Reconciling Privacy Sandbox initiatives with EU data protection laws.

Lukasz Olejnik
LukaszOlejnik.com
@lukOlejnik @LukaszOlejnik@Mastodon.Social

1. Introduction

Web tracking is high in public awareness and is widely covered in the media. Partly in response to growing concerns, EU data protection law has been enhanced, which culminated in the adoption of the GDPR. A similar process is happening in the U.S.[1]

[1] Meaghan Donahue, "' Times They Are a Changin"-Can the Ad Tech Industry Survive in a Privacy Conscious World?' (2021) 30 Cath. UJL & Tech 193, p. 23.

While various web tracking technologies exist,[2] cookies are prominently utilised, due to their ease of use.

Cookies[3] are small files set in the web browser by visited websites. They enable interesting functionalities, for example, the emblematic “shopping cart”.[4] By storing and accessing information in the user browser, it is possible to identify or track user activity.[5] First-party cookies are set by the websites the user visits directly (i.e. inputting the address in the browser bar or clicking on a link). Third-party cookies[6] are set by (external) websites whose content may be embedded on the visited website. Subsequently, such third-party cookies can be read when visiting other websites that embed the third-party content. Cookies have a “domain” field which denotes the website that may read it (domain “example.com" means that the cookie may be available to example.com when browsing it) and the life-limit duration.[7]

Cookies facilitate targeting of advertisements (ads); user tracking and behavioral monitoring is a common practice in web advertising, cookies being the primary method of choice, and criticised due to privacy issues or abuses. However, tracking abuses identified over the years motivate improvements. Tracking is increasingly

---

[2] Jonathan R Mayer and John C Mitchell, ‘Third-Party Web Tracking: Policy and Technology*2012* ,’ *IEEE symposium on security and privacy* (IEEE 2012), p. 8-10.

[3] Adam Barth, RFC 6265: HTTP State Management Mechanism [2011] (RFC Editor 2011).

[4] Sit, E., & Fu, K. (2001). Inside risks: Web cookies: not just a privacy risk. *Communications of the ACM*, *44*(9), 120.

[5] Balachander Krishnamurthy and Craig Wills, ‘Privacy Diffusion on the Web: A Longitudinal Perspective’, *Proceedings of the 18th international conference on World wide web* (2009).

[6] Supra, Adam Barth (2011), section 7.1. (“third-party servers can use cookies to track the user even if the user never visits the server directly“.

[7] Steven Bingler, Mike West and John Wilander, ‘Cookies: HTTP State Management Mechanism’ (Internet Engineering Task Force 2023) Internet Draft draft-ietf-httpbis-rfc6265bis-12 <https://datatracker.ietf.org/doc/draft-ietf-httpbis-rfc6265bis> [2023] accessed 27 May 2023.

more difficult.[8] Web browsers like Firefox[9] or Safari[10] introduce measures to curb abuses. The Chrome browser also plans improvements, like phasing out third-party cookies.[11] As a "replacement", Google/Chrome proposes to re-architect parts of the web platform to facilitate other methods of directing ads, the so-called "Privacy Sandbox" proposals facilitating certain functions related to ad-serving.[12] The stated aims of Privacy Sandbox[13] are improvements of privacy and data protection qualities concerning the previous industry standards. It would be a large-scale ecosystem migration.[14] Third-party cookies are to be phased out once the new proposals are implemented.[15] Transitioning from the current web economy based on user tracking and personal data processing to an arrangement not based on tracking users could ameliorate data protection standards.

In this dissertation, I consider a complex Privacy Sandbox proposal, the Protected Audience API (PAA).[16] The measure is designed to reach audiences with content/

---

[8] Konrad Kollnig and others, 'Goodbye Tracking? Impact of IOS App Tracking Transparency and Privacy Labels*2022* ,' *ACM Conference on Fairness, Accountability, and Transparency* (2022), p. 10.

[9] 'Firefox Android's New Privacy Feature, Total Cookie Protection, Stops Companies from Keeping Tabs on Your Moves | The Mozilla Blog' <https://blog.mozilla.org/en/mozilla/firefox-androids-new-privacy-feature-total-cookie-protection-stops-companies-from-keeping-tabs-on-your-moves/> accessed 9 June 2023.

[10] 'Full Third-Party Cookie Blocking and More' (*WebKit*, 24 March 2020) <https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/> accessed 9 June 2023.

[11] 'Expanding Testing for the Privacy Sandbox for the Web' (*Google*, 27 July 2022) <https://blog.google/products/chrome/update-testing-privacy-sandbox-web/> accessed 7 June 2023.

[12] 'The Privacy Sandbox' <https://www.chromium.org/Home/chromium-privacy/privacy-sandbox/> accessed 9 June 2023.

[13] 'The Privacy Sandbox' <https://www.chromium.org/Home/chromium-privacy/privacy-sandbox/> accessed 9 June 2023.

[14] Dylan A Cooper and others, 'Privacy Considerations for Online Advertising: A Stakeholder's Perspective to Programmatic Advertising' (2023) 40 Journal of Consumer Marketing 235, p. 16-18, p. 28.

[15] 'Building a More Private Web: A Path towards Making Third Party Cookies Obsolete' (*Chromium Blog*) <https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html> accessed 18 May 2023. Citation: "*Once these approaches have addressed the needs of users, publishers, and advertisers, and we have developed the tools to mitigate workarounds, we plan to phase out support for third-party cookies in Chrome*".

[16] 'Protected Audience (Formerly FLEDGE)' [2023] <https://wicg.github.io/turtledove/> accessed 9 June 2023.

ads in privacy-improved ways. To appreciate the changes, the analysis must be firmly anchored in the context of data protection.

2. The core concepts of data protection

Data protection has a special, quasi-constitutional[17] [18] place in the European law framework. The European Convention on Human Rights guarantees the right to respect for one's private and family life.[19] The related case law of the European Court of Human Rights (ECtHR) is rich.[20]
The rights to the protection of personal data,[21] and to privacy,[22] are included in the EU Charter. The Court of Justice of the European Union (CJEU) has dedicated guidance concerning the relevance of past cases and data protection.[23]

EU data protection laws are placed on these strong foundations. Legislation is based[24] on the Treaty on the Functioning of the European Union's (TFEU) right to the protection of personal data.[25]

---

[17] Shawn HE Harmon, 'Review of Reinventing Data Protection?' (2010) 4 Studies in Ethics, Law, and Technology, p. 3.

[18] Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, vol 16 (Springer Science & Business 2014), p. 2.

[19] European Convention on Human Rights [1950], article 8.

[20] European Court of Human Rights, 'Guide to the Case-Law of the of the European Court of Human Rights, Data protection' <https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf> [2022] accessed 23.05.2023.

[21] Charter of Fundamental Rights of the European Union [2012] OJ C 326, article 8.

[22] Charter of Fundamental Rights of the European Union [2012] OJ C 326, article 7.

[23] Court of Justice of the European Union, 'Fact Sheet, PROTECTION OF PERSONAL DATA'<https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf> accessed 15 May 2023.

[24] Christopher Docksey and Gabriela Zanfir-Fortuna, 'Article 16 [Protection of Personal Data] (Ex-Article 286 TEC)', *Treaty on the Functioning of the European Union-A Commentary: Volume I: Preamble, Articles 1-89* (Springer 2021), p. 1.

[25] Treaty on the Functioning of the European Union (TFEU) OJ C 326 [2012], article 16(1).

The strong rooting of data protection in the EU has direct consequences on the perception of online identifiers as personal data, an aspect of critical relevance in this dissertation.

2.1 Data protection provisions

Fundamental legal texts must be mentioned. The most important, and concrete, data protection law is the General Data Protection Regulation (GDPR).[26] It defines crucial concepts, including data protection principles.[27] It gives grounds for the European Data Protection Board (EDPB)[28] [29] to issue guidelines and oversee the application and enforcement. When considering issues of online ads, the ePrivacy Directive[30] concerning confidentiality in electronic communication[31] is important. The Directive is transposed into the law of Member States.[32] The proposal for an updated ePrivacy (Regulation)[33] is also relevant.

---

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) [2016] OJ L 119/1.

[27] GDPR, Chapter II (Principles).

[28] GDPR, art. 68.

[29] 'EDPB | European Data Protection Board' <https://edpb.europa.eu/edpb_en> accessed 15 May 2023.

[30] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, ePrivacy Directive) [2002] OJ L 201.

[31] ePrivacy Directive, article 5.

[32] European Data Protection Board. 'Report of the Work Undertaken by the Cookie Banner Taskforce' <https://edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en> accessed 5 June 2023, p. 4, para 1.

[33] 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 [2017] COM/2017/010 final - 2017/03 (COD).

Together, the GDPR and ePrivacy uphold the rights enshrined by the Charter: to data protection, and to privacy.[34] The gravity of data protection in the EU is evidenced by *Digital Rights Ireland Ltd,* which resulted in the invalidation of an EU directive.[35]

2.1.1. Personal data and data processing

Personal data[36] are defined as "any information relating to an identified or identifiable natural person",[37] or "data subject",[38] used here interchangeably with "user". The data subject is an "identifiable natural person … who can be identified, directly or indirectly, in particular by … an online identifier".[39] When this threshold of identifiability is met, the processed data *are* personal data. Such 'processing'[40] is then in the scope of the GDPR. Data processing considers many operations: "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".[41] Consequently, not only operations on, or uses of, data are relevant, but also the collection, storage, or destruction. Users may be identified by various means: demographic data, biometric data, but also online identifiers.[42]

More concretely, in *Breyer,* the CJEU established that online identifiers (dynamic IP addresses) may constitute personal data (when the data processor[43] has the means

---

[34] GDPR, recital 1; ePrivacy Directive, recital 2.

[35] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] para 68-71.

[36] GDPR, article 4(1).

[37] Ibid.

[38] Ibid.

[39] Ibid.

[40] GDPR, article 4(2).

[41] Ibid.

[42] Such as cookies; see below.

[43] GDPR, article 4(8), article 28.

to use them to establish user identity).[44] It followed *Scarlet Extended* (considering static IP addresses).[45] IP addresses (dynamic) as identifiers were in the scope of *Benedik v. Slovenia,*[46] which concerns the path of establishing the identity of *a natural person* from a dynamic IP.[47] In line with *Breyer*, processing of online identifiers requires consent (unless it is important for the provision of the service).[48]

The important takeaway from these cases is that online identifiers constitute personal data when the processor is *reasonably* able to link data to persons. In the case of large internet platforms, this may be the case.

2.1.2. Singling out

EU data protection law applies “to any information concerning an identified or identifiable natural person”.[49] To guarantee strong privacy or data protection qualities, products or services could, in principle, operate on de-identified data. Establishing when this may or may not be the case can be made using the *singling-out test*.[50] It can be performed considering “all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly”.[51] The test considers whether it may *reasonably* be possible to analyse the information held to extract information

---

[44] Court of Justice of the European Union, Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779, paras 47-49.

[45] Court of Justice of the European Union, Case C-70/10 Scarlet Extended [2011] ECLI:EU:C:2011:771, paras 50-51.

[46] Benedik v. Slovenia Application no. 62357/14 (ECtHR 24 April 2018) [2018], paras 107-108.

[47] Ibid, paras 6-10.

[48] Supra, *Breyer*, para 64.

[49] GDPR, recital 26.

[50] Ibid.

[51] Ibid.

establishing that some data may relate to a user.[52] This cannot be a purely hypothetical capability. It should be *reasonable*.[53] [54]

Singling out can be a useful socio-technical test of the ability to *identify* individuals.[55] When applied literally — the *absolutist* stance[56] — it requires to consider an important point: singling out by whom? The test might need to consider not only the possibilities of the data controller but also of the potential third parties.[57] This may give rise to a 'grey area' of identifiability: (1) by the data controller, or (2) by a resourceful third-party actor.[58] Importantly, *Breyer*[59] did not consider an absolutist situation. The case was about a data controller having the (potential) means to establish that a dynamic IP address belonged to an identified person.[60] The Court's stance is the most legally relevant, risk-based approach, where it is considered if singling out is *reasonably* possible, and not just *potentially*[61] possible.

---

[52] Working Party 29, Opinion 05/2014 on Anonymisation Techniques, p. 11 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 15 May 2023.

[53] Working Party 29, Opinion 4/2007 on the concept of personal data, p. 15 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 15 May 2023.

[54] Keeping in mind that such opinions are to help in interpreting law, but are not binding; Consider the treaty on the Functioning of the European Union [2012] OJ C 326, article 288. ("Recommendations and opinions shall have no binding force").

[55] Nadezhda Purtova, 'From Knowing by Name to Targeting: The Meaning of Identification under the GDPR' (2022) 12 International Data Privacy Law 163, p. 20.

[56] Ibid, p. 5. ("absolutist stance indicates that anonymization ought to be permanent").

[57] Michèle Finck and Frank Pallas, 'They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10 International Data Privacy Law 11, p. 7.

[58] Ibid, p. 8.

[59] Supra, Case C-582/14.

[60] Frederik Zuiderveen Borgesius, 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition' (2017) 3 Eur. Data Prot. L. Rev. 130, p. 8.

[61] Daniel Groos and Evert-Ben van Veen, 'Anonymised Data and the Rule of Law' (2020) 6 Eur. Data Prot. L. Rev. 498, p. 5.

The ‘singling out’ test can be translated to technical requirements,[62] and is “the only criterion for identifiability explicitly mentioned in the GDPR”.[63] It forms a useful link between technology and law; it may lower the uncertainty of when personal data are processed.[64] Systems or data may be audited for meeting proper standards. If singling out is impossible, processing personal data does not arise, and operations are not subject to the GDPR.

2.1.3. Data protection principles

Data protection principles “should apply to any information concerning an identified or identifiable natural person”.[65] Considering these principles is useful to anchor the subsequent analysis, the technical one in section 3, and the legal one in sections 4 and 5 — as applied to the technical content in section 3.

The data protection principles are defined in Chapter II of the GDPR.[66] They do not apply to “information which does not relate to an identified or identifiable natural person”,[67] such as anonymous data processing. Principles may be translated to technology systems, design, and deployments.[68]

2.1.3.1. Lawfulness, fairness and transparency

---

[62] Aloni Cohen and Kobbi Nissim, ‘Towards Formalizing the GDPR’s Notion of Singling out’ (2020) 117 Proceedings of the National Academy of Sciences 8344.

[63] Ibid, p. 2.

[64] Ibid, p. 1.

[65] GDPR, recital 26.

[66] GDPR, chapter II.

[67] Ibid.

[68] Fredrik Blix, Salah Addin Elshekeil and Saran Laoyookhong, ‘Data Protection by Design in Systems Development: From Legal Requirements to Technical Solutions*12 2017* ,’*th International Conference for Internet Technology and Secured Transactions (ICITST)* (IEEE 2017), p. 2.

Processing must be *lawful*, *fair*, and *transparent*. A legal basis for processing must exist.[69] There are six bases, among them *consent*,[70] often the most appropriate legal basis of choice in online advertising.[71]

2.1.3.2. Purpose limitation

Data must be processed for specified *purposes*,[72] "an essential condition to processing personal data and a prerequisite for applying other data quality requirements".[73] Reusing data for an incompatible purpose than originally specified ("function creep"[74]) is disallowed, unless further processing is compatible with the original purpose,[75] or a proper basis is used (i.e. for consent, consent may be asked for).

2.1.3.3. Data minimisation

Data should be adequate, *relevant*, and *limited*[76] for the aims of processing. Data minimisation can be designed, or implemented in deployed technology. It revolves around the processing of data that is actually necessary.[77] Compliance may be

---

[69] GDPR, article 6(1).

[70] Ibid, article 4(11), article 6(1)(a), article 7.

