechanisms' to inform users about what data apps can access, and providing 'appropriate settings' for users to change the parameters of such data processing.[49] These includes that OS and device manufactures must update their APIs, app store rules and user interfaces to offer users sufficient control to exercise valid consent over the data processed by apps; and offer granular access to data, sensors and services, in order to ensure that app developers can only access data necessary for the app.[50] Further, the Art 29 WP also briefly addressed app stores in its guidelines on transparency under the GDPR, and recommended that an app's privacy notice should be made available in app stores before download.[51]

Further, the EU's proposed ePrivacy Regulation contains a provision that could require browsers and platforms to ensure appropriate privacy settings and defaults with respect to tracking by websites and mobile apps. There has been a good deal written about this proposal,[53] and is designed to replace the current ePrivacy Directive, which lays down rules for ensuring privacy and confidentiality of electronic communications.[54] The ePrivacy Directive is perhaps best known for its rule on consent and the storing of cookies on users' equipment.[55] In the new proposals, Article 10 regulates software 'permitting electronic communications, including the retrieval and presentation of information on the internet' in terms of privacy settings and defaults for third-party tracking. Like the rest of the proposal, which has been stalled by the Member States after the adoption of the European Parliament's report, the provision is contested and may not be adopted in a final version of the Regulation. If we look at the United States, platforms similarly do not have a formal status in any existing data privacy statutes, but they have received significant attention in regulatory guidance and enforcement actions. The FTC's central recommendations on effectuating transparency in the mobile context are directed at platforms.[57] The FTC concluded that platforms are 'gatekeepers to the app marketplace and possess the greatest ability to effectuate change with respect to improving mobile privacy disclosures'.[58] It recommended platforms implement just-in-time disclosure and affirmative consent mechanisms for sensitive data, develop privacy dashboards, and consider the use of icons. It also recommended that platforms impose contractual requirements on apps in view of privacy and reasonably enforce these provisions, be more transparent about their review process for apps, and develop do-not-track settings for the mobile environment.[59]

The recommendations from the FTC built on guidance of (then) California Attorney General, Kamala D. Harris, on mobile privacy,[60] and a Joint Statement of Principles issued by Harris and agreed to by leading US-based mobile platform companies.[61] The Joint Statement is particularly interesting in how it strategically seeks to leverage the power of mobile platforms ('Mobile Apps Market Companies') to increase protection of user privacy between apps and mobile users. The participating companies, including Apple, Google, Microsoft

[48] Art 29 WP, 'Opinion 02/2013 on apps on smart devices' (2013) WP 202.

[49] Ibid. 11.

[50] Ibid. 29.

[51] Art 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 rev.01.

[52] Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM(2017) 10 final. Notably, the provision on privacy settings (Article 10) has been removed from the version approved by the Council of the European Union (see Interinstitutional File: 2017/0003(COD), Doc No. 6087/21, 10 February 2021).

[53] See Giovanni Buttarell, 'The Commission Proposal for a Regulation on ePrivacy: Why Do We Need a Regulation Dedicated to ePrivacy in the European Union?' (2017) 3 *European Data Protection Law Review* 155; Frederik Zuiderveen Borgesius, Joris van Hoboken, Ronan Ó Fathaigh, Kristina Irion, and Max Rozendaal, *An assessment of the Commission's Proposal on Privacy and Electronic Communications* (Study for the LIBE Committee, European Union 2017); Joris van Hoboken and Frederik Zuiderveen Borgesius, 'Scoping Electronic Communication Privacy Rules: Data, Services and Values' (2015) 6 JIPITEC 198.

[54] 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.

[55] See Eleni Kosta, 'Peeking into the cookie jar: the European approach towards the regulation of cookies' (2013) 21 *International Journal of Law and Information Technology* 380; and Vagelis Papakonstantinou and Paul de Hert, 'The Amended EU Law on ePrivacy and Electronic Communications after its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights' (2011) 29 *John Marshall Journal of Computer and Information Law* 29.

[56] For more detailed discussion, see Ó Fathaigh and Van Hoboken (n 17).

[57] FTC, *Mobile Privacy Disclosures: Building Trust Through Transparency* (FTC Staff Report, 2013).

[58] Ibid. 14.

[59] The FTC has also issued guidance on security for developers highlighting the role of platforms (see 'App Developers: Start with Security' (*FTC*, 17 May 2017) <www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security>); and guidance for mobile health app developers, which did not address platforms (see 'Mobile Health App Developers: FTC Best Practices' (*FTC*, 4 April 2016) <www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices>).

[60] Attorney General Kamala D. Harris, *Privacy on the Go: Recommendations for the Mobile Ecosystem* (California Department of Justice 2013).

[61] 'Joint Statement of Principles' (State of California, Office of the Attorney General, 22 February 2012) <https://oag.ca.gov/system/files/attachments/press_releases/Apps_signed_agreement_0.pdf>

and Amazon, agreed to 'creative and forward-looking solutions that give consumers greater transparency and control over their personal data without unduly burdening innovative mobile platforms and application developers', while clarifying that it does 'not seek to impose any binding obligations on the platforms or affect existing obligations under law'.[62] Its principles develop the terms of service as instruments of privacy regulation, including a promise to allow for reporting and enforcement related to non-compliance of apps with relevant contractual restrictions by platforms, in addition to non-compliance with the law.[63] In summary, the agreement effectively enlists mobile platforms as (voluntary) enforcement agencies with respect to California's privacy laws.[64]

Platforms also feature in the FTC's enforcement actions in the last decade on the basis of the FTC's role in policing deceptive and unfair trade practices. These enforcement actions show that platforms may act deceptively in their relation between service and end-users. Two counts in the original FTC complaint from 2012 against Facebook concerned its role as a platform for apps, and its role as a platform for advertisers. The complaint charged that Facebook as a platform engaged in deceptive practices when, in contrast to public statements, apps 'could access profile information that was unrelated to the Application's purpose or unnecessary to its operation'.[65] Further, the FTC consent decree with Apple in 2014 included changes to the App Store's in-app charges' mechanism and how consent is gathered.[66] In relation to mobile ad networks, in 2016, the FTC reached a settlement with mobile ad network InMobi on location tracking practices.[67] Notably, inMobi's practices circumvented measures taken by the mobile platforms to protect users from having their location data tracked without consent (through operating systems permission architectures and enforcement of terms of service).[68] Thus, the platforms' role as privacy regulators through terms of service gained additional backing by the FTC.

Of the different platforms, Facebook has been amongst the most aggressive in opening up its platform for data-driven business practices without properly informing its end-users. This is reflected in a series of scandals of apps operating well beyond the use of Facebook for adding social features, beginning with Beacon and Cambridge Analytica more recently.[69] Whereas the permissiveness of the Facebook platform for data harvesting was widely known in expert circles, the Cambridge Analytica scandal highlighted the permissiveness of the Facebook platform for apps to harvest the data of Facebook users and use these data in controversial political microtargeting operations in the US elections.[70] Specifically, the Facebook platform made it possible for the 'This Is Your Digital Life' app to harvest data from users that installed the app, as well as data of their friends. The harvesting reportedly included sensitive data of users such as private messages.[71] In 2019, Facebook agreed to pay a record-breaking $5 billion penalty to settle FTC charges that it deceived its users about its privacy practices, and violated its 2012 consent decree.[72] The FTC also reached a 20-year settlement with Facebook, which included Facebook exercising greater oversight over third-party apps, including by terminating app developers that fail to certify that they are in compliance with Facebook's platform policies or fail to justify their need for specific user data.[73]

Partly as a result of the Cambridge Analytica scandal, the US Senate has placed significant focus on platforms in its recent hearings on consumer privacy. The US Senate hearings on 'Cambridge Analytica, data privacy, use and abuse of data' focused in detail on the Facebook platform and its failure to protect users against abusive third-party services.[74] Both Apple and Google made submissions to the Senate Judiciary Committee on the operation of their app stores and user privacy mechanisms.[75]

Finally, the new California Consumer Privacy Act came into effect in 2020, and similar to the GDPR, does not explicitly address platforms.[76] The Act includes new rights for consumers, such as right to delete personal information held by busi-

