Technology and Regulation

Cookies and EU Law: History, Future Regulation and Critique

Jan Tomíšek

cookies, ePrivacy directive, ePrivacy regulation, consent, tracking, fingerprinting

jantomisek@gmail.com

Cookies and similar technologies can be used to track the online behaviour of internet users and can pose risks to their privacy and other fundamental rights. The use of cookies and similar technologies is therefore regulated by EU law. The article describes the history of EU law regulating cookies, analyses its current form and application to different technologies, and describes the proposals for the ePrivacy Regulation. Based on the analysis, it provides a critique of both the current law and the proposals and suggests ways forward in the regulation of cookies and similar technologies.

1. Introduction

Cookies and other similar technologies can be used to track the online behaviour of internet users for the purpose of targeted advertising.[1] Targeted advertising poses a threat to users' fundamental rights and freedoms through chilling effects,[2] potential for manipulation[3] and discrimination.[4] Because of their potential for privacy-invasive tracking, the use of cookies and similar technologies is regulated under EU law.[5]

The purpose of this article is to describe the history of EU law regulating cookies and similar technologies, to analyse its current form and application to different technologies, to describe its future as presented by the proposals for the ePrivacy Regulation[6], to provide a critique of both the current law and the proposals, and to suggest ways forward in the regulation of cookies and similar technologies.

The article is therefore structured as follows: Part Two introduces cookies and similar technologies, including technologies proposed to replace third-party cookies after they are blocked in major web browsers. Part Three analyses the application of Article 5(3) of the current ePrivacy Directive[7] to cookies and similar technologies, including the proposed ones. Part Four describes the proposals for the ePrivacy Regulation to replace the ePrivacy Directive and analyses its application to these technologies. Part Five critiques the largely consent-based approach of the ePrivacy Directive and the proposed ePrivacy Regulation and suggests possible changes to the approach. Part Six concludes.

2. Cookies and other tracking technologies

Cookies are short strings of text that a website can store in a user's web browser, and retrieve later when the user revisits the website.[8]

1 Adam Barth, ‹HTTP State Management Mechanism - Request for Comments› (*Internet Engineering Task Force*, April 2011), 28 https://datatracker.ietf.org/doc/html/rfc6265 accessed 21 August 2023.

2 Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (OUP 2015) 101.

3 Matthew Crain and Anthony Nadler, ‹Political Manipulation and Internet Advertising Infrastructure› (2019) 9 Journal of Information Policy https://scholarlypublishingcollective.org/psup/information-policy/article/doi/10.5325/jinfopoli.9.2019.0370/314495/Political-Manipulation-and-Internet-Advertising accessed 21 August 2023, 370ff; Ryan Calo, ‹Digital Market Manipulation› (2013) 9 George Washington Law Review https://digitalcommons.law.uw.edu/faculty-articles/25/ accessed 21 August 2023, 995, 996, 1001.

4 Julia Angwin and Terry Parris, ‹Facebook Lets Advertisers Exclude Users by Race› (*propublica.org*, 28 October 2016) https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race accessed 21 August 2023; Till Speicher and others, 'Potential for Discrimination in Online Targeted Advertising' (2018) Proceedings of the 1st Conference on Fairness, Accountability and Transparency http://proceedings.mlr.press/v81/speicher18a/speicher18a.pdf accessed 21 August 2023, 9, 10.

5 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, Art. 5(3).

6 Commission, 'Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM (2017) 10 final 2017/0003(COD) (hereafter the "Commission proposal").

7 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).

8 Barth (n 1) 5. Specifically, a web server may include a Set-Cookie field in the response header of a request to send the content of a particular web page, which may include key-value pairs such as «Set-Cookie:

The author is a PhD student at the Institute of Law and Technology, Faculty of Law, Masaryk University and a partner in the Czech law firm ROWAN LEGAL.