[71] Célestin Matte, Cristiana Santos and Nataliia Bielova, 'Purposes in IAB Europe's TCF: Which Legal Basis and How Are They Used by Advertisers?', *Privacy Technologies and Policy: 8th Annual Privacy Forum, APF 2020, Lisbon, Portugal, October 22–23, 2020, Proceedings 8* (Springer 2020), p. 16-17.

[72] GDPR, article 5(1)(b).

[73] Working Party 29. 'Opinion 03/2013 on purpose limitation' 00569/13/EN WP 203 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> (2013), p. 11, accessed 18 May 2023.

[74] Bert-Jaap Koops, 'The Concept of Function Creep' (2021) 13 Law, Innovation and Technology 29, p. 7-9.

[75] Working Party 29. Opinion 03/2013, p. 12-13.

[76] GDPR, article 5(1)(c).

[77] European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default', [2019] <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf>, paras 11, 68-71 , accessed 19 May 2023.

simple if the collection/processing of unnecessary data does not arise. For example, in web technologies, this may be implemented by designing systems without unnecessarily unique identifiers. In cases of online ads, not collecting extraneous data (or no data) may help in compliance.
This principle is explicitly mentioned in article 25 (data protection by design).[78]

2.1.3.4. Accuracy

Data should be *accurate* (e.g. up to date).[79] It is applied both to concepts of factual and temporal accuracy.[80] The simplest example in the realm of online ads would be not classifying persons to be interested in things in which they are not interested.

2.1.3.5. Storage limitation

Storage aspects consider the necessary (maximum) duration, guaranteeing contextual usability of the data.[81] Storing for no longer than is needed may mean that if the data is not necessary, it should not be stored at all (in line with the data minimisation principle).[82] Processing information that are effectively not personal data would be superior.

Therefore, *in extremis*, the application of this principle may mean no data of identified persons collected, for no time. Such inference is relevant in subsequent sections. In technical deployment, the principle is realised by the implementation of measures such as anonymisation, appropriate configurations of automated deletion or backing up necessary data.[83]

---

[78] GDPR, article 25(1).

[79] GDPR, article 5(1)(d).

[80] Dara Hallinan and Frederik Zuiderveen Borgesius, 'Opinions Can Be Incorrect! In Our Opinion. On the Accuracy Principle in Data Protection Law' [2020] Our Opinion. On the Accuracy Principle in Data Protection Law (February 19, 2020). Dara Hallinan, Frederik Zuiderveen Borgesius, Opinions can be incorrect, p. 5.

[81] GDPR, article 5(1)(e).

[82] Ibid.

[83] Supra, EDPB, 'Guidelines 4/2019', paras 80-82.

2.1.3.6. Integrity and confidentiality

Data processing must guarantee a proper level of security, considering the use of "appropriate technical or organisational measures".[84] It refers to the common information security standard of the confidentiality-integrity-availability triad.[85] As such, it is closely related to the provisions of security of processing.[86]

2.1.3.7. Accountability

A data controller is accountable,[87] meaning that compliance with data processing principles must be demonstrable.[88]

2.2. Other relevant concepts

2.2.1. Data protection by design and by default (DPbD)

DPbD[89] introduces the requirement of the pro-active design of systems and services by implementing "appropriate technical and organisational measures",[90] conforming to the "*state of the art*".[91] It is not prescribed what to do exactly.[92] It is reasonable to

---

[84] GDPR, article 5(1)(f).

[85] Magda Brewczyńska, Suzanne Dunn and Avihai Elijahu, 'Data Privacy Laws Response to Ransomware Attacks: A Multi-Jurisdictional Analysis' [2019] Regulating New Technologies in Uncertain Times 281, p. 291.

[86] GDPR, article 32(1)(b).

[87] GDPR, article 5(2).

[88] Tuulia Karjalainen, 'All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm' (2022) 8 Eur. Data Prot. L. Rev. 19, p. 3-4.

[89] GDPR, article 25.

[90] GDPR, article 25(1)

[91] Ibid.

[92] Ira S Rubinstein and Nathaniel Good, 'The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default' (2020) 10 International Data Privacy Law 37, p. 4.

conclude that high standards should be integrated by controllers.[93] Various strategies[94] could be followed.

At a certain point, some high-quality "state of the art"[95] measure might constitute a required standard. Such stipulations may also apply in the case of online advertising,[96] where the sole availability of solutions with superior qualities would warrant their uses. This premise is important for the remainder of this dissertation.

2.2.2. Data protection impact assessment (DPIA)

It is mandatory to conduct a DPIA[97] when the processing may "likely result in high risk".[98] The prerequisite is to establish whether conducting a DPIA is necessary.[99] The EDPB lists data processing activities when DPIA may be relevant.[100] One premise for conducting it is the use of "new technologies".[101]

DPIA can be integrated with the broader production process as part of the necessary reviews.[102] It can therefore be relevant in cases of technology assessments concerning data protection. Various methodologies[103] can be employed.[104]

---

[93] Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 Oslo Law Review 105, p. 10-11.

[94] Seda Gürses, Carmela Troncoso and Claudia Diaz, 'Engineering Privacy by Design Reloaded', *Amsterdam Privacy Conference* (2015), p. 2-4.

[95] Supra, Ira S Rubinstein and Nathaniel Good (2017), p. 6.

[96] Ibid, p. 11-14.

[97] GDPR, article 35.

[98] Ibid.

[99] Working Party 29. 'Guidelines on Data Protection Impact Assessment (DPIA)' 17/EN WP 248 <https://ec.europa.eu/newsroom/document.cfm?doc_id=44137> (2017) accessed 24 May 2023, p. 7.

[100] Ibid, p. 7-10.

[101] Ibid, p. 9, point (8).

[102] Ibid, p. 19.

[103] Nicolás Notario and others, 'PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology*2015* ,' *IEEE Security and Privacy Workshops* (IEEE 2015), p. 2-4.

[104] Ibid, p. 14.

2.2.3. User terminal

Concepts of user devices and web browsers meet the ePrivacy Regulation definition[105] of "terminal equipment".[106] Compatible with the notion in the Directive,[107] it considers a device connected to the network (directly or indirectly). This definition is commonly applied to cover a web browser,[108] which meets the capabilities of being able "to store information or to gain access to information stored…".[109] Web browser software is of key relevance in this dissertation.

2.3. W3C standardisation process

When web browsers implement standardised features, they function similarly or identically, facilitating compatibility. For example, websites 'look' the same regardless of the used web browser, an interoperability issue.

The World Wide Web Consortium (W3C)[110] is a standards development organisation (SDO) focused on web standards.[111] Development happens in working groups (formed by stakeholders, like web browser vendors, online platforms, and external experts), where deliberations over proposals or existing standards take place. The W3C Process[112] specifies the need to consider feedback from many stakeholders,

---

[105] ePrivacy Regulation proposal, art. 4(1)(c).

[106] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment, OJ L 162.

[107] ePrivacy Directive, recital 24.

[108] Martino Trevisan and others, '4 Years of EU Cookie Law: Results and Lessons Learned' (2019) 2019 Proceedings on Privacy Enhancing Technologies 126, p. 1.

[109] ePrivacy Directive, art. 5(3).

[110] 'World Wide Web Consortium (W3C)' <https://www.w3.org/> accessed 15 May 2023.

[111] Raymund Werle and Eric J Iversen, 'Promoting Legitimacy in Technical Standardization' (2006) 2 Science, Technology & Innovation Studies 19, p. 4.

[112] 'W3C Process Document' <https://www.w3.org/2021/Process-20211102/> accessed 15 May 2023.

and multiple rounds of reviews. Work is consensus-based,[113] relying on discussion, and finding common grounds, including varying views, objections, etc. Standards help in interoperability.[114] Large platforms must consider these points,[115] including for reasons of competition.[116]

The W3C is the forum of choice where discussions and developments over Privacy Sandbox proposals take place. Community Groups[117] like the Web Incubator Community Group[118] facilitate work, though discussions take place in various places. Formal reviews may be asked from the W3C Technical Architecture group.[119]

Reviews are of critical consequence. These include basic reviews within particular groups, but also horizontal ones, such as privacy or security. This highlights the need to consider a structured technology review process.

2.4. Privacy reviews and assessments

An important part of W3C review activity is technical reviews.[120] In the context of this dissertation, the most relevant are security and privacy. Considering privacy during the design phase is good practice and a standardisation need.[121] Privacy

---

[113] Alison Harcourt, George Christou and Seamus Simpson, 'Internal Governance of the IETF, W3C and IEEE: Structure, Decision-Making and Internationalisation', *Global Standard Setting in Internet Governance* (Oxford University Press 2020).

[114] Chris Riley, 'Unpacking Interoperability in Competition' (2020) 5 Journal of Cyber Policy 94, p. 7.

[115] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act, DMA) [2022] PE/17/2022/REV/1 OJ L 265.

[116] Ibid, art. 2(29).

[117] 'About W3C Community and Business Groups | Community and Business Groups' <https://www.w3.org/community/about/> accessed 15 May 2023.

[118] 'Web Incubator Community Group (WICG)' <https://wicg.io/> accessed 15 May 2023.

[119] 'W3C Technical Architecture Group' <https://www.w3.org/2001/tag/> accessed 15 May 2023.

[120] Nick Doty, 'Reviewing for Privacy in Internet and Web Standard-Setting', *2015, IEEE Security and Privacy Workshops* (IEEE 2015), p. 3.

[121] Alissa Cooper and others, RFC 6973: Privacy Considerations for Internet Protocols (RFC Editor 2013), p. 23-25.

engineering[122] concerns building products or services with privacy qualities considered, including in ways facilitating obligations of data protection,[123] and supporting the practical implementation of regulations such as the GDPR,[124] which may require conducting impact assessments.[125] [126] This phase may also review the use of privacy-enhancing technologies.[127]

The review process may support compliance, ensuring that products or services have desirable privacy and data protection qualities (i.e. as part of a DPIA process). The W3C has a specific process supporting privacy aspects.[128] Reviews may identify vulnerabilities to help address them.[129] When performed on the level of standards it may lead to the improvement of multiple conforming web browsers at once, contributing to the limitation, or removal of, functions considered as risk-increasing.[130] Auditing the uses of features may reveal various risks, including not foreseen uses or even abuses. For example, the Geolocation API feature considered

---

[122] Seda Gürses and Jose M Del Alamo, 'Privacy Engineering: Shaping an Emerging Field of Research and Practice' (2016) 14 IEEE Security & Privacy 40, p. 2-3.

[123] Seda Gürses and Jose M Del Alamo, 'Privacy Engineering: Shaping an Emerging Field of Research and Practice' (2016) 14 IEEE Security & Privacy 40, p. 2.

[124] Giovanni Maria Riva, Alexandr Vasenev and Nicola Zannone, 'SoK: Engineering Privacy-Aware High-Tech Systems', *Proceedings of the 15th International Conference on Availability, Reliability and Security* (2020), p. 3.

[125] Dariusz Kloza and others, 'Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements' (2019) 1 d. pia. lab Policy Brief 1, p. 2.

[126] GDPR, article 35.

[127] Ian Goldberg, David Wagner and Eric Brewer, 'Privacy-Enhancing Technologies for the Internet', *Proceedings IEEE COMPCON 97. Digest of Papers* (IEEE 1997), p. 6.

[128] 'Self-Review Questionnaire: Security and Privacy' <https://www.w3.org/TR/security-privacy-questionnaire/> accessed 18 May 2023.

[129] Łukasz Olejnik and others, 'The Leaking Battery: A Privacy Analysis of the HTML5 Battery Status API', Data Privacy Management, and Security Assurance: 10th International Workshop, DPM 2015, and 4th International Workshop, QASA 2015, Vienna, Austria, September 21–22, 2015. Revised Selected Papers 10 (Springer 2016), p. 4-5.

[130] Lukasz Olejnik, Steven Englehardt and Arvind Narayanan, 'Battery Status Not Included: Assessing Privacy in Web Standards*2017* ,' *International Workshop on Privacy Engineering* (2017), p. 4-6.

that users should be informed about the details related to the collection of the geolocation data, but websites were found not to do it.[131]

Privacy considerations and assessments are important wherever private or personal data are concerned, including cases of online advertisement technologies. Specific considerations may be motivated by user preferences.[132] Some design choices may be desirable by consumers who prefer “relevant ads”,[133] or have a “high desire to prevent data collection”[134] by advertisers.[135]

3. Privacy Sandbox and Protected Audience API

The stated aim of Privacy Sandbox is to change the current approach used to serve and display ads, to steer away from the collection of data or user tracking. As declared by the initial proponent (Google), this requires alterations to the web platform.[136] Those changes are to be reflected in proposals for new web browser mechanisms (ultimately to be transferred to the mobile environment).[137] One important component that is to be replaced is the de facto industry standard in ad-serving. This status quo must be explained.

3.1 Real-Time Bidding, online behavioural advertising, privacy risks

---

[131] Nick Doty, Deirdre K Mulligan and Erik Wilde, ‘Privacy Issues of the W3C Geolocation API’ [2010] arXiv preprint arXiv:1003.1775, p. 10.

[132] Dylan A Cooper and others, ‘Privacy Considerations for Online Advertising: A Stakeholder’s Perspective to Programmatic Advertising’ (2023) 40 Journal of Consumer Marketing 235, p. 6-7.

[133] Supra, Dylan A Cooper and others (2023), p. 8.

[134] Ibid, p. 8.

[135] Ibid.

[136] Mark Nottingham, ‘Playing Fair in the Privacy Sandbox: Competition, Privacy and Interoperability Standards’ [2021] Privacy and Interoperability Standards (February 3, 2021), p. 5.

[137] ‘Privacy Sandbox on Android’ (*Android Developers*) <https://developer.android.com/design-for-safety/privacy-sandbox> accessed 18 May 2023.

The online ad ecosystem heavily depends on tracking user activities. This landscape evolved over the previous decades. Real-Time Bidding (RTB) is the current industry standard measure for dynamic ad targeting.[138] The simplified picture[139] of its operation considers five sides: the user, the website (publisher), the RTB platform,[140] the bidders for ad space, and the advertiser.[141] The advertiser runs campaigns, using the RTB platform, via bidders. The RTB platform holds auctions for ad space on the publisher's websites. When the user visits a website, the scripts on the website inform the RTB platform about this visit. The RTB platform then holds an auction. Data related to the user and the visit are sent to the participants/bidders,[142] to evaluate and bid. The winner's ad may be displayed. This system relies on user data processing; user data flows to many parties.[143]

Users may be unaware of such data exchanges. RTB's compatibility with EU data protection law is questioned,[144] if only due to the difficulty to comply with transparency requirements, the need for valid consent,[145] or the ability to withdraw it.[146] Whether the approach to consent in RTB is sufficient is disputed,[147] not even mentioning other issues of public concern. Consequently, there is a push to prohibit

---

[138] Yong Yuan and others, 'A Survey on Real Time Bidding Advertising', Proceedings of 2014 IEEE International Conference on Service Operations and Logistics, and Informatics (IEEE 2014), p. 1-2.

[139] Shuai Yuan, Jun Wang and Xiaoxue Zhao, 'Real-Time Bidding for Online Advertising: Measurement and Analysis', *Proceedings of the seventh international workshop on data mining for online advertising* (2013), p. 3.

[140] Closely linked to ad exchanges, who mediate between the publishers and bidders.

[141] SSP (supply-side platforms) manage ad inventory (i.e. ad space on websites), and advertisers may use DSP (demand side platforms) to facilitate reaching those inventories (i.e. placing bids).

[142] Parties bidding in the auction on behalf of advertisers.