[62] Ibid.
[63] Ibid.
[64] For a more detailed discussion of the California AG's office's efforts in the area of mobile apps, as an important example of AG privacy policymaking, see Danielle Keats Citron, 'The Privacy Policymaking of State Attorneys General' (2017) 92 *Notre Dame Law Review* 691, 765-767.
[65] *In the Matter of Facebook, Inc.* (Complaint) Federal Trade Commission Docket No. C-4365 (10 August 2012), 10.
[66] *In the Matter of Apple, Inc.* (Decision and Order) Federal Trade Commission Docket No. C-4444 (27 March 2014).
[67] Nithan Sannappa and Lorrie Cranor, 'A deep dive into mobile app location privacy following the InMobi settlement' (*FTC*, 9 August 2016) <www.ftc.gov/news-events/blogs/techftc/2016/08/deep-dive-mobile-app-location-privacy-following-inmobi-settlement>.
[68] Ibid.
[69] For a discussion of the FTC's enforcement history, see David C. Vladeck, 'Facebook, Cambridge Analytica, and the Regulator's Dilemma: Clueless or Venal?' (*Harvard Law Review Blog*, 4 April 2018) <https://blog.harvardlawreview.org/facebook-cambridge-analytica-and-the-regulators-dilemma-clueless-or-venal/>.
[70] Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach' *The Guardian* (17 March 2019) <www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.
[71] Ibid.
[72] *In the Matter of Facebook, Inc.* (n 2).
[73] Ibid.
[74] See 'Facebook, Social Media Privacy, and the Use and Abuse of Data' (US Senate Commerce Committee Hearing, 10 April 2018) <www.commerce.senate.gov/2018/4/facebook-social-media-privacy-and-the-use-and-abuse-of-data> 'Examining Safeguards for Consumer Data Privacy' (US Senate Commerce Committee Hearing, 26 September 2018) <www.commerce.senate.gov/2018/9/examining-safeguards-for-consumer-data-privacy> and 'Policy Principles for a Federal Data Privacy Framework in the United States' (US Senate Commerce Committee Hearing, 27 February 2019) <www.commerce.senate.gov/public/index.cfm/2019/2/policy-principles-for-a-federal-data-privacy-framework-in-the-united-states>.
[75] See 'Letter to Senator Charles E. Grassley' (*Apple*, 3 July 2018) <www.judiciary.senate.gov/download/apple-to-grassley_-data-privacy>; and 'Letter to Charles E. Grassley' (*Google*, 25 April 2018) <www.judiciary.senate.gov/imo/media/doc/2018-04-25%20Google%20to%20CEG%20-%20Data%20Privacy.pdf>.
[76] California Consumer Privacy Act of 2018, Civil Code, section 1798.100. See, Stuart L. Pardau, 'The California Consumer Pri-

nesses, the right to know what personal information is collected, used, shared or sold, and the right to opt-out of the sale of personal information. Notably, the definition of 'homepage' does include an app's 'platform page', and this implies that app distribution platforms would have to make it possible for apps to display an opt-out for the sale of a consumer's personal information.[77] While the law does not explicitly place obligations upon platforms in relation to app developers, and other business users, large platforms have been putting in place mechanisms to assist their business users comply with the law. For example, Facebook, while insisting that businesses that use its platform 'reach their own decisions on how to best comply with the law', nonetheless help business users 'manage their compliance', with Facebook making 'updated contractual commitments available' to business partners.[78]

3. Privacy Governance Functions of Platforms

The previous section demonstrated that platforms are not specifically targeted under privacy laws in the United States and Europe, above and beyond the obligations placed on other companies. In other words, privacy law does not explicitly take account of the role platforms play in the data practices of other companies that use their platforms. In this section, we build upon this legal reality,[79] and analyse the privacy governance functions of smartphone platforms. After discussing how such platforms create and govern infrastructures for access to personal data, we distinguish and discuss three layers of privacy governance: technical standards, contractual standards, and enforcement.

3.1. *Platforms and the data economy*

Platforms create and govern the infrastructures for access to personal data. And because today's digital economy rests so much on the monetisation of personal data, platforms have become an essential pillar in the data economy. As Cohen notes, platforms provide a combination of access (e.g. to consumers) and legibility (e.g. of consumers), and crucially, data collection and use are central ingredients for both.[80] Policymakers have recognised this reality, with the European Commission emphasising that a specific feature of platforms is the ability to facilitate new forms of conducting business based on collecting and processing large amounts of data.[81] Indeed, platforms are able to capture significant value through 'data accumulation', and 'creating new strategic dependencies'.[82]

Notably, outside the area of privacy law, and when it comes to competition law and policy, policymakers recognise the gatekeeper and regulatory role of platforms.[83] A 2019 study for the European Commission examining how competition policy should evolve in the digital age explicitly framed online platforms as regulators.[84] The authors noted that a 'special feature of the intermediation function that platforms frequently fulfil is that it is accompanied by a rule-setting function: many platforms, in particular marketplaces, actually act as regulators, setting up the rules and institutions through which their users interact'.[85] The authors also argued that 'because of this function as regulators, the operators of dominant platforms have a responsibility to ensure that competition on their platforms is fair, unbiased, and pro-users'.[86] Further, dominant platforms that set up marketplaces must 'ensure a level playing field' in these marketplaces and must not use 'rule-setting power to determine the outcome of the competition'.[87] Similarly, the European Commission's 2020 European strategy for data has also recognised the competition concerns relating to platforms' control over access to data. This 'data advantage' allows platforms to set the rules and unilaterally impose conditions for access and use of data, according to the Commission.[88]

The specific platforms we are concerned with in this article, namely the dominant smartphone ecosystem providers, are particularly prone to capturing this data advantage through their control of smartphone operating systems (iOS and Android), access to the mobile app marketplaces (App Store and Google Play Store), access to the app developer platforms (Apple Developer Program and Google Play Console), and the manufacture of smartphones (iPhone and Pixel). Indeed, even in relation to non-Google manufactured smartphones, Google was found in 2018 to have beached EU antitrust law by preventing device manufacturers from using any alternative version of Android that was not approved by Google ('Android forks').[89] Both also set the rules for app monetisation mechanisms, whether through in-app purchases or mobile advertising. Indeed, platforms not only govern the types of access to user data (through the platform or direct access), but also facilitate data access and explain how to best use the platform and the data that becomes accessible.[90] In

vacy Act: Towards a European-Style Privacy Regime in the United States' (2018) 23 *Journal of Technology Law and Policy* 68.

[77] California Consumer Privacy Act of 2018, Civil Code, section 1798.100.

[78] 'Ready for California's New Privacy Law' (*Facebook*, 12 December 2019) <https://about.fb.com/news/2019/12/californias-new-privacy-law/>.

[79] See Ronan Ó Fathaigh, Joris van Hoboken, and Nico van Eijk, 'Mobile Privacy and Business-to-Platform Dependencies: An Analysis of SEC Disclosures' (2018) 14 *Journal of Business and Technology Law* 49.

[80] Cohen (n 7) 137.

[81] Commission, 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe' (Communication) COM(2016) 288 final.

[82] Ibid. s. 2.

[83] See also, OECD, *Measuring the Digital Transformation: A Roadmap for the Future* (OECD Publishing 2019), and OECD, *An Introduction to Online Platforms and Their Role in the Digital Transformation* (OECD Publishing 2019).

[84] Crémer, de Montjoye and Schweitzer (n 8).

[85] Ibid. 60.

[86] Ibid. 61.

[87] Ibid. 62.

[88] Commission, 'Shaping Europe's digital future' (Communication) 19 February 2020 <http://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf>.

[89] *Google Android* (Case AT.40099) Commission Decision C(2018) 4761 final.

[90] See Ronan Ó Fathaigh, Joris van Hoboken, and Nico van Eijk, 'Data Privacy, Transparency and the Data-Driven Transformation

the sections that follow, we tease out the specific role these platforms play.

3.2. *Technical standards*

Smartphones and mobile apps present unique risks for user privacy that have been well-documented.[91] Crucially, through sensors and on-device storage of data, smartphones have access to an array of the most personal information, are constantly running, and almost always on the person of a user. Smartphones have an array of sensors, such as GPS, WiFi, Bluetooth, accelerometers, gyroscopes, as well as microphones and cameras.[92] Smartphones also emit various signals containing unique identifiers, which can be captured for the purpose of tracking. As the European Union's agency for cybersecurity ENISA has found, smartphone users can be 'easily' identified and authenticated from 'smartphone-acquired signals'.[93] As the FTC has also warned, smartphones facilitate 'unprecedented amounts of data collection', which can reveal sensitive and highly-personal information.[94] And of course, tracking of location data can pose a serious threat to the privacy of users.[95]

Given the risks that smartphones present for user privacy, Apple and Google have put in place technical mechanisms to put conditions on the data that app providers can access when operating on people's smartphones. As such, Apple and Google build the architectures that determine the conditions under which different sources of data can be collected from smartphones by apps and related services. These sorts of mechanisms, in particular the various APIs integrated in the operating system, recently received particular attention during the Covid-19 pandemic, when the French government asked Apple to loosen the technical standards in the iOS operating system which prevents Bluetooth technology from running constantly in the background.[96]

At a fundamental level, mobile operating systems such as iOS and Android use what is called permission architecture for apps accessing various functions of a mobile device and data.[97] Both Apple and Google state that the purpose of permissions is to protect user privacy. Android functions with so-called normal and dangerous permissions. Normal permissions include access to data or functions that are considered to entail little risk to users' privacy, such as setting the time zone, and Android automatically grants apps such permissions at install time. Dangerous permissions are those that carry a risk to user privacy, or the operation of other apps, such as access to contacts, location, or Bluetooth. Apps can only access such permissions where the user has, through the respective mechanisms built into the permission architecture, allowed it. Google itself decides upon what functions, capabilities, features and data are normal and dangerous permissions. Similarly, iOS uses a permission architecture, and distinguishes between entitlements and permissions.[98] Entitlements allow specific capabilities, such push notifications, while permissions allow access to certain personal data such as location, calendar, contact information, or photos. When an app is running and a permission is required by the app, users are prompted to allow or deny permissions. Again, Apple decides what functions and data are entitlements or permissions. Notably, there is considerable critique of the current permission architecture, including that apps request permissions that are not necessary for their core functionality.[99]

Importantly, both Apple and Google implement a technical feature called app sandboxing. Apple describes this technical feature as isolating user data in one app from other apps, as well as protecting user data from unwanted access by other apps. This 'privacy by design technique' isolates ('sandboxes') apps within containers that hold only data that the app itself generates.[100] Similarly, Google implements an app sandbox, to ensure apps cannot interact with each other and have limited access to the operating system.[101]

Second, some platforms not only govern access to smartphone capabilities and data, but also make software freely available for app providers to engage in data analytics, or to sell personalised advertising. Prominent examples are Google's Firebase software development kit (SDK), which incorporates Google analytics software, and is made available for not only Android apps, but also iOS apps. Similarly, Google, Amazon, and Facebook all make their advertising and audience-measuring mobile software freely available to app developers using Android and iOS (e.g., Google Mobile Ads, Amazon Mobile Ads, or Facebook Audience Network). Further, social media integration with apps is facilitated by both Apple and Google, and allows use of SDKs such as Facebook SDK for iOS, which includes Facebook Analytics, Facebook Login, and its Graph API.[102] The Facebook Audience Network API serves ads on iOS and Android apps and mobile websites, and allows use of all Facebook's targeting options to find an audience within those mobile apps and mobile websites.[103] Google also offers its mobile ad advertising platform to iOS develop-

of Games to Services' (2018) *IEEE Games, Entertainment, Media (GEM)* 136 <https://doi.org/10.1109/GEM.2018.8516441>.

[91] See FTC (n 57); Jennifer M. Urban, Chris Jay Hoofnagle, and Su Li, 'Mobile Phones and Privacy' (Berkeley Center for Law and Technology Research Paper 2012); and Anjanette Raymond, Jonathan Schubauer, and Dhruv Madappa, 'After Over-Privileged Permissions: Using Technology and Design to Create Legal Compliance' (2019) 15 *Journal of Business and Technology Law* 67.

[92] ENISA (n 43) 11.

[93] Ibid.

[94] FTC (n 57).

[95] Commission Proposal (n 52), recital 20.

[96] Helene Fouquet, 'France Says Apple Bluetooth Policy Is Blocking Virus Tracker' *Bloomberg* (20 April 2020) <www.bloomberg.com/news/articles/2020-04-20/france-says-apple-s-bluetooth-policy-is-blocking-virus-tracker> and Alex Hern, 'France urges Apple and Google to ease privacy rules on contact tracing' *The Guardian* (21 April 2020) <www.theguardian.com/world/2020/apr/21/france-apple-google-privacy-contact-tracing-coronavirus>.

[97] See ENISA (n 43) 42-46.

[98] Apple (n 75) 6.

[99] ENISA (n 43) 43.

[100] Apple (n 75) 3.

[101] 'Application Sandbox' (*Android*) <https://source.android.com/security/app-sandbox>.

[102] 'Facebook SDK for iOS' (*Facebook*) <https://developers.facebook.com/docs/ios/getting-started/>.

[103] 'Marketing API' (*Facebook*) <https://developers.facebook.com/docs/marketing-apis>.

ers, called Google Mobile Ads SDK. Notably, the default integration of the Mobile Ads SDK collects information such as device information and location information.[104]

Crucially, platforms such as Google build some amount of compliance tools into their software such as Firebase in order to assist app developers comply with laws such as the GDPR or the California Consumer Privacy Act.[105] In a similar vein, its Mobile Ads SDK has an in-built 'Child-directed' setting, which allows an app developer to indicate to Google to treat content as child-directed when an ad request is made.[106] Google also offers a Consent SDK which can be used with its Mobile Ads SDK (including for iOS), and is designed to help developers meet their duties under both the ePrivacy Directive and the GDPR.[107] Similarly, Facebook's SDK for iOS and Android has in-built tools to assist developers comply with the GDPR, including an option to delay automatic event collection within an app until the user has gone through the 'in-app consent flow'.[108] Beyond its contractual rules for developers, Facebook also provides in-built technical mechanisms for its advertising software (Facebook Audience Network SDKs) to facilitate compliance with COPPA. Developers can include the 'isChild-Directed' flag within the software to ensure Facebook will only serve ads to non-US users of that app through its services.[109]

Notably, platforms also build the architecture to support privacy policies being offered in particular places, such as within apps and app store listings. For example, in 2018, Apple introduced a new requirement that all apps, irrespective of whether the app collect data, must include a privacy policy link within the app in an easily accessible manner. The privacy policy must detail what data is collected, and is not limited to personal data.[110] Google also requires a privacy policy within an app where the app 'handles sensitive user data',[111] and Facebook requires developers to link to a privacy policy in any app store that allows this.[112] But the question arises whether privacy policies are accurately describing the data being collected by apps, such as documented in a 2019 study on depression and anti-smoking apps.[113] The study found that of the apps technically examined, 81% transmitted data for advertising and marketing purposes or analytics to Google and Facebook, but less than half of these apps accurately disclosed this in their privacy policies. In another recent technical examination over 5000 Android apps, the study found that a majority of these apps were potentially in violation of COPPA as a result of the use of third-party SDKs. It also found that nearly a fifth collected identifiers or other personally identifiable information through the use of SDKs whose terms of service prohibit use in child-directed apps.[114]

Finally, platforms have also been putting some efforts into combatting over-permissions, by using machine learning to detect apps that seek permission requests that are not related to the app's core functionality. Google emphasised to the US Senate its use of machine learning, with its tool Google Play Protect, which is pre-installed on all Google-licensed Android devices and continuously monitors users' phones, along with apps in Play and across the Android ecosystem. The tool is said to scan more than 50 billion apps per day, and notably, over 60% of all 'potentially harmful' apps were detected via machine learning in 2017.[115]

3.3. *Contractual standards*

In addition to setting the technical standards for the use of smartphone functionality and collection of data, platforms impose another layer of governance through contractual terms. Platforms use this layer of governance to incorporate their own terms of service, and also rules that derive from laws on consumer protection, anti-discrimination, privacy and data protection.[116] Thus, some protections for user privacy are not technically enforced, but set through contract and terms of service.

First, platforms impose a general requirement on app providers to comply with relevant local laws. For example, both Apple and Google require developers to ensure that apps are compliant with local laws.[117] Second, platforms implement rules on mobile device identification, use of certain unique identifiers, and other types of data. Apple allows app providers and contracted third-parties to use a device's unique advertising identifier, and any information obtained through the use of the advertising identifier, but only for the purpose of

[104] 'Mobile Ads SDK' (*Google Ad Mob*) <https://developers.google.com/ad-manager/mobile-ads-sdk/>.