[143] Claude Castelluccia, Lukasz Olejnik and Tran Minh-Dung, 'Selling off Privacy at Auction', *Network and Distributed System Security Symposium (NDSS)* (2014), p. 8-9.

[144] Michael Veale and Frederik Zuiderveen Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law' (2022) 23 German Law Journal 226, p. 28.

[145] Supra, Michael Veale and Frederik Zuiderveen Borgesius (2022) p. 24.

[146] CNIL. Deliberation SAN-2023-009 of June 15, 2023 (CRITEO sanctionné d'une amende de 40 millions d'euros) <https://www.cnil.fr/fr/publicite-personnalisee-criteo-sanctionne-dune-amende-de-40-millions-deuros> accessed 22 June 2023, section F.

[147] Michael Veale, Midas Nouwens and Cristiana Santos, 'Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?' [2022], p. 8.

targeted ads completely.[148] Targeting ads based on profiling using special categories of personal data[149] is prohibited.[150] The ad ecosystem is therefore shifting towards different approaches.

3.2. High-level architectural overview

This dissertation focuses on the Protected Audience API (later: *PAA*; API stands for Application Programming Interface),[151] [152] a complex part of the Privacy Sandbox. It is based on previous iterations developed since 2020: TURTLEDOVE,[153] and the tested FLEDGE.[154]

PAA facilitates ad targeting that may happen in isolated environments. It lets (1) "marking" users along their interests, and (2) the ability to reach them with related content. PAA may fulfil the use case of remarketing, when a visitor browsing websites of products may subsequently see ads of these or related products during the later browsing on other websites. Today this is based on user tracking. PAA transitions the ecosystem to an approach not involving tracking.

To facilitate analysis of PAA concerning data protection, I distill crucial *points of interest (PoI)* concerning stages of operations involving user information in specific

---

[148] Bennett Cyphers and Adam Schwartz, 'Ban Online Behavioral Advertising' (*Electronic Frontier Foundation*, 21 March 2022) <https://www.eff.org/deeplinks/2022/03/ban-online-behavioral-advertising> accessed 23 May 2023.

[149] GDPR, article 9(1).

[150] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act, DSA) [2022] PE/30/2022/REV/1 OJ L 277, article 26(3).

[151] 'Protected Audience (Formerly FLEDGE)' [2023] <https://wicg.github.io/turtledove/> accessed 9 June 2023.

[152] API stands for "Application Programming Interface"; '*n. Computing* a set of routines, protocols, and tools designed to allow the development of applications that can utilize or operate in conjunction with a given item of software, set of data, website, etc.; abbreviated *API*' <https://www.oed.com/view/Entry/9705#eid376049> accessed 23 May 2023.

[153] 'Turtledove/Original-TURTLEDOVE.Md.' <https://github.com/WICG/turtledove/blob/main/Original-TURTLEDOVE.md> accessed 23 May 2023.

[154] 'FLEDGE' <https://github.com/WICG/turtledove> accessed 23 May 2023.

ways.[155] Careful distillation of *PoI* is fundamental, if only to explain the system. Such high-level *PoI* pollinate the subsequent data protection analysis (sections: 4, 5).

3.3. Points of Interest

The data is assumed to not leave the user browser, and all (or most) operations are performed in the user's web browser. On the device, in some circumstances, certain activities may be delegated to external nodes assumed to be trusted.

An example use case[156] considers a user browsing shoe products on a website. The website can mark the user as having an *interest* in shoes (e.g., *likes-shoes*, *likes-shoes-sneakers*, etc.). Users are assigned to an *interest group* via programming calls executed on the website, either scripts of the website or supplied by the third parties. Such information is subsequently available for uses in auctions during future web browsing (including of other websites), and ads may be displayed along such interests.

The high-level view of PAA, therefore, considers *users* (the web browser), *publishers* (websites, mobile apps), *buyers* (used interchangeably with script providers, ad providers, ad suppliers; parties controlling ad campaigns), and optionally some third party servers. PAA execution can be divided in phases.

3.3.1. Joining an interest group (PoI#1)

Users browsing websites may perform various actions, like adding products to a shopping cart (activity: purchase), removing them (activity: changing minds), and so on. Such actions may be observed, and attributed to the user, by noting it in the browser at the request of the website scripts.

---

[155] The analysis is based on the shape of standards or explainers as of June 2023 (mature proposals of a system put to tests, but still subject to some modifications, but the parts identified in Points of Interests appear to be stable at this point).

[156] Supra, 'Turtledove/Original-TURTLEDOVE.Md.'

Assignment happens by the execution of PAA's *joinAdInterestGroup* function of the web browser *(PoI#1)*,[157] which modifies or adds such information (it is "stored on disk"[158]), along with information like the name of the interest group, or the owner (i.e. the script provider, offering ad content to be displayed). The immediate observation is that user web browser state is modified (information added).

3.3.2. Leaving an interest group (PoI#2)

User assignment to an interest group may be removed. If the user has been part of a particular interest group, after the execution of the *leaveAdInterestGroup*[159] (*PoI#2*), the user is no longer marked as in this group. Furthermore:

- The result of this operation is unverifiable to the script executor to protect from the risk of learning that the user has previously been in this group, which would be an information leak.
- The maximum duration of assignment to a group is 30 days.[160] Websites or buyers must periodically reassign users in groups.

Such a design is in stark contrast to cookies; cookie value can be accessed, and the lifetime may be long (until recently, even unlimited).

3.3.4. Obtaining information for auction and ad display (PoI#3)

The browser maintains configuration, like ads to be displayed, or the bidding logic algorithms to be used during the auction. The web browser fetches ad content from the ad suppliers (from servers). The content requests are executed for contextual (non-targeted) ads and those based on interest groups (targeted). This data is stored in the user's device.

---

[157] Supra, 'Protected Audience (Formerly FLEDGE)' (2023), section 2.

[158] Ibid, section 6.

[159] Ibid, section 3.

[160] Supra, 'FLEDGE', section 1.1 "Joining Interest Group": "*The browser will remain in an interest group for only a limited amount of time. The duration is specified in the call to joinAdInterestGroup(), and will be capped at 30 days*".

Auction configuration consists of data structures with versatile information. Aside from utilising interest group membership information, ad suppliers may provide[161] [162] (to be used during the auction) signals such as *userBiddingSignals* or *trustedBiddingSignals*,[163] for example for "storage of additional metadata that the owner can use during on-device bidding".[164] Other data enable the display of ads composed of multiple product parts (*adComponents/ad components*[165] data field), etc. The parameter *updateURL* lets the browser update the configuration in the future, to have the latest configuration or ad content.

This information is relevant in the analysis of the risk of singling-out individuals. Since they are provided by script providers, it is partially their responsibility to ensure that the risks are limited, though the browser may mitigate risks, with randomisation (i.e. noise introduction), or for example limiting the number of components when displaying ads formed from multiple products, to reduce the risk of identification.[166]

The auctions and the ad display are assumed to be well-isolated, and impossible to allow the tracking of users, e.g. across the visited websites, a detail of implementation.

3.3.3. Ad auction (PoI#4)

Scripts on the visited website run an auction to decide about the displayed ad (*PoI#3*). This is performed by execution of the *runAdAuction* function (executed by

---

[161] Supra, 'FLEDGE', section 2.1-2.3.

[162] Supra, 'Protected Audience (Formerly FLEDGE)' (2023), section 8.1.

[163] Supra, 'FLEDGE', section 1.2 "Interest Group Attributes". "The userBiddingSignals is for storage of additional metadata that the owner can use during on-device bidding, and the trustedBiddingSignals attributes provide another mechanism for making real-time data available for use at bidding time".

[164] Ibid.

[165] Supra, 'Protected Audience (Formerly FLEDGE)' (2023), section 8.1.

[166] Supra, 'FLEDGE', section 3.4.

code of the script providers, or the websites).[167] The auction utilises previously retrieved configurations. Bid logic (algorithm) is executed. During the bidding, ad-configuration (interest groups, the metadata, or signals from *PoI#3*) is assessed according to the PAA design and is used in line with the provided logic.

As part of the bidding logic and the auction algorithm, scores are computed and compared to decide which (winning) advertisement is to be displayed. The only (final) outcome is the displayed ad, which may be the one aligned towards user interest, or a contextual one — based on information such as the visited website (not the interest group).

In this system, the web browser is in a privileged position:[168] "the browser is in control of interest group membership, and has full insight into what interest group a particular ad targeted".[169]

Only ad providers (buyers who bid in auctions) marked by the web browser as owners of an interest group can bid to display such ads. Once again, the data protection guarantees of this arrangement rest on the effective isolation of the bid and auction process. No information should exit such an execution environment. Otherwise, the risk of singling-out individuals may rise.

It is important to understand that the auction is not executed on the visited website. This is performed in a designated environment of the web browser.[170] In a designated, isolated execution environment, the design disallows access to information about the details of the execution. This environment should be unable to access — receive or send — external information,[171] apart from the strictly needed input data, as defined in the specification or provided for the auction execution. The

---

[167] Supra, 'Protected Audience (Formerly FLEDGE)' (2023), section 4.

[168] Which may be relevant in context of competition law, considered in section 7.

[169] Supra, 'Turtledove/Original-TURTLEDOVE.Md.'

[170] Supra, 'Protected Audience (Formerly FLEDGE)' (2023), section 5 ("Are not scoped to a particular Document, but are rather scoped to a user agent").

[171] Ibid, section 5.

isolation is to be strong.[172] The ad display is also separated. The winning ad is displayed in a “fenced frame”,[173] an isolated environment, precluding the information concerning the details of the selected winning ad from leaking outside.

While the processed information is isolated in the web browser, some of it is supplied by the buyers. This means that the data, in some form, and at some point, reside in their systems. Such parties are responsible for the data protection side of the processing in their systems. The broader system warrants case-by-case analyses. The analysis of this part is not the subject of this dissertation (which would require a case-by-case analysis of deployments that may not even exist yet).[174] The scope of this analysis is PAA.

Disallowing unsanctioned tracking is in the scope of PAA’s design. Still, as with other browser features or standards developed within the W3C, it must be assumed that PAA’s design will evolve in the future to respond to any deficiencies, if identified.

3.3.4. Infrastructure, servers, microtargeting protection with Privacy Infrastructure (PoI#5)

Microtargeting is the precise targeting of individuals.[175] [176] When a particular ad wins once or a few times — it is precisely targeted, potentially implying the possibility of singling out individuals,[177] ‘identifying’ them. PAA may address such risks by displaying ads only when the same ad is marked as to be displayed to a specific number of people.[178] Combinations of data like the “interest group owner, bidding

---

[172] Supra, ‘FLEDGE’, section 3.2. “On-Device Bidding”.

[173] ‘Fenced Frame’ <https://wicg.github.io/fenced-frame/> accessed 27 May 2023.

[174] If only due to the number of ad-suppliers, on the one side, and the length limitation of this work, on the other.

[175] Aleksandra Korolova, ‘Privacy Violations Using Microtargeted Ads: A Case Study*2010* ,’ *IEEE International Conference on Data Mining Workshops* (IEEE 2010), p. 5.

[176] Frederik J Zuiderveen Borgesius and others, ‘Online Political Microtargeting: Promises and Threats for Democracy’ (2018) 14 Utrecht Law Review 82, p. 1-2.

[177] Supra, Aloni Cohen and Kobbi Nissim (2020).

[178] Supra, ‘FLEDGE’, section 1.2.

script URL, rendered creative",[179] uniquely denoting ads, must appear a number of times, in line with k-anonymity.[180] *Privacy Infrastructure* (PI)[181] may monitor if ads are selected a sufficient number of times (i.e. not just once, which could mean that an ad is microtargeted), and display ads validated in this way.

Furthermore, key-value (KV) servers are an optional infrastructure. KV servers would offer read-only data, a basic storage for dynamic, real-time information; for example, the remaining campaign budget, etc.[182] Such infrastructure would have to be technically and organisationally separated from other actors involved in the system. A verifiable, isolated trusted execution environment (TEE)[183] could be used to help achieve this.

The challenge with KV servers is that they may accept data, including lists of interest groups. While proper technical and organisational[184] separation is foreseen, those servers may still obtain versatile information. However, since the use of KV servers is optional, and the feature is relatively newly proposed (potentially subject to changes), in this dissertation uses of KV servers are not considered, while acknowledging that this is a high-risk part.

3.3.5. Reporting on winning/losing bids (PoI#6)

---

[179] Ibid.

[180] Khaled El Emam and Fida Kamal Dankar, 'Protecting Privacy Using K-Anonymity' (2008) 15 Journal of the American Medical Informatics Association 627, p. 3.

[181] 'Outcome-based TURTLEDOVE' <https://github.com/WICG/turtledove> accessed 23 May 2023.

[182] Supra, 'FLEDGE', section 1.2.

[183] Riad Ladjel and others, 'Trustworthy Distributed Computations on Personal Data Using Trusted Execution Environments', 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (IEEE 2019), p. 2-3.

[184] Jatinder Singh and others, 'Enclaves in the Clouds: Legal Considerations and Broader Implications' (2021) 64 Communications of the ACM 42, p. 2-3, 5-6.

Reporting about the ad campaign performance is an industry need. In the final PAA, such information for buyers is to be delivered in an aggregated manner,[185] to ensure that it cannot be linked to the particular ad auction or display. When well designed, this should limit tracking or make it effectively impossible.

3.3.6. “IP Protection” (PoI#7)

Network requests could be *masked* by passive infrastructure[186] providers[187] — not modifying the content, but only the network metadata. Intermediary “mere conduit”[188] services[189] strictly offering only a layer of “technical functionality”,[190] may be exempt from liability[191] when not modifying content unrelated to the transmitted information.[192]

3.4. Interim considerations

During the tests,[193] and the early functioning, some technical and organisational guarantees are to be relaxed. For example:

- The isolation in ad auctions would not be as tight as it must be in the final product.
- The ad reporting would be event-based, not aggregate (which could technically enable user monitoring or tracking until transitioned to aggregate).

---

[185] ‘Private Aggregation API’, section 8.1 <https://patcg-individual-drafts.github.io/private-aggregation-api/> accessed 23 May 2023.

[186] “GoogleChrome/Ip-Protection’ <https://github.com/GoogleChrome/ip-protection/> accessed 27 May 2023.

[187] ‘Google Selects Fastly Oblivious HTTP Relay for Privacy Sandbox Initiative to Enhance Online Privacy for Billions of Chrome Users’ <https://www.fastly.com/press/press-releases/google-selects-Fastly-Oblivious-HTTP-Relay-for-Privacy-Sandbox> accessed 27 May 2023.

[188] DSA, recital 5, recital 17, article 3(g)(i).

[189] DSA, recital 28. The “… virtual private networks, …” are technically close, or equivalent, to IP masking relays as considered in Privacy Sandbox.

[190] DSA, recital 29.

[191] DSA, article 4(1).

[192] DSA, recital 21. (“… in no way involved with the information transmitted or accessed…”).

[193] In 2023, or 2024.

- Some server infrastructure is to be provided by the buyers, which also potentially may facilitate forms of user tracking[194] until it is fully transitioned to the final stage.

Such aspects may introduce substantial risks. However, this dissertation concerns the assumed final state and deployment setup, as defined in the specification and explanatory documents.[195] Such concerns in the interim phase must be adequately addressed by the buyers or ad-infrastructure suppliers, on a case-by-case basis.

Additionally, some parts of the system (like the auction execution) are considered to be performed not necessarily on-device (in the user's browser), but in isolated infrastructures (TEEs), for performance reasons. Considering these optional aspects would further lengthen the analysis, while the main conclusions in this work should still stand, if the custom measures are constructed appropriately (depending on the deployment). The phases in this system (i.e. buyers/advertisers, web browser suppliers such as Google/Chrome), and all the used infrastructure (like the PI in *PoI#5*) are assumed to be isolated technically and organisationally.