[105] 'Privacy controls in Google Analytics' (*Google*) <https://support.google.com/analytics/answer/9019185?hl=en>.

[106] 'Targeting' (*Google AdMob*) <https://developers.google.com/ad-manager/mobile-ads-sdk/ios/targeting>.

[107] 'Requesting Consent from European Users' (*Google AdMob*) <https://developers.google.com/admob/ios/eu-consent>.

[108] 'FB SDK Best Practices for GDPR Compliance' (*Facebook*) <https://developers.facebook.com/docs/app-events/gdpr-compliance>.

[109] 'Information for Child-Directed Apps and Services' (*Facebook*) <https://developers.facebook.com/docs/audience-network/coppa/>.

[110] 'Privacy Policy Reminder' (*Apple*, 31 August 2018) <https://developer.apple.com/news/?id=08312018a>.

[111] 'Google Play Developer Content Policies' (*Google*, 16 April 2020) <https://play.google.com/about/developer-content-policy-print/>.

[112] 'Facebook Platform Policy' (*Facebook*) <https://developers.facebook.com/policy/>.

[113] See Kit Huckvale, John Torous, and Mark E. Larsen, 'Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation' (2019) *JAMA Network Open* 2(4):e192542 <http://doi:10.1001/jamanetworkopen.2019.2542> and Rachel Siegel, 'Smoking and depression apps are selling your data to Google and Facebook, study finds' *The Washington Post* (22 April 2019) <www.washingtonpost.com/business/2019/04/22/smoking-depression-apps-are-selling-your-data-google-facebook-study-finds/>.

[114] Irwin Reyes et al., '"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale' (2018) 3 *Proceedings on Privacy Enhancing Technologies* (PoPETS) 63.

[115] Google (n 75) 3.

[116] For example, on anti-discrimination, see Till Speicher et al., 'Potential for Discrimination in Online Targeted Advertising' (2018) 81 *Proceedings of Conference on Fairness, Accountability, and Transparency (FAT*)* 1.

[117] 'App Store Review Guidelines' (*Apple*, last updated 4 March 2020) <https://developer.apple.com/app-store/review/guidelines/> and 'Google Play Program Policies' (*Google*, last update 16 April 2020) <https://play.google.com/about/developer-content-policy-print>.

serving advertising.[118] Crucially, Apple requires app providers to agree to abide by a user's setting in the advertising preference in their use of the advertising identifier.

Further, both iOS and Android provide options for users to limit ad-tracking and personalisation, and also allow users to reset their device's advertising identifier. Facebook implements a technical setting within its software for developers which 'honours' Android and iOS settings, with Facebook stating that it only uses data obtained through the use of the advertising identifier for 'limited advertising purposes' as defined by the iOS Developer Program License Agreement.[119] Similarly, both platforms impose requirements on developers and third-parties to comply with do-not-track (DNT) standards. Apple and Google provided a DNT option in their Safari and Chrome browsers. However, Apple removed the DNT feature from iOS 12.1 in 2019 due to 'potential use as a fingerprinting variable',[120] and instead introduced what is called Intelligent Tracking Prevention to prevent cross-site tracking 'by default'.[121]

Third, platforms impose child-specific rules, with Apple, for example, prohibiting 'behavioural' advertising in children's apps, and contextual ads are required to be appropriate for young audiences.[122] Google also prohibits 'interest-based' advertising for its 'Designed for Families' apps.[123] Further, Google requires that apps which target child audiences should not use Google's sign-in or other Google API services that access data associated with a Google account. As noted in the previous section, platforms not only have contractual rules relating to children, but also provide technical mechanisms within software made available to app developers to help compliance with child-specific rules contained in legislation. For example, the Google Mobile Ads SDK (which can also be used in iOS) has a child-directed setting to help app developers comply with COPPA.[124] The Google Mobile Ads SDK also has a feature to help developers comply with age restrictions under the GDPR. This allows developers to include a 'Tag For Users under the Age of Consent in Europe' parameter to be included in an ad request, which disables (a) personalised advertising for that specific ad request, and (b) requests to third-party ad vendors.[125]

Fourth, the use of certain technical resources is governed under contractual conditions, such as using a social media account log-in. Apple has rules prohibiting the forcing of users to log-in with a social media account to use an app. Apple imposes a rule on developers that if an app's 'core' functionality is not related to a specific social network, the app must provide access without a login, or via another mechanism.[126] Apple also recognises that 'pulling' basic profile information, sharing to a social network, or inviting friends to use an app, are not considered 'core' app functionality.[127]

Facebook takes a different approach to marketing its Facebook login tools in its Facebook SDK for iOS, emphasising that Facebook login provides two major benefits: authentication, and crucially, data access.[128] Notably, Facebook introduced a review process for using the Facebook SDK to ensure 'data is not misused'.[129] Review is not required if the app only asks for a user's public profile and email, while all other permissions require a review by Facebook. Facebook's CEO admitted that the Cambridge Analytica scandal had occurred '[*g*]iven the way our platform worked at the time this meant [the developer] was able to access tens of millions of [users'] friends' data'.[130] After the scandal, Facebook announced it was tightening its login review.[131]

Finally, the power platforms have to set rules beyond privacy protections must also be mentioned, with a prominent and controversial example being Apple forcing app developers to use the in-app purchasing mechanism provided by Apple, and going so far as to prohibit apps from criticising this mechanism, or suggesting other payment methods. Indeed, Apple requires that app developers 'must not directly or indirectly target iOS users to use a purchasing method other than in-app purchase', and 'general communications about other purchasing methods must not discourage use of in-app purchase'.[132] This practice is currently under investigation by the European Commission.[133]

3.4. *Policing behaviour through enforcement*

The final layer of privacy regulation by platforms is through enforcement practices, such as review and potential removal or suspension of apps from app stores, or removal of accounts from developer platforms.[134] Through these mechanisms, platforms can implement direct and indirect enforce-

[118] 'Apple Developer Program License Agreement' (*Apple*) <https://developer.apple.com/terms/>.
[119] 'Audience Network FAQ' (*Facebook*) <https://developers.facebook.com/docs/audience-network/support/faq>.
[120] Juli Clover, 'Apple Removes Useless 'Do Not Track' Feature From Latest Beta Versions of Safari' (*MacRumors*, 6 February 2019) <www.macrumors.com/2019/02/06/apple-removes-safari-do-not-track-option/>.
[121] 'About iOS 12 Updates' (*Apple*) <https://support.apple.com/en-gb/HT209084>.
[122] Apple (n 117).
[123] 'Designing Apps for Children and Families' (*Google*) <https://play.google.com/about/families/designed-for-families/ads-and-monetization/>.
[124] Google AdMob (n 106).
[125] Ibid.
[126] Apple (n 117).
[127] Ibid.
[128] 'Authentication Versus Data Access' (*Facebook*) <https://developers.facebook.com/docs/facebook-login/auth-vs-data>.
[129] Ibid.
[130] Mark Zuckerberg (*Facebook*, 21 March 2018) <www.facebook.com/zuck/posts/10104712037900071>.
[131] Mike Schroepfer, 'An Update on Our Plans to Restrict Data Access on Facebook' (*Facebook*, 4 April 2018) <https://about.fb.com/news/2018/04/restricting-data-access/>.
[132] Apple (n 117).
[133] See *Apple - App Store Practices* (Commission Case AT.40716) (Opening of Proceedings, 16 June 2020) ('The investigation will, in particular, focus restrictions on [developers] ability to communicate with iOS users and inform them about potential alternative (cheaper) purchasing possibilities outside of the app').
[134] For a developer's experience, see Tim Anderson, 'Zapped from the Play store: Another developer gets no sense from Google, appeals to the public' (*The Register*, 29 August 2019) <www.theregister.com/2019/08/29/zapped_from_the_play_store_another_developer_gets_no_sense_from_google_appeals_to_the_public/>.

ment of a platform's data privacy standards on a number of relevant players, including developers, app providers, and third-party libraries. In a sense, this layer is about exercising platform power and leveraging the dependency on platforms. Crucially, while setting standards is one thing, actively policing and enforcement is another. As such, platform power partly derives from openness, and a lack of full review. And as O'Keefe notes, the 'regulatory lever' enjoyed by platforms enables considerable power over third-parties where the platform chooses to exercise this power.[135] It boils down to a question of risk management by platforms on (ab)use of platform tools, which usually comes to the fore following media coverage of various abuses, such as the Cambridge Analytica scandal.