Seen as a whole, the considered system is fragile. To function, the design, implementation, and deployments must be carefully calibrated, with crucial protection responsibility put on the web browser. After the final release, any proposed changes must be considered extremely carefully.

4. Data protection analysis

In this section, PAA is analysed with respect to data protection. I end with a fundamental point of how information is processed in the system.

4.1. PAA and EU data protection principles

4.1.1. Purpose limitation

---

[194] Supra, 'FLEDGE', section 5.1.

[195] And not temporary, interim measures.

GDPR puts a special focus on purpose limitation on the collection of personal data.[196] However, no personal data collection happens within the execution of PAA, as defined by the specification.[197] While the data for purposes of auction execution may be provided by buyers,[198] PAA does not foresee functionality of collection, except for aggregate reports, or a design peculiarity letting websites learn the type of an ad (contextual, or interest-group-based), understood as not a realistic risk.[199]

The purpose of potential uses is assumed to be the display of content such as advertisements, or similar. “Further processing” is disallowed as data collection is not facilitated in the first place.

4.1.2. Data minimisation

PAA only allows operations aimed at displaying content to the user. Some information (*PoI#3*) may be supplied by buyers. Support for bounding the size of supplied information is built-in; for example, the number of provided ad components is limited to 20 URLs (i.e. web resource links).[200] [201]

Information used in PAA is well-defined, limited, and determined for the intended design purpose.[202] The potential point of risk is the use of KV servers (*PoI#5*), which are to allow the supply of real-time data, possibly not defined by the specification.

---

[196] GDPR, article 5(1)(b)

[197] As explained previously, on technical grounds the information may potentially be read out by some network calls for example to KV servers (which is outside the scope of this work), or with event-based reporting, to be available just initially, and not in the final deployment.

[198] How the data on the buyer side is collected or treated is assumed to be a separate problem in this work.

[199] ‘Utilizing the 1-Bit Leak to Build a Cross Site Tracker · Issue #211 · WICG/Turtledove’ (*GitHub*) <https://github.com/WICG/turtledove/issues/211#issuecomment-889269834> accessed 27 May 2023.

[200] URL stands for universal resource locator — such as an address of the website, subpages, address of image files, etc.

[201] Supra, ‘Protected Audience (Formerly FLEDGE)’ (2023), section 8.6.

[202] GDPR, article 5(1)©.

Still, the queried information would be simple to inspect (they are network requests). The system is to have precautions limiting risks of identifying specific users. For example, logging is minimised, IP addresses may be masked (*PoI#7*).[203]

Masking IPs[204] would deny ad infrastructures the ability to learn the true IP address of the user. It would not constitute an identifier linked with user activities. Reasoning in line with *Breyer,* buyers/ad-side obtaining masked IPs would be unable to use it as a user network identifier.[205] While the IP address, or the network calls assessed as a whole, may be potentially identifying, it must be established whether there are realistic means for performing such a mapping.[206] When appropriate organisational divisions are in place for the IP-masking infrastructure, it may be *unreasonable* to consider that the buyer or ad infrastructure has such capabilities.[207]

The technical measures, therefore, uphold this data protection principle (see also *PoI#5*).

4.1.3. Accuracy

Accuracy is supported by limiting the duration of processing information. For example, the user is automatically removed from interest groups after 30 days,[208] which can also be done explicitly (*PoI#2*);[209] interest group assignments can be removed in response to user actions. Data structures to be considered in the auction phase can be updated (*PoI#3*).

---

[203] 'Protected Audience Documentation' <https://github.com/privacysandbox/fledge-docs> accessed 27 May 2023.

[204] Martin Thomson and Christopher A Wood, 'Oblivious HTTP' (Internet Engineering Task Force 2023) Draft <https://datatracker.ietf.org/doc/draft-ietf-ohai-ohttp> accessed 27 May 2023, section 2.

[205] Supra, Case C-582/14, paras 47-49.

[206] Ibid, paras 44-45. ("… it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject…").

[207] Such points should be addressed in the DPIA.

[208] I.e. user will not be marked as "interested" in something, for example, in five years, in which time the user interest might evolve.

[209] It is then assumed that the associated configuration data is also removed after some time.

4.1.4. Storage limitation

Data is removed after a predefined time. However, as is discussed later, there is likely limited rationale to consider whether the information “permits identification of data subjects for no longer than is necessary”,[210] as nowhere in the design of PAA the support for such “identification” is included. In multiple places, it is ensured that client or user identification is to be difficult or impossible by design (*PoI#5*).

4.1.5. Integrity and confidentiality

For confidentiality, the auction is executed in the user browser (*PoI#4*), with the information never leaving the device (alternatively/optionally — in isolated TEEs). The communication channel is encrypted.

For integrity: processed information may change in response to user actions. Unsanctioned information modification appears impossible in such a tight design.

4.1.6. Accountability

Demonstrability rests on the precise implementation of the specifications. If external servers are to be used, they may be remotely inspectable (via software attestation proving the type of used software). When necessary, it would be the requirement of the parties concerned (i.e. buyers) to demonstrate compliance, for example via a DPIA.

4.1.7. Lawfulness, fairness, and transparency

The browser is responsible for user interfaces informing on aspects such as the interest group assignment. As for the lawfulness,[211] an appropriate basis of

---

[210] GDPR, article 5(1)(e).

[211] GDPR, article 6.

processing should be considered. Several bases may be analysed; for example, performance of a contract,[212] legitimate interests,[213] or consent.[214]

The performance of a contract may not be a suitable basis.[215] Among the reasons may be the fact that the "data controller has not been contracted to carry out profiling".[216] It is unlikely that this could be the case when using PAA when the technical and organisation decoupling between users, the auction execution, and the buyers, is strong. Alternatively, an argument of another nature may apply: "it would be hard to argue that the contract had not been performed because there were no behavioural ads".[217]

Two legal bases may be appropriate for ad targeting: legitimate interests, or consent.[218] In *Fashion ID* CJEU lays out the conditions for processing based on legitimate interests: "1) the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; 2) the need to process personal data for the purposes of the legitimate interests; 3) the condition that the fundamental rights and freedoms of the data subject whose data require protection

---

[212] Ibid, article 6(1)(b).

[213] Ibid, article 6(1)(f).

[214] Ibid, article 6(1)(a).

[215] Working Party 29. 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC844/14 '/EN WP 217 [2014] <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 27 May 2023.

[216] Ibid, p. 17.

[217] European Data Protection Board, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' [2019] <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en> accessed 27 May 2023, pt. 52-53.

[218] European Data Protection Board, 'Guidelines 8/2020 on the Targeting of Social Media Users' [2020] <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en> accessed 27 May 2023, pt. 43.

do not take precedence".[219] Therefore, for *legitimate interests* ground, a *balancing test* must be carried out.[220] [221]

If fundamental freedoms like data protection[222] were not to be impacted to the degree as in the case of the older (or current) behavioral advertising involving the heavy processing of personal data, strong data protection guarantees could contribute to the conclusion that the balance is acceptable. PAA does not work on the principle of monitoring user activity:[223] (1) the ad targeting happens on the device (or in isolation), (2) no personal data is acquired to be brokered subsequently, (3) there are no means for "further processing".[224] This is an important consideration because the *balancing test* must consider impacts on the data subject,[225] taking into account aspects like issues of power imbalance between the user and the controller.[226] The details of processing might tip the balance in favour of the controller.[227] Especially if advanced techniques would be deployed, such as: "technical and organisational measures; extensive use of anonymisation techniques; aggregation of data; privacy-enhancing technologies".[228] These are included in the PAA's design.

Furthermore, if the information was not to be disproportionately processed, or not at all, the impact on the data subject would be low, minimal, or even none. This may

---

[219] Court of Justice of the European Union, Case C-40/17 Fashion ID, 29 July 2019, para. 95.

[220] Supra, Working Party 29 [2014], p. 1.

[221] Supra, EDPB Guidelines 2/2019 [2019], pt. 48.

[222] Supra, Charter of Fundamental Rights, article 8.

[223] See also the next subsection (4.2).

[224] GDPR, recital 47.

[225] Supra, Working Party 29 (2014).

[226] Ibid, p. 40.

[227] Ibid, p. 34, 42.

[228] Ibid, p. 42.

potentially unlock the use of legitimate interests as the basis, at least in some cases. Though then, users would have the right to object.[229]

An alternative basis to consider could be consent,[230] understood as appropriate when profiling may be in use.[231]

4.2. Does ‘data processing’happen in context of Protected Audience API?

A fundamental question to consider is whether personal data processing arises as part of the PAA. It is important to recall where the data is processed. As noted in section 3, the processed information never leaves the user’s web browser (i.e. *user terminal*).[232]

4.2.1. External servers add complexity

As part of PAA, some information is obtained from the buyers (*PoI#3*),[233] which may contain information about concrete products relating to user interests.

An important caveat follows:

- Web browser implementations should be wary of this detail (variety of information).
- It is the task of the buyers to consider whether they process identifiable data that may single out users, as part of their infrastructures. However, this element would

---

[229] GDPR, article 21(1).

[230] See next section.

[231] Supra, EDPB Guidelines 2/2019 [2019], pt. 50-52.

[232] Except for the reports sent in aggregated form, though initially aggregation will not be used. Another point is downloading bidding logic, ad contents, or issuing queries to TEE-servers. According to the design documents, all such requests are to be isolated, which is assumed in this dissertation.

[233] Like trustedBiddingSignals, see section 3.

be relevant for individual buyers and their systems. It is not a direct issue of the processing in the context of the PAA.

- The option to execute the auction process in trusted execution environments (i.e. not on-device) adds complexity. Such environments are assumed to be verifiably isolated from buyers or browser vendors. Appropriate technical and organisational isolation may still guarantee that no external interferences are possible.

The information from the KV servers may complicate the analysis, as it allows sending/receiving additional information. The risk here is limited by the fact that the requests may be of a "static" form. Such calls may include interest group names, or other metadata, but are auditable. As noted previously, this part appears to be sensitive. The servers must be isolated using technical and organisational measures since the list of user interest groups could potentially be identifiable if accessed as a whole. Still, the KV server maintainer may be organisationally unable to use such information to identify particular users, which would limit the risk.[234]

4.2.2. The case of personal data processing

Considering the potential versatility of interest groups stored on the device, it is imaginable that all of the interest groups the user joined (*PoI#1*), when considered holistically, are a very likely candidate for being unique, potentially enabling precise targeting[235] or singling-out the user. Is it, then, *identifiable* in the sense of GDPR? The list of interest group data is not supposed to leave the user's web browser. Accessing the list of interest groups that the user is a member of is impossible.[236] No external party can access it (unlike with cookies, it is not possible to read this information). Since no party, such as a buyer, or advertiser, can access a full list of interest groups, the possibility of linking such information to identifiable persons may be unreasonable. This would be achieved through the use of technical design (i.e. of the web browser), along organisational ones (if only for the involved servers, when in

---

[234] To repeat, since these details appear not to be finalised, the analysis in this dissertation only considers bidding on the device, and without the use of KV servers.

[235] Supra, Nadezhda Purtova (2022), p. 9.

[236] 'Protected Audience API' (*Chrome Developers*, 27 January 2022) <https://developer.chrome.com/docs/privacy-sandbox/fledge/> accessed 23 May 2023.

use). Especially the execution of auctions purely on the device may fulfil the test of non-identifiability by "any person",[237] [238] making the anonymity guarantees strong (however, in general, true anonymisation may be very challenging).[239] [240] The on-device computation part seems to be particularly strong: the processed information cannot be used as an online identifier[241] like cookies. As for the content display part, micro-targeting precautions (*PoI#5*) lend credence to the conclusion that the aim of such design is not to enable the reaching of specific persons.

When such access is impossible technically, it would then be unreasonable to consider it as identifiable. Furthermore, in line with *Breyer*, any foreseen accesses could be made in ways segregated organisationally. Therefore, I conclude, that the list of interest groups is not identifiable information in the sense of GDPR.

With IP address protection (*PoI#7*), online identifiers are also sanitised.[242] The IP masking would be done by providers organisationally separated from other functions in PAA. Theoretically, this operation may be reversed, potentially not meeting the *absolutist*[243] standard of personal data (i.e. that nobody can identify a person), though even data protection authorities reference the 'relative' notion when "personal data are identifiable for one party, while they are not identifiable for another party".[244] The ECJ also prefers the nuanced, risk-based approach.[245] While some information sent to KV servers could potentially become identifiable (still, not necessarily *reasonably*, when organisational separation is adequate, and no other information is

---

[237] Supra, Michèle Finck and Frank Pallas (2020), p. 7.

[238] GDPR, recital 26.

[239] Emily M Weitzenboeck and others, 'The GDPR and Unstructured Data: Is Anonymization Possible?' (2022) 12 International Data Privacy Law 184, p. 6-9.

[240] Supra, Michèle Finck and Frank Pallas (2020), p. 10.

[241] GDPR, recital 30.

[242] GDPR, recital 30.

[243] Supra, Michèle Finck and Frank Pallas (2020), p. 5 (but compare to discussion on p. 25: "worth considering the alternative and ponder what would happen to data protection law if the absolutist approach to identification were adhered to").

[244] Supra, Frederik J Zuiderveen Borgesius (2016), p. 9.

[245] Supra, Daniel Groos and Evert-Ben van Veen (2020), p.4.

available to KV servers), the analysis in this dissertation is based on an on-device processing not involving KV servers.[246]

When considering the execution on the device, and the design details of PAA, it would seem that it may be possible to utilise PAA in ways not processing personal data. Consequently, the information used as part of the PAA operations would not, technically or legally (limited to reasonable means,[247] concerning time, effort, cost, etc.), constitute personal data. To guarantee this, the system must be tightly designed and implemented technically. For example, it must disallow technical leaks via side channels. The risk of using personal data may be further limited by the design of PAA, like the technical microtargeting protection. Organisational precautions must be in place to limit the tracking risk.

Notably, it is not about the processing of pseudonymous[248] data, as no *controller* or *processor*[249] can add identity data to re-identify the user (without user cooperation, that is). The information processing happens on the device; profiling[250] does not arise. No information is read by any party in this system, outside of the (aggregated) reports (*PoI#6*). Unlike in the previous/current system,[251] behavioral targeting based on profiling is not facilitated. Centralisation of data storage/processing is not the case.

---

[246] Depending on the nature of the communication with KV servers, when it does happen, it may affect the outlook of the situation.

[247] Court of Justice of the European Union, Judgment of the General Court (Ninth Chamber), Case T-384/20 [2022] ECLI:EU:T:2022:273, paras 45-46.

[248] GDPR, article 2(5).

[249] GDPR, article 2(7), article 2(8).

[250] GDPR, article 2(4).

[251] Frederik J Zuiderveen Borgesius, 'Singling out People without Knowing Their Names–Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation' (2016) 32 Computer Law & Security Review 256, p. 13.

Personal data[252] are therefore not "*reasonably likely*"[253] to be processed, as supported[254] by the premises of *Breyer.*[255] Similarly to some privacy-enhancing technologies, when the utilised information does not allow for identifying users, avoiding[256] falling in scope of the GDPR provisions may be possible. When users are technically/organisationally not distinguishable,[257] then the "principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person".[258] When it is unreasonable to identify such a user, the information is not personal data.[259] When a system allows operation without the involvement of personal data, it would not fall in the scope of the GDPR.[260] Such a conclusion is not necessarily unprecedented. Some privacy-enhancing technologies, such as multi-party computations, support (or claim to) similar guarantees of not processing personal data.[261]

It is ultimately a matter of the design, the actual implementation, and all the parts functioning together. Still, as explained in section 5 some requirements remain valid due to the current law.