This power is evident when we consider the app review systems implemented by the major platforms. Platforms control not only the technical and contractual standards, but also the app developer platforms (Apple Developer Program and Google Play Console), and crucially, the app marketplaces (App Store and Play Store). Platforms police privacy behaviour both during the app development phase, submission phase, and while the app is available in the app store. This policing has evolved over the years. For example, only in 2015 did Google bring human review for all apps on the Play Store,[136] recognising the trade-off between preventing violations of developer policies, and rapid innovation for app developers on Google Play. Notably, Apple controls (and moderates) how developers can respond to user reviews in the App Store, and only allowed developers communicate with users through the App Store in 2017.[137]

In addition to the app review mechanism at the moment of submission of apps for distribution, platforms investigate and monitor behaviour of apps. During US congressional hearings following the Cambridge Analytica scandal, we gained a window into how Google and Apple police behaviour. Google admitted that it had to put processes in place to 'address the possibility that apps change their behaviour after the verification process', and used machine learning to continually evaluate apps to identify anomalous behaviour.[138] If such behaviour is detected, the app is flagged for manual review.[139] Further, Google conducts periodic audits of apps to ensure c[52 and 56]ompliance with privacy policies, including to confirm that developers' uses of privileges were reasonable. In contrast, Apple talks about a more hands-off approach, acknowledging that Apple 'does not and cannot monitor what developers do with the customer data they have collected or prevent the onward transfer of such data'.[140] However, where Apple receives 'credible information' that a developer is not acting in accordance with Apple's rules, there will be an investigation, followed by actions which may include removal from the App Store and removal of the developer from the Apple Developer Program.[141]

Platforms have a range of restrictive measures they can impose, such as exclusion or suspension from platforms. But platforms also have more subtle measures, such as the ability to demote and promote apps, specifically mechanisms to give prominence (including though ads and paid promotion) within the app store. Google sets out the range of measures that may be applied to an app developer, including app rejection, app removal, suspension and warnings.[142] Google informs Google Play developers that it is not required to send developers a warning prior to suspension or termination.[143] Google also operates an appeal mechanism. In contrast, Apple is not as forthright as Google over the range of mechanisms it may take against an app developer, but does provide a Resolution Centre and App Review Board appeal mechanisms for rejection or removal of apps.[144]

There has been considerable criticism of the app review and app store policing by platforms. A prominent example was Facebook blocking a company (Power Ventures) that allowed users to login and manage all of their social networking accounts from one place. Power Ventures unsuccessfully petitioned the US Supreme Court, arguing that it provided a form of data portability.[145] Spotify also lodged a complaint with the European Commission over Apple's app store practices,[146] and in June 2020, the Commission opened an anti-trust investigation.[147] Other companies, such as the subscription-based digital news company The Information, have described their negative experience with app store policies, including the use of privacy rules.[148] Notably, the European Union recently enacted new legislation that seeks to give business users more rights vis-à-vis platforms, given the unequal power dynamics in the relationship between large dominant platforms and business users. This Platform-to-Business Regulation 2019, also applies to app stores, and mandates that platforms provide reasons to business users where their account is restricted, suspended or

[135] See Amanda O'Keefe, 'What privacy pros can learn from the Facebook-Cambridge Analytica revelations' (*IAPP*, 19 March 2018) <https://iapp.org/news/a/what-privacy-pros-can-learn-from-the-facebook-cambridge-analytica-incident/>.

[136] Eunice Kim, 'Creating Better User Experiences on Google Play' (*Google*, 17 March 2015) <https://android-developers.googleblog.com/2015/03/creating-better-user-experiences-on.html>.

[137] Sarah Perez, 'Developers can finally respond to App Store reviews – here's how it works' (*TechCrunch*, 28 March 2017) <https://techcrunch.com/2017/03/28/developers-can-finally-respond-to-app-store-reviews-heres-how-it-works/>.

[138] Google (n 75) 6.

[139] Ibid.

[140] Apple (n 75) 4.

[141] Ibid.

[142] 'My app has been removed from Google Play' (*Google*) <https://support.google.com/googleplay/android-developer/answer/2477981?hl=en>.

[143] 'Fair warnings' (*Google*)<https://support.google.com/googleplay/android-developer/answer/2985876?hl=en&ref_topic=3453554>.

[144] 'App Review' (*Apple.com*) <https://developer.apple.com/app-store/review/>.

[145] Power Ventures, et al. v. Facebook, Docket No. 16-1105 (Certiorari denied) 10 October 2017.

[146] Daniel Boffey, 'Apple braces for EU investigation after Spotify complaint' *The Guardian* (6 May 2019) <www.theguardian.com/technology/2019/may/06/apple-eu-investigation-spotify-iphone-app-store>.

[147] See *Apple - App Store Practices* (Commission Case AT.40716) (Opening of Proceedings, 16 June 2020).

[148] Jessica E. Lessin, 'Inside Our Apple App Store Ordeal' (*The Information*, 7 December 2019) <www.theinformation.com/articles/inside-our-apple-app-store-ordeal>.

terminated.[149] The Regulation further requires that platforms establish internal complaint-handling systems for business users. While not a privacy law, this is one of the few regulations that have been specifically enacted to address platform dominance in setting the conditions for access to certain markets.

4. Higher-level privacy governance functions of platforms

In this section we move to discussing a set of higher-level privacy governance functions of platforms, again focusing primarily on the smartphone context. After discussing the connection between platforms and the creation of trust, we highlight the role of platforms in bridging transnational regulatory requirements, their role in engaging as stakeholders in regulatory discussions and sources of policy-relevant information, and their role in striking a balance between respect for data privacy in data-driven environments and the optimization of business opportunities connected to the platform and underlying data.

4.1. *Creating trust*

The role platforms play in seeking to protect user privacy can be viewed through the lens of seeking to create trust with users. On this notion of trust, Bodó's work is particularly illuminating, defining trust on an interpersonal level as the 'willingness to cooperate with another in the face of uncertainty, contingency, risk, and potential harm'.[150] Importantly, Bodó argues that digital technologies which mediate interactions are, in a sense, trust mediators, with digital trust mediation becoming a 'core element of the digital infrastructure'.[151] In this regard, platforms have a strong incentive to appear to protect user privacy, as gaining user trust will contribute to optimising engagement (and monetisation). This lens of trust-creation goes beyond dominant smartphone platforms, but also across the platform economy. In this vein, Lobel has argued that platforms are characterised by access, scale, repeat interactions, and technological identification, which combine to create a 'new system of stranger-orientated trust'.[152] Lobel also ties this to platforms engaging in private regulation, whether through reviews, ratings, and social network recommendations, which are alternatives to traditional regulation. This private regulation creates multiplayer trust: trust in participants; trust in value exchanged; and crucially, trust in the platform.[153] Nooren et al. also emphasise the point that consumer trust in platforms very much depends on the integrity of the service provided, including the technical standards set by platforms for safe transactions.[154] While Hong and Cho have examined the impact of trust on consumer behaviour in e-marketplaces, and argue that trust is transferred from an intermediary to the community of sellers, implying that the trustworthiness of the intermediary plays a critical role in determining the extent to which consumers trust and accept the sellers in the e-marketplace.[155]

Policymakers tie the creation of trust in platforms with the growth of the digital economy, where trust in platforms is necessary to fully exploit the benefits of the online platform economy. Indeed, the European Commission argues that access to data spurs marketplace efficiency and innovation, and loss of trust in platforms can undermine their (data-driven) business models.[156] As such, a high level of trust is essential for the data-driven economy, where compliance with rules on personal data will create trust for both businesses and the general public to confidently engage with online platforms. Similarly, the FTC argues that implementation of its recommendations for companies in the mobile ecosystem will result in 'enhancing the consumer trust that is so vital to companies operating in the mobile environment'.[157] Indeed, the whole point of the FTC's recommendations is to build trust through transparency.

In the smartphone context, trust is at the centre of platform policies. For example, Apple places trust as a centrepiece in its App Store policies, with customer trust the 'cornerstone' of the App Store's success.[158] It strives to make the App Store a 'trustworthy ecosystem', and expects app developers to follow suit, declaring that 'if you're dishonest, we don't want to do business with you'.[159] Apple now goes so far as invoke user 'faith' in the apps discovered and transactions made in the App Store.[160] In a similar vein, Google places trust at the centre of its Google Play policies, seeking to deliver the 'most trusted source' for apps, and the most 'trusted' apps.[161] And in public statements and interviews, Facebook's CEO Mark Zuckerberg also invokes the value of trust, framing Facebook's latest changes to move away from a town square platform to private communications, as designed to create a 'more trustworthy platform'.[162] Indeed, in Facebook's 2020 annual filing to the SEC, the importance of user trust is highlighted, and if users do not perceive its products trustworthy, Facebook 'may not

[149] Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186.
[150] Balázs Bodó, 'Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators' (2020) *New Media & Society* 1, 2.
[151] Ibid., 18.
[152] Lobel (n 23) 147.
[153] Ibid., 153.
[154] Nooren, Van Gorp, Van Eijk, and Ó Fathaigh (n 18) 277.
[155] Ilyoo B. Hong and Hwihyung Cho, 'The impact of consumer trust on attitudinal loyalty and purchase intentions in B2C e-marketplaces: Intermediary trust vs. seller trust' (2011) 31 *International Journal of Information Management* 469.
[156] Commission, 'Towards a thriving data-driven economy' (Communication) COM(2014) 442 final, 3.
[157] FTC (n 57) 29.
[158] Apple (n 117).
[159] Ibid.
[160] 'Addressing Spotify's claims' (*Apple*, 14 March 2019) <www.apple.com/newsroom/2019/03/addressing-spotifys-claims/>.
[161] Google (n 117).
[162] Mike Isaac, 'Facebook Unveils Redesign as It Tries to Move Past Privacy Scandals' *The New York Times* (20 April 2019) <www.nytimes.com/2019/04/30/technology/facebook-private-communication-groups.html>.

be able to attract or retain users or otherwise maintain or increase the frequency and duration of their engagement'.[163]

Scholars have also examined the nature of trust in platforms in various ways. Hillman and Neustaedter conducted studies on mobile commerce, with participants 'mentally transferring' their trust from larger companies, such as Apple, that approve apps to the apps themselves.[164] However, Mylonas, Kastania and Gritzalis have explored user trust of app stores relating to security and privacy, and find such trust is generally lacking.[165] The authors examined trust in both Android and iOS, with around three out of four respondents in each smartphone platform not trusting the app repository.[166] Similarly, Eurobarometer studies conducted by the European Commission have tracked trust online. In 2011, only 22% of respondents trust platforms such as search engines or social networks.[167] In 2018, almost two thirds of respondents said that they did not trust online businesses to protect their personal information, with more than a quarter saying that they did not trust them at all. Less than a quarter of respondents said they trust online businesses, including only 3% who totally trust them.[168]

4.2. *Translating regulatory requirements into platform policies*

Another consequence of platforms engaging in regulatory behaviour is their ability to bridge transnational regulatory requirements. Indeed, viewed through the lens of the EU internal market, platforms can be seen as allowing and facilitating cross-border trade and service access. Platforms can use the enforcement of terms of service, instead of direct enforcement of national laws, to facilitate transnational operations. For example, in 2018, Apple extended GDPR-type data access rights for US users.[169] Similarly, as part of its app store rules, app developers are required to comply with GDPR-type data minimisation, where apps should only request access to data relevant to core functionality of the app, and only collect and use data that is required to accomplish the relevant task.[170] For children's apps, Apple also include rules from both COPPA and the GDPR for all developers. And in its documentation for app developers, Apple encourages developers to consult the FTC's recommendations on Mobile Privacy Disclosures, the EU's Article 29 WP Opinion 02/2013 on Apps on Smart Devices, and the California AG's Privacy on the Go recommendations.[171] Further, the Do Not Track (DNT) (W3C) standard is an example of one standard aiming to facilitate two regimes with different defaults. Apple and Google provided a DNT option in their Safari and Chrome browsers and apps. The Chrome app for Android had DNT off by default.[172] However, Apple removed the DNT feature from iOS 12.1 in 2019 due to 'potential use as a fingerprinting variable'.[173] Instead, Apple introduced Intelligent Tracking Prevention against cross-site tracking 'by default'.[174]

4.3. *Platforms as stakeholders in policy discussion*

A source of power that platforms derive from their regulatory role is their control over the level of transparency into their ecosystem, whether the app development system, entry to the app marketplace, or the policing of the marketplace.[175] This also means that platforms have considerable leverage in policy discussion around the mobile app ecosystem, as they can control transparency levels by engaging as stakeholders in relevant policy discussions and providing information to regulators, other stakeholders and the general public.

Both Apple and Google have provided information to various US Senate committees that have been investigating aspects of smartphone ecosystems. For example, Apple and Google have provided documentation to US Senate committees on the operation of their mobile ecosystems.[176] Apple and Google representatives have also given Congressional testimony relating to US federal privacy legislation.[177] And as mentioned earlier, there is the example of the Apple and Google entering into agreement with California's AG to increase consumer privacy protection in the mobile marketplace.[178] This included, '[i]n an effort to promote greater transparency' and 'increase developer awareness of privacy issues', the platforms agreed to include in the 'application submission process for new or updated apps, either an optional data field for a hyperlink to the app's privacy policy or a statement describing the app's privacy practices'.[179]

And of course, platforms have already been centrally involved in government responses to the Covid-19 pandemic, in

[163] Facebook, Inc., Annual Report (Form 10-K) (30 January 2020), 10.
[164] Serena Hillman and Carman Neustaedter, 'Trust and mobile commerce in North America' (2017) 70 *Computers in Human Behavior* 10, 14.
[165] Alexios Mylonas, Anastasia Kastania, and Dimitris Gritzalis, 'Delegate the smartphone user? Security awareness in smartphone platforms' (2013) 34 *Computers & Security* 47.
[166] Ibid., 50.
[167] Commission, 'Attitudes on Data Protection and Electronic Identity in the European Union' (2011) Special Eurobarometer 359, 2.
[168] Commission, 'Data Protection' (2015) Special Eurobarometer 431, 63.
[169] Zack Whittaker, 'Apple overhauls its privacy pages, and now lets U.S. customers download their own data' (*TechCrunch*, 17 October 2018) <https://techcrunch.com/2018/10/17/apple-privacy-pages-data-access-requests/>.
[170] Apple (n 117).
[171] 'Protecting the User's Privacy' (*Apple*)<https://developer.apple.com/documentation/uikit/protecting_the_user_s_privacy>.
[172] 'Turn "Do Not Track" on or off' (*Google*) <https://support.google.com/chrome/answer/2790761?co=GENIE.Platform%3DAndroid&hl=en&oco=1>.
[173] Clover (n 120).
[174] 'About iOS 12 Updates' (*Apple*) <https://support.apple.com/en-gb/HT209084>.
[175] See Jef Ausloos, Paddy Leerssen, and Pim ten Thije, 'Operationalizing Research Access in Platform Governance: What to learn from other industries? (Algorithm Watch 2020) 9 <https://algorithmwatch.org/wp-content/uploads/2020/06/GoverningPlatforms_IViR_study_June2020-AlgorithmWatch-2020-06-24.pdf> (describing how some platforms 'only rarely release data under their control for independent outside inquiry').
[176] Apple (n 75) and Google (n 75). See also Timothy Powderly, 'Letter to Senator Greg Walden' (*Apple*, 7 August 2018) <https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rg5Kb.hn528o/v0>.
[177] See above, n 74.
[178] State of California, Office of the Attorney General (n 61).
[179] Ibid., s 2.

particular relating to location data, and contact-tracing mobile apps. First, Apple released data from its Apple Maps app to help governments and health authorities tackling the Covid-19 pandemic. Apple was at pains to state that Maps does not associate mobility data with a user's Apple ID, and Apple does not keep a history of where a user has been. While Google also began releasing location data from Google Maps app to help governments and health authorities make decisions around Covid-19.[180] Second, and for the first time, Apple and Google collaborated on a Bluetooth-based contact tracing platform by building this functionality into the underlying platforms. And also, for the first time, both companies released APIs that enable interoperability between Android and iOS devices using apps from public health authorities.[181] Finally, Apple and Google have been able to frame their collaborative efforts as based on 'user privacy and security central to the design'.[182]