4.3. DPbD

[252] GDPR, article 4(1).

[253] GDPR, recital 26.

[254] Lukas Helminger and Christian Rechberger, 'Multi-Party Computation in the GDPR', Privacy Symposium 2022: Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT) (Springer 2022), p. 6.

[255] Supra, Case C-582/14

[256] Supra, Lukas Helminger and Christian Rechberger (2022), p. 12.

[257] Supra, Michèle Finck and Frank Pallas (2020), p. 3.

[258] GDPR, recital 26.

[259] Supra, Michèle Finck and Frank Pallas (2020), p. 4.

[260] GDPR, article 2(1).

[261] Supra, Lukas Helminger and Christian Rechberger (2022), p. 12.

High relevance of DPbD is due to the notion of “state of the art”,[262] the aspects of “current progress in technology”.[263] Available[264] [265] systems with superior data protection qualities should be the technological standard of choice.[266] In this case — for ad serving.

This does not mean that different (to PAA) high-quality standards cannot be adopted if they offer comparable qualities. However, it would mean that the advertising technologies based on tracking or heavy processing of personal data would become sub-standard.

4.4. Targeting/profiling based on certain information

Targeting or display restraints should be supported[267] to avoid targeting ads along special categories of data.[268] The targeting of political ads must meet transparency obligations,[269] which would require compliance from the buyers bidding in PAA auctions, perhaps even web browser vendors (transparency of user interface). Targeting of political ads based on special categories[270] is also prohibited.[271]

A compliant user-facing transparency interface may be implemented in the browser. Interest groups (*PoI#1*) could be used in the negative sense: adding the user to a

---

[262] GDPR, article 25(1).

[263] Supra, EDPB (2019), paras 18-22.

[264] Lina Jasmontaite and others, ‘Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR’ (2018) 4 Eur. Data Prot. L. Rev. 168, p. 11.

[265] Supra, Ira S Rubinstein and Nathaniel Good (2020) p. 6.

[266] Lee A Bygrave, ‘Data Protection by Design and by Default: Deciphering the EU’s Legislative Requirements’ (2017) 4 Oslo Law Review 105, p. 18.

[267] DSA, article 26(3).

[268] GDPR, article 9(1).

[269] Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising. COM/2021/731 final, Chapter II.

[270] GDPR, article 9(1).

[271] Supra, Proposal for a Regulation on the transparency and targeting of political advertising, article 12(1).

group indicating that some ads should not be displayed.[272] Similar capabilities to avoid the display of ads for brand safety[273] reasons could be included in the bidding phase (*PoI#4*).

4.5. Rationale for data protection principles

While personal data may not be processed in the context of PAA, considering the full spectrum of the system (including the buyer side) may broaden the issue. For this reason, it is still appropriate to consider how such a novel proposal like PAA stands with respect to the principles. Deployers must be wary of maintaining the right balance should they choose to base processing on legitimate interests. Future development of standards, technology, and implementation must be done with extreme care.

5. Consent in PAA

In online behavioural advertising based on tracking and processing personal data, relying on legitimate interests is inappropriate, if only because of the significant personal data processing;[274] the appropriate basis is consent.[275] However, even when assuming that personal data is not processed, the construction of the EU data protection framework means that the need for consent may still be the case. It is central to this section, and an important consideration of this dissertation.

5.1. Rationale for consent

---

[272] Supra, 'FLEDGE', section 3.5. (provides an example of using an 'NoPolitics' interest group that would be used to omit political-like ads).

[273] 'Protected Audience: Integration Guide' (*Android Developers*) <https://developer.android.com/design-for-safety/privacy-sandbox/integration/protected-audience> accessed 1 June 2023.

[274] Frederik J Zuiderveen Borgesius, 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?' (2015) 5 International Data Privacy Law 163, p. 7.

[275] Supra, Frederik J Zuiderveen Borgesius (2015), p. 8.

Even when personal data are not processed, consent may still be necessary due to the *lex specialis,* ePrivacy Directive. Article 5 of the Directive considers confidentiality of the communication.[276] The “listening, tapping, storage or other kinds of interception or surveillance of communication”[277] is prohibited. Article 5(3) requires user consent when information in the user terminal is accessed.[278] The term *personal data* is not used; ePrivacy applies also when personal data processing does not arise.[279] [280] It is meant as a protection of the user terminal from the insertion of “spyware, web bugs, hidden identifiers”.[281] The legislator considered storage of “hidden information”, applied to “trace the activities of the user”.[282] While it is relevant even when personal data thresholds of the GDPR are not reached, non-compliance with ePrivacy article 5(3) may result in non-compliance with relevant GDPR provisions.[283]

When accessing the user terminal, active consent is required,[284] the rationale being the protection of the user “from interference with his or her private sphere, regardless of whether or not that interference involves personal data”.[285] Even when no data is “accessed by advertising network providers when data subjects visit a partner

---

[276] ePrivacy Directive, article 5(1).

[277] Ibid.

[278] ePrivacy Directive, article 5(3).

[279] Supra, Frederik J Zuiderveen Borgesius (2015), p. 12.

[280] Working Party 29. ’Opinion 2/2010 on online behavioural advertising’ 00909/10/EN WP 171 [2010] <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf> accessed 01 June 2023, p. 9.

[281] ePrivacy Directive, recital 24.

[282] Ibid.

[283] Supra, European Data Protection Board. ’Report of the Work Undertaken by the Cookie Banner Taskforce’ (2023), p. 7, para 24.

[284] Court of Justice of the European Union, Judgment of the Court, Case C-673/17 Planet49 [2019] ECLI:EU:C:2019:801, para 56.

[285] Ibid, para 69-71.

website",[286] like in PAA, ePrivacy necessitates consent.[287] [288] [289] Execution of operations causing the user browser to join or leave an interest group (*PoI#1, PoI#2*) modify information in the user terminal, and may suffice to meet ePrivacy Directive thresholds.[290]

The proposed ePrivacy Regulation[291] maintains provisions of the Directive[292]. However, the proposal for a Regulation is similarly outdated when referring to "third-party cookies",[293] soon to be an issue of the past.

The detail of the consent process matter.

5.2. Valid consent

[286] Supra, Working Party 29 (2010), p. 8.

[287] Supra, Frederik J Zuiderveen Borgesius (2015), p. 13.

[288] Supra, Working Party 29, Opinion 06/2014 (2014).

[289] Supra, Working Party 29 (2010), p. 8.

[290] Supra, Working Party 29 (2010), p. 8-9.

[291] 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, ePrivacy Regulation) [due to the length limitations, the version of the European Parliament or the latest Council versions are not compared; the final Regulation text is still not approved in July 2023].

[292] ePrivacy Regulation, articles 5-6.

[293] ePrivacy Regulation, recital 24.

ePrivacy consent refers to the GDPR.[294] [295] [296] Consent must be “freely given, specific, informed and unambiguous”.[297] It should be possible to withdraw it.[298]

Informed consent requires the provision of information,[299] for example about the purposes of processing.[300] It is not specified how it should be provided.[301] However, the information given to the user should be “clear and plain”,[302] and valid consent requires unambiguous, clear, and affirmative action.[303] To be unambiguous, consent must be active, following a user action, or decision.[304]

The obligation to provide information[305] rests on the party that performs the modifying activities (of the user terminal). An explanation of processing must be given.[306] However, some calls in PAA at least appear to be subject to execution at varying times (this is not specified). In such a case, for example, the updating of the configuration data (*PoI#3*) might technically happen (in the background) when browsing unrelated websites. For example, it is imaginable that when browsing a

---

[294] European Data Protection Board. ’Opinion 5/2019 on the Interplay between the EPrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities | European Data Protection Board’ <https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_en> [2019] accessed 2 June 2023, p. 74.

[295] European Data Protection Board. ’Guidelines 05/2020 on Consent under Regulation 2016/679 | European Data Protection Board’ <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en> accessed 2 June 2023, p. 6, para 7.

[296] GDPR, article 94(2).

[297] GDPR, article 4(11).

[298] GDPR, article 7(3).

[299] Supra, Working Party 29 (2010), p. 15. (“clear, comprehensive and fully visible information”).

[300] Supra, Working Party 29 (2010), p. 17.

[301] Supra, European Data Protection Board. Guidelines 05/2020 on Consent (2020), p. 16 (para 66).

[302] Ibid, p. 16 (para 67).

[303] Ibid, p. 18 (paras 75-77).

[304] Supra, European Data Protection Board. Guidelines 05/2020 on Consent (2020), p. 18.

[305] Ibid, p. 18.

[306] Ibid, p. 14.

website (e.g. cnn.com), configuration data for future uses could be downloaded to be used later in the context of unrelated websites (e.g. bbc.co.uk). How to identify the controller, then?[307] [308] Would it be clear to notify the user about such (unrelated) content retrieval when browsing cnn.com in ways not confusing the user? Designers, implementers, or deployers must tackle such issues. What is clear is that the information given should be clear to avoid confusion. Consent obligations for future updates should likely be addressed before any data retrieval. What matters ultimately is informing users.[309]

While fulfilling the needs of informed consent should not be difficult technically,[310] it must be decided where and when this happens: on the website, or as part of the browser interface. The latter could be superior since the interface would be standard for all the visited websites. Deployment aspects may necessitate a case-by-case analysis.

5.3 Technical provision

Consent could be conveyed using various means.[311] For example, on the visited website,[312] as part of the browser interface, and/or perhaps signalled to websites via

---

[307] GDPR, recital 42.

[308] Supra, European Data Protection Board. Guidelines 05/2020 on Consent (2020), p. 15.

[309] Ibid, p. 18.

[310] Ibid, p. 15.

[311] Dominique Machuletz and Rainer Böhme, 'Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR' [2019] Proceedings on Privacy Enhancing Technologies, 2, 481-498, p. 3-4.

[312] Maximilian Hils, Daniel W Woods and Rainer Böhme, 'Measuring the Emergence of Consent Management on the Web', *Proceedings of the ACM Internet Measurement Conference* (2020), p. 2.

the browser.[313] [314] [315] [316] [317] To be meaningful, it should avoid misleading users through lack of information,[318] or using manipulative techniques.[319] Cookie consent collection methods often lack usability.[320] The technical implementation should benefit from such experience and avoid resulting in uninformed consent.[321]

Although in current practice, the information given to the user is sometimes partial, or cookies were found to be set before consent is granted;[322] [323] consent requirements can be translated to technical implementations.[324]

Withdrawing consent is also important.[325] When the publisher or buyer (script-providers) would not hold information about the user, the reasonable way of consent

---

[313] 'Tracking Preference Expression (DNT)' <https://www.w3.org/TR/tracking-dnt/> accessed 2 June 2023.

[314] Do Not Track and Tracking Preferences Expression ultimately were not successful, but are added here as some potential measures.

[315] Maximilian Hils, Daniel W Woods and Rainer Böhme, 'Privacy Preference Signals: Past, Present and Future' (2021) 4 Proceedings on Privacy Enhancing Technologies 249, p. 13-14.

[316] 'Global Privacy Control (GPC)' <https://privacycg.github.io/gpc-spec/> accessed 2 June 2023.

[317] Sebastian Zimmeck and others, 'Usability and Enforceability of Global Privacy Control' (2023) 2 Proceedings on Privacy Enhancing Technologies 1, p. 6.

[318] Cristiana Santos and others, 'Cookie Banners, What's the Purpose? Analyzing Cookie Banner Text Through a Legal Lens', *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society* (2021), p. 3.

[319] PAJ Graßl and others, 'Dark and Bright Patterns in Cookie Consent Requests' (2021) 3 Journal of Digital Social Research 1, p. 25-26.

[320] Hana Habib and others, "'Okay, Whatever": An Evaluation of Cookie Consent Interfaces', *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (2022), p. 10.

[321] Christine Utz and others, '(Un) Informed Consent: Studying GDPR Consent Notices in the Field', *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security* (2019), p. 3-4.

[322] Cristiana Santos, Nataliia Bielova and Célestin Matte, 'Are Cookie Banners Indeed Compliant with the Law? Deciphering Eu Legal Requirements on Consent and Technical Means to Verify Compliance of Cookie Banners' [2019] arXiv preprint arXiv:1912.07144, p. 17, 36.

[323] Martino Trevisan and others, '4 Years of EU Cookie Law: Results and Lessons Learned' (2019) 2019 Proceedings on Privacy Enhancing Technologies 126, p. 9.

[324] Cristiana Santos, Nataliia Bielova and Célestin Matte (2019), p. 4-5.

[325] Supra, European Data Protection Board. Guidelines 05/2020 on Consent (2020), p. 23.

withdrawal is reseting browser configuration that would remove the assigned interest groups (*PoI#1*), or any configuration data.

However, technical design and implementation may motivate concerns of another nature.

6. Competition aspects and privacy vs competition

Limiting tracking and phasing out third-party cookies rejuvenate debates around the competition consequences of technological changes, including the effects of privacy-motivated evolution.

Technology developments in an existing market are in the scope of competition proceedings, especially when introduced by undertakings[326] [327] holding dominant positions.[328] [329]
This premise may partly explain the openness by Google, when working on the Privacy Sandbox.[330]

6.1. Competition and data protection laws

[326] Treaty on the Functioning of the European Union, OJ C 115, article 101.

[327] Court of Justice of the European Union. Judgment of the Court (Third Chamber) of 14 December 2006. Confederación Española de Empresarios de Estaciones de Servicio v Compañía Española de Petróleos [2006] ECLI:EU:C:2006:784 , Case C-217/05, par. 39.

[328] Treaty on the Functioning of the European Union, OJ C 115, article 102(1).

[329] European Commission. 'Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings', 2009/C 45/02, paras. 9-10 <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A52009XC0224%2801%29%3AEN%3AHTML> accessed 20 June 2023.

[330] Damien Geradin and Dimitrios Katsifis, 'Taking a Dive into Google's Chrome Cookie Ban', p. 9.

Competition investigations require understanding the links between numerous areas.[331] Privacy improvement should count as technological progress. If privacy qualities may offer competitive advantages, they could become the subject of competition investigations.[332] An important goal of competition law is the promotion of innovation.[333] TFEU lays out the legal grounds for competition protection, listing[334] technological progress as a point to consider. The European Commission (EC) considers privacy a non-price parameter[335] in competition proceedings.[336] The Parliament supports it.[337] The EU EDPS is aware of the links and convergences[338] between privacy and competition, investigating joint enforcement of data protection and competition.[339] While competing with privacy may have economic justification,[340] competition, and data protection laws serve different purposes.[341] Still, data

---

[331] Christophe Carugati, 'The Antitrust Privacy Dilemma' [2023] European Competition Journal 1, p. 3-4.

[332] Ibid, p. 8.

[333] Rupprecht Podszun and Stefan Kreifels, 'Digital Platforms and Competition Law' (2016) 5 Journal of European Consumer and Market Law 33. p. 1.

[334] Treaty on the Functioning of the European Union OJ C 326, article 101(3).

[335] Selcukhan Unekbas, 'Competition, Privacy, and Justifications: Invoking Privacy to Justify Abusive Conduct under Article 102 TFEU' [2022] Journal of Law, Market & Innovation, p. 12.

[336] European Commission (2021). 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A competition policy fit for new challenges - COM(2021)713' <https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2021)713&lang=en> accessed 6 June 2023, p. 15.

[337] European Parliament resolution of 5 May 2022 on competition policy — annual report 2021 (2021/2185(INI)) 2022 OJ C 465, para. 61.

[338] European Data Protection Supervisor. 'Privacy and Competitiveness in the Age of Big Data' (2014) <https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-and-competitiveness-age-big-data_en> accessed 6 June 2023. p. 31-33, 37.