4.4. *Balancing privacy with value optimisation*

Crucially, in all of this, platforms are striking a (or perhaps better, their) balance between ensuring the respect for data privacy in data-driven environments on the one hand, and the optimization of the value and business opportunities connected to the platform and underlying data for users of the platform on the other hand. Facebook CEO Mark Zuckerberg has perhaps most clearly admitted this trade-off, commenting that Facebook's vow to 'supervise' its users' information 'more closely' would mean 'greater restrictions on developer access', and make developing for the platform 'harder for a lot of these folks'.[183] However, any short-term difficulties for developers would be 'worth the long-term benefit of greater user trust in the platform'.[184] Indeed, in its 2019 annual filings with the SEC, Facebook disclosed that it was making 'significant investments' in efforts to combat misuse of its services and user data by third parties, including 'investigations and audits of platform applications that previously accessed information of a large number of users of our services'.[185] Notably, Facebook 'anticipated' that due to its ongoing investments, it would 'continue to discover and announce, additional incidents of misuse of user data or other undesirable activity by third parties'.[186] Again, connecting this to trust, Facebook stated that discovery of this activity 'may negatively affect user trust and engagement, harm our reputation and brands, require us to change our business practices in a manner adverse to our business, and adversely affect our business and financial results'.[187] This illustrates how platforms are in a position of making trade-offs between user privacy and revenue-making, in ways that are not stipulated by law.

5. Disclosure requirements for regulatory privacy functions

From the foregoing, it seems clear that platforms are acting as de facto privacy regulators for the mobile app ecosystem. This has been highlighted recently by platforms even setting the privacy standards for Bluetooth-based contact-tracing apps being rolled out to tackle a pandemic. From a user privacy perspective, platforms have indeed introduced many policies and standards to increase privacy for mobile devices and apps, and policing the behaviour of apps available in app marketplaces undoubtedly reduces risks to user privacy. However, this reality raises three fundamental points: First, this role played by platforms is taking place outside of a legislative data protection framework that specifically applies to platforms. Platforms are incorporating legal rules in their terms of service, changing them at will, and have the ability to either restrictively or expansively interpret these rules. There are little legislative rules on how platforms should exercise this role, leaving incredible discretion to platforms as regulators.[188] Second, platforms are in a position of making trade-offs between protecting user privacy, and revenue-making from the operation of their app marketplaces. And yet, again, there are no rules in privacy legislation on how this trade-off should be managed.[189] Third, a major issue with this role of platforms acting as privacy regulators is that platforms also provide apps and services that compete with apps available in their app marketplaces. Prominent companies that compete with these services have argued that platforms are misusing privacy rules, and the question must be posed if there is a risk of platforms weaponising these rules to engage in anti-competitive behaviour or other abuse of dominance.

However, we cannot make an informed judgment on whether this role platforms are playing as regulators is sufficient, or whether it might be detrimental. We need to be able to able to evaluate the performance of platforms as privacy regulators. And the question thus arises about how to create the conditions for evaluating this performance? We argue that mandated disclosures about platforms' regulatory behaviour

[180] Jen Fitzpatrick, 'Helping public health officials combat COVID-19' (*Google*, 3 April 2020) <https://blog.google/technology/health/covid-19-community-mobility-reports/>.
[181] Apple (n 13).
[182] Apple (n 14). See, however, Michael Veale, 'Privacy is not the problem with the Apple-Google contact-tracing toolkit' *The Guardian* (1 July 2020) <www.theguardian.com/commentisfree/2020/jul/01/apple-google-contact-tracing-app-tech-giant-digital-rights> (arguing that while it may be 'great for individual privacy', the 'kind of infrastructural power it enables should give us sleepless nights').
[183] Mike Isaac, 'Facebook Unveils Redesign as It Tries to Move Past Privacy Scandals' *The New York Times* (30 April 2019) <www.nytimes.com/2019/04/30/technology/facebook-private-communication-groups.html>.
[184] Ibid.
[185] Facebook, Inc., Annual Report (Form 10-K) (31 January 2019), 15.
[186] Ibid.
[187] Ibid.
[188] See Thomas Germain, 'What the New iPhone Privacy Features Will Really Do' (*Consumer Reports*, 24 June 2020) <www.consumerreports.org/privacy/apples-new-privacy-features/> (arguing how much will depend on Apple's enforcement).
[189] While not privacy legislation, it is important to note that the European Commission's proposed DMA (n 28) may include new obligations for certain platforms in relation to their data practices, including obligations to (a) refrain from using, in competition with business users, any data not publicly which is generated through activities by those business users; and (b) refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services.

is a key method to evaluating the role of platforms as privacy regulators going forward. Our disclosure model builds upon other proposals for enhanced transparency and accountability of social media platforms.[190]

5.1. *Disclosures and regulation theory*

Scholars have long examined disclosure as a form of regulation,[191] and Dalley has explained the widespread use of disclosure-based regulation due to it being 'politically acceptable' and interfering less with 'individual choice and with the operation of markets'.[192] Further, it may be easier to impose disclosure requirements than to regulate substantively; it aligns with the view disclosure 'preserves individual choice while avoiding direct governmental interference'; and notably, the increase in regulation through disclosure may reflect the ability of regulated groups to use the legislative process to avoid direct regulation.[193] In this regard, there are many examples of disclosure-type regulation, such as disclosures under securities law, where publicly-traded companies must disclose a wide range of information to the public before securities can be sold, including business practices, business risks and financial information.

While there are many types of disclosure regulations, it is important to understand the purpose of these disclosure rules, which can vary. As Dalley notes, disclosure-based schemes tend to be based on bland statements such as 'improving transparency' or 'providing information to consumers', which fail to explain the added-value of the additional information.[194] In effect disclosure regulations can serve a number of purposes, including: (a) providing information to decision-makers, such as those 'about to engage in an economic transaction in a market';[195] (b) altering behaviour, and improving the quality of a product or service; (c) improving the operation of government itself, where regulators need information to design and enforce direct regulation; (d) informing consumers about legal rights aimed at 'improving the function of an existing legal regime by reducing information asymmetries';[196] and (e) 'generate interest in the information itself', and create 'public awareness' (which can affect the reputation of companies, and affect competition between companies).[197] As such, an important element of disclosure regulation is the relevant audience for the information, which can include consumers, interest groups, government, and regulators.

5.2. *Application to platforms and privacy*

The question thus arises how a disclosure regime would apply to platforms in their role as privacy regulators in the mobile app ecosystem. We must at the outset make explicit the goals of such a disclosure regime. The overall purpose of disclosure would be to ensure that current legislative rules on privacy are being adequately complied with, by ensuring that government regulators have sufficient information on the operation of platforms. Thus, disclosure would be remedying information asymmetries between government and platforms. However, not only would the disclosures target information for regulators, such information can also be used by interest groups, in order to assess whether further regulation is needed. A final purpose would be altering the behaviour of platforms through increased competition, where the disclosed information affects the reputation of platforms.

Next, we must set out the information that should be disclosed. As discussed above, platforms set and control (a) technical standards on privacy and access to data; (b) contractual terms on privacy and access to data; and (c) the policing of app stores under privacy and data access rules. And yet, we have little information on these activities, and where information is made available, it is very dispersed and selectively disclosed. For example, Google and Apple provide little regular information on the number of apps that are removed from their app stores, or the number of developers that have been removed or suspended from their developer programmes. It was only following the request from the US Senate when conducting hearings following the Cambridge Analytica scandal, did we learn of some precise figures on the number of apps being removed. Further, Apple has begun publishing app removal requests from governments and regulators under national laws, which numbered just over 200 in 2019, with the vast majority requested by the Chinese government (with the apps not named).[198] But there is scant information on apps removed by platforms themselves for violating their terms of service, and the contractual and technical rules they set for

[190] See, for example, 'Creating a French framework to make social media platforms more accountable: Acting in France with a European vision - Mission report "Regulation of social networks – Facebook experiment"' (French Secretary of State for Digital Affairs, May 2019) <www.numerique.gouv.fr/uploads/Regulation-of-social-networks_Mission-report_ENG.pdf>

[191] See Paula J. Dalley, 'The Use and Misuse of Disclosure as a Regulatory System' (2007) 34 *Florida State University Law Review* 1089; Archon Fung, David Weil, Mary Graham, and Elena Fagotto, 'The Political Economy of Transparency: What Makes Disclosure Policies Sustainable?' (John F. Kennedy School of Government, Harvard University, Faculty Research Working Paper No. RWP03-039, October 2003) 20-22 <https://ash.harvard.edu/files/political_econ_transparency.pdf> Julie E. Cohen, 'The Regulatory State in the Information Age' (2016) 17 *Theoretical Inquiries in Law* 369; Margaret Jane Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press 2013); Bradley C. Karkkainen, 'Information as Environmental Regulation: TRI and Performance Benchmarking, Precursor to a New Paradigm' (2001) 89 *Georgetown Law Journal* 257; Cass R. Sunstein, 'Informational Regulation and Informational Standing: Akins and Beyond' (1999) 147 *University of Pennsylvania Law Review* 613; and William M. Sage, 'Regulating Through Information: Disclosure Laws and American Health Care' (1999) 99 *Columbia Law Review* 1701, 1707-10.