[339] European Data Protection Supervisor. 'The Coherent Enforcement of Fundamental Rights in the Age of Big Data' (2016) <https://edps.europa.eu/sites/default/files/publication/16-09-23_bigdata_opinion_en.pdf> accessed 6 June 2023. p. 10-11.

[340] Ramon Casadesus-Masanell and Andres Hervas-Drane, 'Competing with Privacy' (2015) 61 Management Science 229, p. 16.

[341] Court of Justice of the European Union. Judgment of 23 November 2006, ASNEF-EQUIFAX and Administración del Estado, C-238/05 ECLI:EU:C:2006:734, para. 63. ("issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection").

protection can be considered in the context of competition,[342] [343] and it is.[344] [345] Furthermore, in EU Member States data protection is also being considered in competition investigations, such as in the Apple case.[346]

6.2. Competition aspects of Privacy Sandbox

In PAA, the browser is the core mediator between the user, the website, and the buyer(s).[347]

Ad technologies are the subject of interest of several anti-trust bodies. The most consequential proceeding related to Privacy Sandbox is carried out by the UK Competition and Markets Authority (CMA), working with UK Information Commissioner Office.[348] Analysing Privacy Sandbox changes is a case where data protection and competition aspects are closely linked.[349]

---

[342] de Moncuit, A. In which ways should privacy concerns serve as an element of the competition assessment, available at: https://ec.europa.eu/competition/information/digitisation_2018/contributions/aymeric_de_moncuit.pdf, p. 3-4.

[343] Court of Justice of the European Union. Meta Platforms Inc. and Others v Bundeskartellamt [2023] ECJ Case C-252/21 ECLI:EU:C:2023:537, paras 43, 48, 51-52, 59, 62.

[344] European Commission (2016). Commission's decision of 6 December 2016 in Case M.8124 - Microsoft/LinkedIn, paras 121, 255.

[345] Commission Decision of 03/10/2014 declaring a concentration to be compatible with the common market (Case No COMP/M.7217 - FACEBOOK / WHATSAPP) according to Council Regulation (EC) No 139/2004, para. 87. ("according to the market investigation, important areas of improvement include: (i) reliability of the communications service, which has a direct impact on the service's reputation and its appeal to users; and (ii) privacy and security").

[346] *Autorité de la concurrence.* 'Decision 21-D-07 of March 17, 2021' (17 March 2021) <https://www.autoritedelaconcurrence.fr/en/decision/regarding-request-interim-measures-submitted-associations-interactive-advertising-bureau> accessed 19 June 2023.p. 15-17.

[347] Supra, Dylan A Cooper and others (2023), p. 5.

[348] 'CMA-ICO Joint Statement on Competition and Data Protection Law' (*GOV.UK*) <https://www.gov.uk/government/publications/cma-ico-joint-statement-on-competition-and-data-protection-law> accessed 6 June 2023, p. 26-28.

[349] Ibid, p. 28-29.

The CMA started its investigation to asses if “the proposals could cause advertising spend to become even more concentrated on Google’s ecosystem”,[350] acknowledging that “third party cookies currently play a fundamental role online and in digital advertising”.[351] The investigation[352] considered the risk of Google’s self-preferencing, and potential harm to users,[353] including input from stakeholders. The CMA agreed to commitments[354] requiring openness of the design,[355] transparency,[356] of implementation, test and deployment measures, and non-discrimination against rivals.[357] The commitments were accepted,[358] acknowledging that Google may hold a dominant position in the supply of web browsers.[359] The openness of technology tests remains under scrutiny.[360]

---

[350] Competition and Markets Authority. ‘CMA to Investigate Google’s “Privacy Sandbox” Browser Changes’ (*GOV.UK*) [2021] <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1036204/211126_FINAL_modification_notice.pdf> accessed 6 June 2023.

[351] Ibid.

[352] Competition and Markets Authority. ‘Notice of intention to accept modified commitments offered by Google in relation to its Privacy Sandbox Proposals Case number 50972’ [2021] <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1036204/211126_FINAL_modification_notice.pdf> accessed 6 June 2023.

[353] Ibid, p. 10, para 2.3. (”allow Google to exploit its likely dominant position by denying Chrome web users substantial choice in terms of whether and how their personal data is used”).

[354] Competition and Markets Authority. ‘Privacy Sandbox Google Commitments Offer’ [2022] <https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf> accessed 6 June 2023.

[355] Ibid, p. 4-5, para C.8.

[356] Ibid, p. 10-11, paras D.10-11.

[357] Ibid, p. 12, para H.30.

[358] Competition and Markets Authority. ‘Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals Case number 50972’ [2022] <https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf> accessed 6 June 2023, p. 169, paras 5.2-5.3.

[359] Ibid, p. 22, paras 2.47-2.48.

[360] Competition and Markets Authority. ‘Quantitative testing of Google’s Privacy Sandbox technologies – seeking input from affected firms and others on the CMA’s proposals’ [2022] <https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf> accessed 6 June 2023, p. 2, paras 4-5.

While the ecosystem is moving towards a tracking-less reality, the economic impact of tracking limitations indicates that even reducing the cookie lifetime may decrease their monetary value.[361] This is in contrast to previous results arguing a lack of relationship between data value and its lifetime.[362]

However, comparing PAA to cookies is inappropriate. PAA would function in an ecosystem where third-party cookies are not an alternative.

6.3. Competition standards

While scholarship and technical considerations for privacy are rich, this is not the case for competition aspects. Chances are that standards will emerge eventually, if only motivated by the EU DMA's[363] emphasis on *interoperability*,[364] which *gatekeepers*,[365] such as web browser vendors,[366] or advertising services provided by undertakings supplying web browsers,[367] [368] must guarantee.[369] The DMA also prohibits combining and cross-using personal data from different divisions of the gatekeeper,[370] which places data protection in the scope of competition.[371] The DMA

---

[361] Klaus M Miller and Bernd Skiera, 'Economic Consequences of Online Tracking Restrictions' [2023] arXiv preprint arXiv:2303.09147, p. 5. ("a large European ad exchange").

[362] Lesley Chiou and Catherine Tucker, 'SEARCH ENGINES AND DATA RETENTION: IMPLICATIONS FOR PRIVACY AND ANTITRUST', p. 18-19.

[363] Supra, DMA.

[364] Ibid, article 2(29).

[365] Ibid, article 2(1), article 5.

[366] Ibid, article 2(2)(g).

[367] Ibid, article 2(2)(j).

[368] Specifically, Google, the developer of Chrome web browser, and the proponent of Privacy Sandbox.

[369] Ibid, article 6(7).

[370] Ibid, article 5(2)(b)-(c).

[371] Ibid, recital 10-11.

is *complementary*[372] to the EU competition law framework by functioning *ex-ante*.[373] It is justified to expect that such a framework may result in the development of technical standards for competition compliance.

An important point to consider is that the CMA is a UK regulator, and the UK is no longer part of the EU. While the decisions of UK and EU regulators need not be identical, the UK competition framework[374] [375] appears closely related to the EU one.[376] The instrument of commitment exists in the EU[377] and the UK.[378] While the CMA investigation remains relevant, the practical consequences adopted in Privacy Sandbox still effectively impact (help) users and businesses in the EU.

Finally, even the CMA's in-depth investigation did not consider some technical design features. For example, "Chrome allows up to 1000 interest groups per owner [buyer], and up to 1000 interest group owners" (PoI#1).[379] Such an implementation choice has a direct impact on the market size, enacting a hard limit on the number of undertakings.

7. Future steps

---

[372] Viktoria HSE Robertson, 'The Complementary Nature of the Digital Markets Act and Articles 101 and 102 TFEU' [2023] DMA working group (European Parliament's IMCO), p. 3.

[373] Ibid, p. 5.

[374] Competition Act 1998 <https://www.legislation.gov.uk/ukpga/1998/41/contents> accessed 7 June 2023.

[375] The Competition (Amendment Etc.) (EU Exit) Regulations 2019 <https://www.legislation.gov.uk/uksi/2019/93/contents> accessed 7 June 2023.

[376] Alison Jones, 'Brexit: Implications for UK Competition Law' [2017] King's College London Law School Research Paper, p. 1.

[377] Council of the European Union. Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (Text with EEA relevance) [2002], Official Journal L 001, article 9(1).

[378] Competition Act 1998, s. 31A.

[379] 'Buyer Guide: Join Interest Groups and Generate Bids' (*Chrome Developers*, 1 November 2022) <https://developer.chrome.com/docs/privacy-sandbox/fledge-api/interest-groups/> accessed 7 June 2023.

After discussing the “Privacy Sandbox” and aspects of EU law it is appropriate to consider what could or should, be considered in the future for the legal or regulatory landscape.

7.1. Facilitate the use of technology with superior privacy qualities

It appears to be possible to use PAA in ways not processing personal data. That is a clear improvement concerning the current industry standards. However, even when a system does not process personal data, certain uses of *information* (storage, access) necessitate asking the user for consent.[380] ePrivacy played a crucial and necessary role in the protection of the confidentiality of user information. Is such broad reach still justified in the current, and the future, technological landscape, considering the current evolution? Confidentiality and user terminal must remain protected from unsanctioned “spyware, web bugs, hidden identifiers”,[381] and other tracking techniques. However, with third-party cookies phased out, this part of the legislation’s motivation may lose relevance. There is an opportunity for the driver of the web economy to cease being the ‘Wild West’ for tracking users.

Not admitting the consequences of the ePrivacy Directive in such a reality would be unfortunate. It could potentially bring undesirable impacts on the future development of privacy-improving or preserving technologies. Such technology may process information, in ways that are privacy-respecting, with high data protection qualities, for example not involving personal data. Still, with current ePrivacy, asking for user consent may be necessary, even when user data confidentiality is not affected. When user information is handled in appropriate ways, but the user is still faced with a consent query, the user might not appreciate the improvement. In such circumstances, the source of such undesirable effects would be the existing law. Such a regulatory characteristic might even have undesirable effects of stymying or inhibiting the development of privacy-preserving technologies. Therefore, the framework should be readjusted, making the law fit for the purpose.

---

[380] ePrivacy Directive, article 5(3).

[381] ePrivacy Directive, recital 24.

Not admitting that users complain about the ever-present consent popups is untenable. Aware of these concerns, EC is working on simplifying measures.[382] Realising that some technology may help to put consent popups to rest could be productive. While respecting the EDPB observation that “many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day”,[383] it is clear that on the European web there is a deluge of consent popups, which at a scale may be disrupting or even “annoying”.[384] Considering this ‘annoyance’, and mixed results of the legal provisions implemented in practice in ways flooding the users with cookie consent popups, some argue that such a ‘consent theatre’ should be phased out.[385] It appears that systems not processing personal data could offer a way out. While the cookie-notice flood remains a problem, with the uses of PAA not processing personal data, the root of the problem would be the existing law (ePrivacy).

Among the takeaways of this dissertation is therefore the need to align the legal landscape to support approaches that handle user data with appropriate care, and specifically aim not to process personal data (imaginably, this is an issue not limited to PAA). Provisions balancing the consequences of ePrivacy Directive’s article 5(3), or exemptions — like in the case of the Directive, when cookies are strictly necessary[386] — should be considered. The changes should not lower the protections.

Tracking technologies working similarly to third-party cookies should remain under supervision. Processing information not involving personal data could be a

---

[382] Luca Bertuzzi. ’Cookie Fatigue: The Questions Facing the EU Commission Initiative – EURACTIV.Com’ <https://www.euractiv.com/section/data-privacy/news/cookie-fatigue-the-questions-facing-the-eu-commission-initiative/> accessed 7 June 2023.

[383] Supra, European Data Protection Board. Guidelines 05/2020 on Consent (2020), p. 19.

[384] Andrea Maria Garofalo, ‘Cookies and the Passive Role of the Data Subject’ [2022] Privacy and Data Protection in Software Services 73, p. 7.

[385] Fassl, M., Gröber, L. T., & Krombholz, K. (2021, May). Stop the consent theater. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-7), p. 5.

[386] ePrivacy Directive, article 5(3).

requirement in such a narrow exemption. Such exceptions could reduce the friction of the frequently displayed consent notices, a consequence of ePrivacy.

The EC is aware that parts of the ePrivacy Directive are “outdated”.[387] When considering ePrivacy reform, consumer NGOs focused on the risks of tracking and the need to uphold the protection by ePrivacy.[388]
Industry boards argued for repealing of ePrivacy Directive article 5(3), or introducing exceptions (different from the ones suggested here).[389] As was argued, it is justified with legal developments in the EU, for example, that protection of confidentiality and online identifiers are explicitly mentioned in the GDPR.[390]
The EDPB advises that updates to ePrivacy should not lower the protections, the exceptions should be narrow,[391] and consent requirements for cookies or ‘similar technologies’ should be stipulated.[392] However, dissimilar technologies (also requiring consent) were not considered.
The EDPS highlights the need to keep the terminal-access provisions[393] but it also admits that ePrivacy has “failed to live up to its potential to provide a genuine opportunity to choose, and to give control to the individuals”,[394] and expresses

---

[387] REFIT Evaluation and Impact Assessment of Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2017) <https://ec.europa.eu/smart-regulation/roadmaps/docs/2016_cnect_013_review_eprivacy_en.pdf> accessed 9 June 2023, p.4.

[388] Access Now. ’Review of the e-Privacy Directive<https://www.accessnow.org/wp-content/uploads/2016/12/Access-Now-ePrivacy-Directive-policy-paper.pdf> accessed 9 June 2023, p. 7-8.

[389] ‘POSITION ON THE REVIEW OF THE ePRIVACY DIRECTIVE’ (*Internet Advertising Bureau*) <https://iabeurope.eu/wp-content/uploads/2020/06/20161201_IAB-Europe-Position-on-ePrivacy-Directive-Review.pdf> accessed 9 June 2023, p. 5.

[390] GDPR, recital 30, article 4(1).

[391] European Data Protection Board. ’Statement of the EDPB on the Revision of the ePrivacy Regulation and Its Impact on the Protection of Individuals with Regard to the Privacy and Confidentiality of Their Communications’ <https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_en.pdf> accessed 5 June 2023, p. 1.

[392] Ibid, p. 3.

[393] European Data Protection Supervisor. ‘EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)’ (24 April 2017) <https://edps.europa.eu/data-protection/our-work/publications/opinions/eprivacy-regulation_en> accessed 9 June 2023, p. 16-17.

[394] Ibid, p. 17.

concern about barring the entrance to websites if consent for cookies is not granted.[395]

In PAA, cookies are not used, and it can be used in ways not tracking user behaviour. It thus may be in line with the advice expressed by the EDPS.

Lastly, the ePrivacy Regulation proposed in 2017 does not account for the sunset of third-party cookies and the emergence of cookie-less technologies that would not be based on tracking or disproportionate processing of personal data. Considering that this would be part of an important market activity in the EU, it would be appropriate to reconcile solutions such as PAA, placing them on reasonable regulatory grounds. Article 8 of the ePrivacy Regulation proposal considering “use of processing and storage capabilities of terminal equipment”[396] should reflect this.

7.2. Soft-law

Considering the activities of regulators, such as the EDPB, the European Board for Digital Services,[397] and the high-level group for the DMA[398] is important. Guidelines should be developed to accommodate for the current-era technology uses, how the law may apply to certain uses, but also how the new technology developments may result in new complexities for data protection, competition, and reconciling the two at the same time. Specific legal grounds for the cooperation of data protection regulators and competition regulators should be introduced.

7.3. Generative AI

---

[395] Ibid.

[396] ePrivacy Regulation proposal, article 8.

[397] Ibid, DSA, article 61.

[398] Ibid, DMA, article 40.

Generative AI may enable the creation of dynamic, real-time ad production,[399] including at the time of the user's visit to a website, even near the time of the ad auction (*PoI#4*). It is not clear how future development of PAA would account for real-time-generated content. Generative AI uses may fall in the scope of the AI Act,[400] necessitating compliance with additional requirements, if only for transparency purposes.

8. Conclusion

This dissertation analysed Protected Audience API and its standing concerning EU data protection laws. Uses of PAA may be reconciled with EU data protection laws. Furthermore, it appears to be possible to use PAA in ways not processing personal data. Proposals such as PAA[401] introduce qualitative changes that may warrant specific treatment by regulations. Currently, this is not the case. If only as evidenced by the lack of recitals in regulations referencing technologies even close to PAA.

EU Data Protection law with respect to web user monitoring is partly motivated by user tracking, a substantial problem of the 2000s and 2010s. This is evident due to applicable laws explicitly referencing cookies or similar approaches. The use of such capabilities is being reduced or phased out (in the optimistic scenario). As such, developing laws to account for the realities of technology is appropriate. The GDPR is fit for purposes, but ePrivacy Directive[402] should be adjusted to bring it in line with reality.

---

[399] 'Introducing a new era of AI-powered ads with Google' (2023) <https://blog.google/products/ads-commerce/ai-powered-ads-google-marketing-live/> accessed 9 June 2023.

[400] DRAFT Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9 0146/2021 – 2021/0106(COD)) (2023) <https://www.europarl.europa.eu/resources/library/media/20230516RES90302/20230516RES90302.pdf> accessed 9 June 2023, article 28b.

[401] Potentially also others, like Apple's: 'The Storage Access API' <https://privacycg.github.io/storage-access/> accessed 9 June 2023.

[402] Even the proposal for a Regulation introduced in 2017 and still being in-development (stalled) in mid 2023.

While technology like PAA can be reconciled with EU data protection, a consideration of the developing standards, fairness,[403] ethics of use, and competition aspects are examples for future research.

Finally, considering the current mass spread of consent notices on websites in Europe, it is justified to ask if it is reasonable when solutions with improved data protection qualities are in place.

Bibliography

Primary sources

European treaties

1. European Convention on Human Rights [1950].
2. Charter of Fundamental Rights of the European Union [2012] OJ C 326.
3. Treaty on the Functioning of the European Union (TFEU) [2012] OJ C 326.

Directives, regulations

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) [2016] OJ L 119/1.
2. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, ePrivacy Directive) [2002] OJ L 201.
3. 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

[403] 'Digital fairness – fitness check on EU consumer law' (2022) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en> accessed 9 June 2023.

electronic communications and repealing Directive 2002/58/EC [2017] COM/2017/010 final - 2017/03 (COD).

4. Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment, OJ L 162.
5. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act, DMA) [2022] PE/17/2022/REV/1 OJ L 265.
6. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act, DSA) [2022] PE/30/2022/REV/1 OJ L 277, article 26(3).
7. Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising. COM/2021/731 final.
8. 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, ePrivacy Regulation).
9. Council of the European Union. Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (Text with EEA relevance) [2002], Official Journal L 001.
10. DRAFT Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9 0146/2021 – 2021/0106(COD)) (2023) <https://www.europarl.europa.eu/resources/library/media/20230516RES90302/20230516RES90302.pdf> accessed 9 June 2023.

Court cases

1. Court of Justice of the European Union, Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014].
2. Court of Justice of the European Union, Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779.
3. Court of Justice of the European Union, Case C-70/10 Scarlet Extended [2011] ECLI:EU:C:2011:771.
4. Benedik v. Slovenia Application no. 62357/14 (ECtHR 24 April 2018) [2018].
5. Court of Justice European Union, Case C-40/17 Fashion ID, 29 July 2019.
6. Court of Justice of the European Union, Judgment of the General Court (Ninth Chamber), Case T-384/20 [2022] ECLI:EU:T:2022:273.
7. Court of Justice of the European Union, Judgment of the Court, Case C-673/17 Planet49 [2019] ECLI:EU:C:2019:801.
8. Court of Justice of the European Union. Judgment of the Court (Third Chamber) of 14 December 2006. Confederación Española de Empresarios de Estaciones de Servicio v Compañía Española de Petróleos [2006] ECLI:EU:C:2006:784 , Case C-217/05.
9. Court of Justice of the European Union. Judgment of 23 November 2006, ASNEF-EQUIFAX and Administración del Estado, C-238/05 ECLI:EU:C:2006:734.
10. Court of Justice of the European Union, Meta Platforms Inc. and Others v Bundeskartellamt [2023] ECJ Case C-252/21 ECLI:EU:C:2023:537.
11. Court of Justice of the European Union. Meta Platforms Inc. and Others v Bundeskartellamt [2023] ECJ Case C-252/21 ECLI:EU:C:2023:537.

National laws

1. Competition Act 1998. (UK)
2. The Competition (Amendment Etc.) (EU Exit) Regulations 2019. (UK)

Regulator opinions, decisions, or communication

1. European Data Protection Board. ’Report of the Work Undertaken by the Cookie Banner Taskforce’ <https://edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en> accessed 5 June 2023.
2. Working Party 29, Opinion 05/2014 on Anonymisation Techniques, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 15 May 2023.
3. Working Party 29, Opinion 4/2007 on the concept of personal data, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 15 May 2023.
4. Working Party 29. ’Opinion 03/2013 on purpose limitation’ 00569/13/EN WP 203 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> (2013), accessed 18 May 2023.
5. European Data Protection Board, ‘Guidelines 4/2019 on Article 25 Data Protection by Design and by Default’, [2019] <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf>, accessed 19 May 2023.
6. Working Party 29. ’Guidelines on Data Protection Impact Assessment (DPIA)’ 17/EN WP 248 <https://ec.europa.eu/newsroom/document.cfm?doc_id=44137> (2017) accessed 24 May 2023.
7. CNIL. Deliberation SAN-2023-009 of June 15, 2023 (CRITEO sanctionné d’une amende de 40 millions d’euros) <https://www.cnil.fr/fr/publicite-personnalisee-criteo-sanctionne-dune-amende-de-40-millions-deuros> accessed 22 June 2023.
8. Working Party 29. ’Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC’ 844/14/EN WP 217 [2014] <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 27 May 2023.
9. European Data Protection Board, ’Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects’ [2019] <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en> accessed 27 May 2023.

10. European Data Protection Board, ’Guidelines 8/2020 on the Targeting of Social Media Users’ [2020] <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en> accessed 27 May 2023.
11. Working Party 29. ’Opinion 2/2010 on online behavioural advertising’ 00909/10/EN WP 171 [2010] <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf> accessed 01 June 2023.
12. European Data Protection Board. ’Opinion 5/2019 on the Interplay between the ePrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities | European Data Protection Board’ <https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_en> [2019] accessed 2 June 2023.
13. European Data Protection Board. ’Guidelines 05/2020 on Consent under Regulation 2016/679 | European Data Protection Board’ <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en> accessed 2 June 2023.
14. European Commission. ’Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings’, 2009/C 45/02, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A52009XC0224%2801%29%3AEN%3AHTML> accessed 20 June 2023.
15. European Commission (2021). ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A competition policy fit for new challenges - COM(2021)713’ <https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2021)713&lang=en> accessed 6 June 2023.
16. European Parliament resolution of 5 May 2022 on competition policy — annual report 2021 (2021/2185(INI)) 2022 OJ C 465.
17. European Data Protection Supervisor. ‘Privacy and Competitiveness in the Age of Big Data’ (2014) <https://edps.europa.eu/data-protection/our-work/

publications/opinions/privacy-and-competitiveness-age-big-data_en> accessed 6 June 2023.

18. European Data Protection Supervisor. ‘The Coherent Enforcement of Fundamental Rights in the Age of Big Data’ (2016) <https://edps.europa.eu/sites/default/files/publication/16-09-23_bigdata_opinion_en.pdf> accessed 6 June 2023
19. European Commission (2016). Commission’s decision of 6 December 2016 in Case M.8124 - Microsoft/LinkedIn.
20. Commission Decision of 03/10/2014 declaring a concentration to be compatible with the common market (Case No COMP/M.7217 - FACEBOOK / WHATSAPP) according to Council Regulation (EC) No 139/2004.
21. Autorité de la concurrence. ’Decision 21-D-07 of March 17, 2021’ (17 March 2021) <https://www.autoritedelaconcurrence.fr/en/decision/regarding-request-interim-measures-submitted-associations-interactive-advertising-bureau> accessed 19 June 2023.
22. ‘CMA-ICO Joint Statement on Competition and Data Protection Law’ (GOV.UK) <https://www.gov.uk/government/publications/cma-ico-joint-statement-on-competition-and-data-protection-law> accessed 6 June 2023.
23. Competition and Markets Authority. ‘CMA to Investigate Google’s “Privacy Sandbox” Browser Changes’ (GOV.UK) [2021] <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1036204/211126_FINAL_modification_notice.pdf> accessed 6 June 2023.
24. Competition and Markets Authority. ‘Notice of intention to accept modified commitments offered by Google in relation to its Privacy Sandbox Proposals Case number 50972’ [2021] <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1036204/211126_FINAL_modification_notice.pdf> accessed 6 June 2023
25. Competition and Markets Authority. ‘Privacy Sandbox Google Commitments Offer’ [2022] <https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf> accessed 6 June 2023.

26. Competition and Markets Authority. ‘Decision to accept commitments offered by Google in relation to its Privacy Sandbox Proposals Case number 50972’ [2022] <https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf> accessed 6 June 2023.
27. Competition and Markets Authority. ‘Quantitative testing of Google’s Privacy Sandbox technologies – seeking input from affected firms and others on the CMA’s proposals’ [2022] <https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf> accessed 6 June 2023.
28. REFIT Evaluation and Impact Assessment of Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2017) <https://ec.europa.eu/smart-regulation/roadmaps/docs/2016_cnect_013_review_eprivacy_en.pdf> accessed 9 June 2023.
29. European Data Protection Board. ’Statement of the EDPB on the Revision of the ePrivacy Regulation and Its Impact on the Protection of Individuals with Regard to the Privacy and Confidentiality of Their Communications’ <https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_en.pdf> accessed 5 June 2023.
30. European Data Protection Supervisor. ‘EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)’ (24 April 2017) <https://edps.europa.eu/data-protection/our-work/publications/opinions/eprivacy-regulation_en> accessed 9 June 2023.

Secondary sources

Scholarship

1. Meaghan Donahue, “‘Times They Are a Changin”-Can the Ad Tech Industry Survive in a Privacy Conscious World?’ (2021) 30 Cath. UJL & Tech 193.

2. Jonathan R Mayer and John C Mitchell, ‘Third-Party Web Tracking: Policy and Technology’, 2012 IEEE symposium on security and privacy (IEEE 2012).
3. Adam Barth, RFC 6265: HTTP State Management Mechanism [2011] (RFC Editor 2011).
4. Sit, E., & Fu, K. (2001). Inside risks: Web cookies: not just a privacy risk. Communications of the ACM, 44(9), 120.
5. Balachander Krishnamurthy and Craig Wills, ‘Privacy Diffusion on the Web: A Longitudinal Perspective’, Proceedings of the 18th international conference on World wide web (2009).
6. Konrad Kollnig and others, ‘Goodbye Tracking? Impact of IOS App Tracking Transparency and Privacy Labels’, 2022 ACM Conference on Fairness, Accountability, and Transparency (2022).
7. Dylan A Cooper and others, ‘Privacy Considerations for Online Advertising: A Stakeholder’s Perspective to Programmatic Advertising’ (2023) 40 Journal of Consumer Marketing 235.
8. Shawn HE Harmon, ‘Review of Reinventing Data Protection?’ (2010) 4 Studies in Ethics, Law, and Technology.
9. Gloria González Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, vol 16 (Springer Science & Business 2014).
10. European Court of Human Rights, 'Guide to the Case-Law of the of the European Court of Human Rights, Data protection’ <https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf> [2022] accessed 23.05.2023
11. European Court of Justice, ‘Fact Sheet, PROTECTION OF PERSONAL DATA'<https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf> accessed 15 May 2023.
12. Christopher Docksey and Gabriela Zanfir-Fortuna, ‘Article 16 [Protection of Personal Data] (Ex-Article 286 TEC)’, Treaty on the Functioning of the European Union-A Commentary: Volume I: Preamble, Articles 1-89 (Springer 2021).
13. Nadezhda Purtova, ‘From Knowing by Name to Targeting: The Meaning of Identification under the GDPR’ (2022) 12 International Data Privacy Law 163.
14. Michèle Finck and Frank Pallas, ‘They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR’ (2020) 10 International Data Privacy Law 11.

15. Frederik Zuiderveen Borgesius, ‘The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition’ (2017) 3 Eur. Data Prot. L. Rev. 130.
16. Daniel Groos and Evert-Ben van Veen, ‘Anonymised Data and the Rule of Law’ (2020) 6 Eur. Data Prot. L. Rev. 498.
17. Aloni Cohen and Kobbi Nissim, ‘Towards Formalizing the GDPR’s Notion of Singling out’ (2020) 117 Proceedings of the National Academy of Sciences 8344.
18. Fredrik Blix, Salah Addin Elshekeil and Saran Laoyookhong, ‘Data Protection by Design in Systems Development: From Legal Requirements to Technical Solutions’, 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST) (IEEE 2017).
19. Célestin Matte, Cristiana Santos and Nataliia Bielova, ‘Purposes in IAB Europe’s TCF: Which Legal Basis and How Are They Used by Advertisers?’, Privacy Technologies and Policy: 8th Annual Privacy Forum, APF 2020, Lisbon, Portugal, October 22–23, 2020, Proceedings 8 (Springer 2020).
20. Bert-Jaap Koops, ‘The Concept of Function Creep’ (2021) 13 Law, Innovation and Technology 29.
21. Dara Hallinan and Frederik Zuiderveen Borgesius, ‘Opinions Can Be Incorrect! In Our Opinion. On the Accuracy Principle in Data Protection Law’ [2020] Our Opinion. On the Accuracy Principle in Data Protection Law, International Data Privacy Law, 10(1), 1-10.
22. Magda Brewczyńska, Suzanne Dunn and Avihai Elijahu, ‘Data Privacy Laws Response to Ransomware Attacks: A Multi-Jurisdictional Analysis’ [2019] Regulating New Technologies in Uncertain Times 281.
23. Tuulia Karjalainen, ‘All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm’ (2022) 8 Eur. Data Prot. L. Rev. 19.
24. Ira S Rubinstein and Nathaniel Good, ‘The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default’ (2020) 10 International Data Privacy Law 37.
25. Lee A Bygrave, ‘Data Protection by Design and by Default: Deciphering the EU’s Legislative Requirements’ (2017) 4 Oslo Law Review 105.