[192] Dalley (n 191), 1090.

[193] Ibid., 1093.

[194] Ibid., 1091.

[195] Ibid., 1108.

[196] Ibid., 1111.

[197] Ibid., 1112.

[198] 'App Removal Requests Legal Violation' (*Apple*) <www.apple.com/legal/transparency/app-removal-requests-legal-violation.html>.

privacy. Google does publish an annual security report on Android, but with little concrete figures on app removals.[199] Further, there are little figures on the amount of internal appeals that are accepted or rejected by Apple and Google concerning their app store removals and suspensions. Indeed, for the operation of control mechanisms for access to the app store, and the technical standards that are imposed on app developers, we must rely on high-profile campaigns from well-known companies, such as Spotify and Epic Games (the developer of the popular Fornite gaming app). For example, Epic's CEO alleged that Google puts apps downloadable outside of Google Play at a disadvantage through technical measures such as 'repetitive security pop-ups for downloaded and updated software', 'restrictive manufacturer and carrier agreements and dealings', with Google 'characterising third-party software sources as malware', and 'efforts such as Google Play Protect to outright block software obtained outside the Google Play store'.[200]

Thus, we propose that smartphone platforms be required to make official disclosures about their privacy-related policies and practices for their respective ecosystems. These disclosures should include statements about relevant conditions for access to data and the platform, the platform's standards with respect to privacy and the way in which these standards ensure or facilitate compliance with existing legal frameworks by platform users, and statements with respect to the risks of abuse of different data sources and platform tools and actions taken to prevent or police such abuses. In particular, these disclosures should operate at three levels: first, regarding the technical standards set, changes to technical standards for privacy under iOS and Android operating systems should be documented and archived in an easily-accessible format. This is to ensure that regulators, interest groups, and indeed, app developers, are made aware of changes to the technical standards implemented to protect privacy. Second, changes to terms of service and developer agreements concerning privacy must be documented and archived in an easily-accessible format. Platforms change the terms of service relating to privacy regularly without notice, and platforms being required to give notice and document these changes in a special disclosure would again allow regulators, interest groups, and app developers to monitor these changes. Third, the enforcement of privacy rules on access to, and removal from, app stores must be disclosed, and archived, in an easily-accessible format. This should include figures on the number of apps removed, or rejected, based on privacy rules; the number of developer accounts suspended, and the level of staffing dedicated to app review processes.[201] Further, disclosures should be made on the amount of decisions taken in the internal-complaints procedures related to privacy, where developers appeal removal or suspension decisions. Fourth, platforms should disclose reasoned decisions made in relation removal of apps based on privacy rules. This is to ensure consistency in the enforcement of privacy rules, which are often vague.

It must of course be recognised that there may be limits to the disclosure regime in curbing potential excesses of platform privacy-related practices, and it would still leave in place the regulatory model that platforms have assumed. However, the disclosure regime could go some way in actually improving not only the functioning of platforms' role as regulator, but also the legitimacy of such a role.[202] it must be also asked why choose disclosures as an instrument to deal with platforms operating as privacy regulators, rather than say imposing full-blown privacy requirements on platforms, such as to ensure that apps made available on their platforms conform to privacy laws.[203] It may be the case that strict liability-type regulation may ultimately be needed. But a disclosure regime is a lighter form of regulation, which works when those required to makes disclosers have an interest in the regime succeeding, and may benefit from increased disclosure.[204] Platforms are already framing their app stores and mobile ecosystems as predicated on trust, and having to disclose their privacy-protecting regulatory role can bolster platforms' reputation in the sphere of privacy. Further, disclosure rules would make the role that platforms already have in practice more explicit. This would help to highlight best practices, create more accountability and could save significant regulatory and compliance resources in bringing relevant information together in one place. In addition, it could provide clarity for business users of platforms, who are now sometimes confronted with restrictive decisions by platforms in ways that lack transparency and oversight.

[199] Android Security & Privacy 2018 Year In Review (*Google*, March 2019) <https://source.android.com/security/reports/Google_Android_Security_2018_Report_Final.pdf>

[200] Alex Hern, 'Fortnite owner gives up battle against Google Play store' *The Guardian* (22 April 2020) <www.theguardian.com/technology/2020/apr/22/fortnite-owner-gives-up-battle-against-gooour gle-play-store>.

[201] Notably, the German Network Enforcement Act 2017 places reporting obligations on certain social media platforms in relation to resources and staffing involved in dealing with user complaints relating to illegal content. See Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG <www.gesetze-im-internet.de/netzdg/BJNR335210017.html> and Heidi Tworek and Paddy Leerssen, 'An Analysis of Germany's NetzDG Law' (Transatlantic High-Level Working Group on Content Moderation Online andFreedom of Expression Working Paper 2019).

[202] Legitimacy here is used in the sense of Suchman's definition: 'Legitimacy is a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs and definitions' (Mark C. Suchman, 'Managing legitimacy: Strategic and institutional approaches' (2005) 20 *Academy of Management Review* 571, 574; and discussed in Lee A Bygrave, *Internet Governance by Contract* (Oxford University Press 2015), 134. See also Terence C. Halliday and Gregory Shaffer, *Transnational Legal Orders* (Cambridge University Press 2015).

[203] There have been some narrower proposals debated, such as the EU's proposed ePrivacy Regulation containing a provision that could require browsers and platforms to ensure appropriate privacy settings and defaults with respect to tracking by websites and mobile apps (see discussion in Ó Fathaigh and Joris van Hoboken (n 17)).

[204] Dalley (n 191) 1129.

6. Conclusion

This article has sought to demonstrate the role platforms play as privacy regulators in the mobile device and app ecosystem. Platforms operate an enormous amount of control, from setting the technical standards for privacy in mobile device operating systems, to the contractual and legal standards for developers, to controlling access to the dominant app marketplaces, and removing apps for violating platform rules on privacy. All of this regulatory-type activity happens outside the contours of current privacy laws, which do not specifically target platforms. Building upon this analysis, the article also sought to demonstrate the problems and possible detrimental consequences of this role platforms play, which is occurring with little oversight. In order to remedy this situation, this article puts forward a disclosure regime where platforms are required to make official disclosures about their privacy-related policies and practices for their respective ecosystems. Not only would such a regime assist regulators, business users, and ultimately, users, it can prevent the weaponisation of privacy through anti-competitive behaviour. Smartphone platforms are already under a great deal of regulatory pressure, whether it is EU policymakers indicating the upcoming reformed regulatory framework for platforms will ensure platforms who act as gatekeepers 'remain fair and contestable for innovators';[205] the U.S. Supreme Court's recent judgment that Apple may be sued by iPhone app users for Apple's alleged monopolisation of the iOS app marketplace,[206] Google's €4 billion fine from the European Commission for violating antitrust laws over its Android practices,[207] and the Commission's investigation into Apple's practices in the operation of the App Store.[208] Enhanced disclosures by platforms concerning their regulatory role in protecting user privacy would not only benefit the app ecosystem, it would also go a step toward strengthening the trust users can place in platforms that platforms so desperately crave.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

[205] Commission (n 28).
[206] *Apple Inc. v Pepper* (2019) 139 S. Ct. 1514.
[207] *Google Android* (Case AT.40099) (n 89).
[208] *Apple - App Store Practices* (Case AT.40716) (n 133).