26. Seda Gürses, Carmela Troncoso and Claudia Diaz, ‘Engineering Privacy by Design Reloaded’, Amsterdam Privacy Conference (2015).
27. Nicolás Notario and others, ‘PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology’, 2015 IEEE Security and Privacy Workshops (IEEE 2015).
28. Martino Trevisan and others, ‘4 Years of EU Cookie Law: Results and Lessons Learned’ (2019) 2019 Proceedings on Privacy Enhancing Technologies 126.
29. Raymund Werle and Eric J Iversen, ‘Promoting Legitimacy in Technical Standardization’ (2006) 2 Science, Technology & Innovation Studies 19.
30. Alison Harcourt, George Christou and Seamus Simpson, ‘Internal Governance of the IETF, W3C and IEEE: Structure, Decision-Making and Internationalisation’, Global Standard Setting in Internet Governance (Oxford University Press 2020).
31. Chris Riley, ‘Unpacking Interoperability in Competition’ (2020) 5 Journal of Cyber Policy 94.
32. Nick Doty, ‘Reviewing for Privacy in Internet and Web Standard-Setting’, 2015 IEEE Security and Privacy Workshops (IEEE 2015).
33. Seda Gürses and Jose M Del Alamo, ‘Privacy Engineering: Shaping an Emerging Field of Research and Practice’ (2016) 14 IEEE Security & Privacy 40.
34. Giovanni Maria Riva, Alexandr Vasenev and Nicola Zannone, ‘SoK: Engineering Privacy-Aware High-Tech Systems’, Proceedings of the 15th International Conference on Availability, Reliability and Security (2020).
35. Dariusz Kloza and others, ‘Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements’ (2019) 1 d. pia. lab Policy Brief 1.
36. Ian Goldberg, David Wagner and Eric Brewer, ‘Privacy-Enhancing Technologies for the Internet’, Proceedings IEEE COMPCON 97. Digest of Papers (IEEE 1997).
37. Łukasz Olejnik and others, ‘The Leaking Battery: A Privacy Analysis of the HTML5 Battery Status API’, Data Privacy Management, and Security Assurance: 10th International Workshop, DPM 2015, and 4th International Workshop, QASA 2015, Vienna, Austria, September 21–22, 2015. Revised Selected Papers 10 (Springer 2016),.

38. Lukasz Olejnik, Steven Englehardt and Arvind Narayanan, ‘Battery Status Not Included: Assessing Privacy in Web Standards’, 2017 International Workshop on Privacy Engineering (2017).
39. Nick Doty, Deirdre K Mulligan and Erik Wilde, ‘Privacy Issues of the W3C Geolocation API’ [2010] arXiv preprint arXiv:1003.1775.
40. Dylan A Cooper and others, ‘Privacy Considerations for Online Advertising: A Stakeholder’s Perspective to Programmatic Advertising’ (2023) 40 Journal of Consumer Marketing 235.
41. Mark Nottingham, ‘Playing Fair in the Privacy Sandbox: Competition, Privacy and Interoperability Standards’ [2021] Privacy and Interoperability Standards (February 3, 2021).
42. Yong Yuan and others, ‘A Survey on Real Time Bidding Advertising’, Proceedings of 2014 IEEE International Conference on Service Operations and Logistics, and Informatics (IEEE 2014),.
43. Shuai Yuan, Jun Wang and Xiaoxue Zhao, ‘Real-Time Bidding for Online Advertising: Measurement and Analysis’, Proceedings of the seventh international workshop on data mining for online advertising (2013).
44. Claude Castelluccia, Lukasz Olejnik and Tran Minh-Dung, ‘Selling off Privacy at Auction’, Network and Distributed System Security Symposium (NDSS) (2014).
45. Michael Veale and Frederik Zuiderveen Borgesius, ‘Adtech and Real-Time Bidding under European Data Protection Law’ (2022) 23 German Law Journal 226.
46. Michael Veale, Midas Nouwens and Cristiana Santos, ‘Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?’ [2022].
47. Aleksandra Korolova, ‘Privacy Violations Using Microtargeted Ads: A Case Study’, 2010 IEEE International Conference on Data Mining Workshops (IEEE 2010).
48. Frederik J Zuiderveen Borgesius and others, ‘Online Political Microtargeting: Promises and Threats for Democracy’ (2018) 14 Utrecht Law Review 82.
49. Khaled El Emam and Fida Kamal Dankar, ‘Protecting Privacy Using K-Anonymity’ (2008) 15 Journal of the American Medical Informatics Association 627.

50. Riad Ladjel and others, ‘Trustworthy Distributed Computations on Personal Data Using Trusted Execution Environments’, 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (IEEE 2019).
51. Jatinder Singh and others, ‘Enclaves in the Clouds: Legal Considerations and Broader Implications’ (2021) 64 Communications of the ACM 42.
52. Emily M Weitzenboeck and others, ‘The GDPR and Unstructured Data: Is Anonymization Possible?’ (2022) 12 International Data Privacy Law 184.
53. Frederik J Zuiderveen Borgesius, ‘Singling out People without Knowing Their Names–Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation’ (2016) 32 Computer Law & Security Review 256.
54. Lukas Helminger and Christian Rechberger, ‘Multi-Party Computation in the GDPR’, Privacy Symposium 2022: Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT) (Springer 2022).
55. Lina Jasmontaite and others, ‘Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR’ (2018) 4 Eur. Data Prot. L. Rev. 168.
56. Lee A Bygrave, ‘Data Protection by Design and by Default: Deciphering the EU’s Legislative Requirements’ (2017) 4 Oslo Law Review 105.
57. Frederik J Zuiderveen Borgesius, ‘Personal Data Processing for Behavioural Targeting: Which Legal Basis?’ (2015) 5 International Data Privacy Law 163.
58. Dominique Machuletz and Rainer Böhme, ‘Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR’ [2019] Proceedings on Privacy Enhancing Technologies, 2, 481-498.
59. Maximilian Hils, Daniel W Woods and Rainer Böhme, ‘Measuring the Emergence of Consent Management on the Web’, Proceedings of the ACM Internet Measurement Conference (2020).
60. Maximilian Hils, Daniel W Woods and Rainer Böhme, ‘Privacy Preference Signals: Past, Present and Future’ (2021) 4 Proceedings on Privacy Enhancing Technologies 249.

61. Sebastian Zimmeck and others, ‘Usability and Enforceability of Global Privacy Control’ (2023) 2 Proceedings on Privacy Enhancing Technologies 1.
62. Cristiana Santos and others, ‘Cookie Banners, What’s the Purpose? Analyzing Cookie Banner Text Through a Legal Lens’, Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society (2021).
63. PAJ Graßl and others, ‘Dark and Bright Patterns in Cookie Consent Requests’ (2021) 3 Journal of Digital Social Research 1.
64. Hana Habib and others, “‘Okay, Whatever”: An Evaluation of Cookie Consent Interfaces’, Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (2022).
65. Christine Utz and others, ‘(Un) Informed Consent: Studying GDPR Consent Notices in the Field’, Proceedings of the 2019 acm sigsac conference on computer and communications security (2019).
66. Cristiana Santos, Nataliia Bielova and Célestin Matte, ‘Are Cookie Banners Indeed Compliant with the Law? Deciphering Eu Legal Requirements on Consent and Technical Means to Verify Compliance of Cookie Banners’ [2019] arXiv preprint arXiv:1912.07144.
67. Martino Trevisan and others, ‘4 Years of EU Cookie Law: Results and Lessons Learned’ (2019) 2019 Proceedings on Privacy Enhancing Technologies 126.
68. Damien Geradin and Dimitrios Katsifis, ‘Taking a Dive into Google’s Chrome Cookie Ban’.
69. Christophe Carugati, ‘The Antitrust Privacy Dilemma’ [2023] European Competition Journal 1.
70. Rupprecht Podszun and Stefan Kreifels, ‘Digital Platforms and Competition Law’ (2016) 5 Journal of European Consumer and Market Law 33.
71. Selcukhan Unekbas, ‘Competition, Privacy, and Justifications: Invoking Privacy to Justify Abusive Conduct under Article 102 TFEU’ [2022] Journal of Law, Market & Innovation.
72. Ramon Casadesus-Masanell and Andres Hervas-Drane, ‘Competing with Privacy’ (2015) 61 Management Science 229.
73. de Moncuit, A. In which ways should privacy concerns serve as an element of the competition assessment, <_____

_____> accessed 14 June 2023.

74. Klaus M Miller and Bernd Skiera, ‘Economic Consequences of Online Tracking Restrictions’ [2023] arXiv preprint arXiv:2303.09147.
75. Lesley Chiou and Catherine Tucker, ‘SEARCH ENGINES AND DATA RETENTION: IMPLICATIONS FOR PRIVACY AND ANTITRUST’.
76. Viktoria HSE Robertson, ‘The Complementary Nature of the Digital Markets Act and Articles 101 and 102 TFEU’ [2023] DMA working group (European Parliament’s IMCO).
77. Alison Jones, ‘Brexit: Implications for UK Competition Law’ [2017] King’s College London Law School Research Paper.
78. Andrea Maria Garofalo, ‘Cookies and the Passive Role of the Data Subject’ [2022] Privacy and Data Protection in Software Services 73.
79. Fassl, M., Gröber, L. T., & Krombholz, K. (2021, May). Stop the consent theater. In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (pp. 1-7).

Websites

1. ‘Firefox Android’s New Privacy Feature, Total Cookie Protection, Stops Companies from Keeping Tabs on Your Moves | The Mozilla Blog’ <https://blog.mozilla.org/en/mozilla/firefox-androids-new-privacy-feature-total-cookie-protection-stops-companies-from-keeping-tabs-on-your-moves/> accessed 9 June 2023.
2. ‘Full Third-Party Cookie Blocking and More’ (WebKit, 24 March 2020) <https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/> accessed 9 June 2023.
3. ‘Expanding Testing for the Privacy Sandbox for the Web’ (Google, 27 July 2022) <https://blog.google/products/chrome/update-testing-privacy-sandbox-web/> accessed 7 June 2023.
4. ‘The Privacy Sandbox’ <https://www.chromium.org/Home/chromium-privacy/privacy-sandbox/> accessed 9 June 2023.

5. ‘Building a More Private Web: A Path towards Making Third Party Cookies Obsolete’ (Chromium Blog) <https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html> accessed 18 May 2023.
6. ‘EDPB | European Data Protection Board’ <https://edpb.europa.eu/edpb_en> accessed 15 May 2023.
7. ‘World Wide Web Consortium (W3C)’ <https://www.w3.org/> accessed 15 May 2023.
8. ‘About W3C Community and Business Groups | Community and Business Groups’ <https://www.w3.org/community/about/> accessed 15 May 2023.
9. ‘Web Incubator Community Group (WICG)’ <https://wicg.io/> accessed 15 May 2023.
10. ‘W3C Technical Architecture Group’ <https://www.w3.org/2001/tag/> accessed 15 May 2023.
11. ‘Privacy Sandbox on Android’ (Android Developers) <https://developer.android.com/design-for-safety/privacy-sandbox> accessed 18 May 2023.
12. Bennett Cyphers and Adam Schwartz, ‘Ban Online Behavioral Advertising’ (Electronic Frontier Foundation, 21 March 2022) <https://www.eff.org/deeplinks/2022/03/ban-online-behavioral-advertising> accessed 23 May 2023.
13. ‘n. Computing a set of routines, protocols, and tools designed to allow the development of applications that can utilize or operate in conjunction with a given item of software, set of data, website, etc.; abbreviated API’ <https://www.oed.com/view/Entry/9705#eid376049> accessed 23 May 2023.
14. ‘Google Selects Fastly Oblivious HTTP Relay for Privacy Sandbox Initiative to Enhance Online Privacy for Billions of Chrome Users’ <https://www.fastly.com/press/press-releases/google-selects-Fastly-Oblivious-HTTP-Relay-for-Privacy-Sandbox> accessed 27 May 2023.
15. Luca Bertuzzi. ’Cookie Fatigue: The Questions Facing the EU Commission Initiative – EURACTIV.Com’ <https://www.euractiv.com/section/data-privacy/news/cookie-fatigue-the-questions-facing-the-eu-commission-initiative/> accessed 7 June 2023.

16. Access Now. ’Review of the e-Privacy Directive <https://www.accessnow.org/wp-content/uploads/2016/12/Access-Now-ePrivacy-Directive-policy-paper.pdf> accessed 9 June 2023.
17. ‘POSITION ON THE REVIEW OF THE ePRIVACY DIRECTIVE’ (Internet Advertising Bureau) <https://iabeurope.eu/wp-content/uploads/2020/06/20161201_IAB-Europe-Position-on-ePrivacy-Directive-Review.pdf> accessed 9 June 2023.
18. ‘Introducing a new era of AI-powered ads with Google’ (2023) <https://blog.google/products/ads-commerce/ai-powered-ads-google-marketing-live/> accessed 9 June 2023.
19. ‘Digital fairness – fitness check on EU consumer law’ (2022) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en> accessed 9 June 2023.

Standards or technical references

1. Steven Bingler, Mike West and John Wilander, ‘Cookies: HTTP State Management Mechanism’ (Internet Engineering Task Force 2023) Internet Draft <https://datatracker.ietf.org/doc/draft-ietf-httpbis-rfc6265bis> [2023] accessed 27 May 2023.
2. ‘Protected Audience (Formerly FLEDGE)’ [2023] <https://wicg.github.io/turtledove/> accessed 9 June 2023.
3. ‘W3C Process Document’ <https://www.w3.org/2021/Process-20211102/> accessed 15 May 2023.
4. Alissa Cooper and others, RFC 6973: Privacy Considerations for Internet Protocols (RFC Editor 2013).
5. ‘Self-Review Questionnaire: Security and Privacy’ <https://www.w3.org/TR/security-privacy-questionnaire/> accessed 18 May 2023.
6. ‘Protected Audience (Formerly FLEDGE)’ [2023] <https://wicg.github.io/turtledove/> accessed 9 June 2023.
7. ‘Turtledove/Original-TURTLEDOVE.Md at Main · WICG/Turtledove · GitHub’ <https://github.com/WICG/turtledove/blob/main/Original-TURTLEDOVE.md> accessed 23 May 2023.

8. ‘FLEDGE’ <https://github.com/WICG/turtledove> accessed 23 May 2023.
9. The analysis is based on the shape of standards or explainers as of June 2023 (mature proposals of a system put to tests, but still subject to some modifications, but the parts identified in Points of Interests appear to be stable at this point).
10. ‘Fenced Frame’ <https://wicg.github.io/fenced-frame/> accessed 27 May 2023.
11. ‘Outcome-based TURTLEDOVE’ <https://github.com/WICG/turtledove> accessed 23 May 2023.
12. ‘Private Aggregation API’ <https://patcg-individual-drafts.github.io/private-aggregation-api/> accessed 23 May 2023
13. ‘‘GoogleChrome/Ip-Protection’ <https://github.com/GoogleChrome/ip-protection/> accessed 27 May 2023.
14. ‘Utilizing the 1-Bit Leak to Build a Cross Site Tracker · Issue #211 · WICG/Turtledove’ (GitHub) <https://github.com/WICG/turtledove/issues/211#issuecomment-889269834> accessed 27 May 2023.
15. ‘Protected Audience Documentation’ <https://github.com/privacysandbox/fledge-docs> accessed 27 May 2023.
16. Martin Thomson and Christopher A Wood, ‘Oblivious HTTP’ (Internet Engineering Task Force 2023) Internet Draft draft-ietf-ohai-ohttp-08 <https://datatracker.ietf.org/doc/draft-ietf-ohai-ohttp> accessed 27 May 2023, section 2.
17. ‘Protected Audience API’ (Chrome Developers, 27 January 2022) <https://developer.chrome.com/docs/privacy-sandbox/fledge/> accessed 23 May 2023.
18. ‘Protected Audience: Integration Guide’ (Android Developers) <https://developer.android.com/design-for-safety/privacy-sandbox/integration/protected-audience> accessed 1 June 2023.
19. ‘Tracking Preference Expression (DNT)’ <https://www.w3.org/TR/tracking-dnt/> accessed 2 June 2023.
20. ‘Global Privacy Control (GPC)’ <https://privacycg.github.io/gpc-spec/> accessed 2 June 2023.
21. ‘Buyer Guide: Join Interest Groups and Generate Bids’ (Chrome Developers, 1 November 2022) <https://developer.chrome.com/docs/privacy-sandbox/fledge-api/interest-groups/> accessed 7 June 2023.

22. ‘The Storage Access API’ <https://privacycg.github.io/storage-access/> accessed 9 June 2023.