Received 26 Aug 2023, Accepted 9 Sep 2023, Published 15 Sep 2023

Cookies were designed to give web servers a way to maintain information (a state) between two views of a web page from the same server (domain).[9] However, the ability to store information (including identifiers) in a user's web browser is also used to analyse user behaviour.[10]

Cookies can only be read by a website on the same internet domain as the website that stored the cookie.[11] However, today's websites are made up of elements loaded from different domains. This allows cookies from different domains to be stored in the user's browser while the user is viewing a website from one domain. Cookies stored from the domain of the website the user is currently viewing are called *first-party cookies*.[12] Cookies from other domains are called *third-party cookies*.[13]

First-party cookies can be used to collect data about user behaviour on a website, but they cannot be used to share that data between websites because they do not provide a way to establish a shared identifier for the user (workarounds such as convincing the user to sign in to a shared account have to be used). Third-party cookies, however, do allow for the establishment of a shared identifier and subsequent sharing of data through a process called *cookie synchronisation*.[14] In this process, a request for a script or image within the website the user is viewing is redirected between other domains, identifiers are shared as parameters of requests and redirections and are read from or stored as cookies.[15]

An entire ecosystem of ad exchanges, demand-side platforms, data exchanges and other internet advertising intermediaries is built around this data sharing based on third-party cookies.[16] This data sharing is also a major source of the threats to fundamental rights mentioned above.[17] Without the sharing of identifiers, users would no longer be "followed" by the products they have recently viewed online,[18] which could reduce the chilling effect of online tracking. Also, without the ability to target an individual user or audience (enabled by the sharing), manipulation and discrimination would be more difficult.

As a result, some web browsers already block third-party cookies by default,[19] and the other major browsers (notably Google Chrome, which has the largest market share) plan to do so shortly.[20] Some website authors try to circumvent these measures by presenting third-party cookies as first-party, using a technique called CNAME cloaking.[21] However, there are also techniques to detect CNAME cloaking at the web browser level.[22]

Similar to cookies, other technologies may be used to track user behaviour. Some of these involve storing data in the user's web browser. Others work with data that can be retrieved from the user's device about its hardware or software.[23] So-called *ETags* work based on the web browser's cache.[24] A feature of web browsers called web storage allows the storage of key-value pairs, but the storage capacity is much larger than that of cookies (5 MB per web page versus 4 kB per cookie).[25] Web storage is tied to the domain of the website the user is viewing, so it cannot be used by third-party domains.[26] In the past, cookies associated with a web browser plug-in called Flash were also used (namely to recover classic cookies that the user had deleted from his browser).[27]

Data about the software or hardware of the user's device is used through a technique known as *device fingerprinting* or *browser fingerprinting*.[28] Websites have access to extensive information about

PHPSESSID=r2t5uvjq435r4q7ib3vtdjq120; language=en». Based on this instruction, the browser will store a «PHPSESSID» cookie with the value «r2t5uvjq435r4q7ib3vtdjq120» and a «language» cookie with the value «en». In such case, the header of the request to display another page from the same domain will also include the «Cookie: PHPSESSID=r2t5uvjq435r4q7ib3vtdjq120; language=en» field.

9 Barth (n 1) 1.

10 Barth (n 1) 28; Peng Liu and Wang Chao, *Computational Advertising: Market and Technologies for Internet Commercial Monetization* (CRC Press 2020) 120; Guangzhi Zheng and Svetlana Peltsverger, 'Web Analytics Overview', in Encyclopedia of Information Science and Technology (IGI Global 2015) https://www.igi-global.com/chapter/web-analytics-overview/112470 accessed 21 August 2023, 3.

11 Barth (n 1) 26.

12 Article 29 Data Protection Working Party, 'Opinion 4/2012 on Cookie Consent Exemption', (WP 194, 7 June 2012) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf accessed 21 August 2023 (hereafter "WP194"), 5.

13 WP194 (n 12) 5.

14 'Cookie Matching | Real-time Bidding' (*Authorized Buyers*) https://developers.google.com/authorized-buyers/rtb/cookie-guide accessed 21 August 2023; Arpita Ghosh and others, 'To Match or Not to Match: Economics of Cookie Matching in Online Advertising' (2015) 2 ACM Transactions on Economics and Computation https://dl.acm.org/doi/10.1145/2745801 accessed 21 August 2023, 12; Papadopoulos and others, 'Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask.' in Ling Liu and Ryen White. *WWW'19: The World Wide Web Conference* (Association for Computing Machinery 2019) https://arxiv.org/abs/1805.10505 accessed 21 August 2023, 1432.

15 Papadopoulos (n 14).

16 Information Commissioner's Office, 'Update Report into Adtech and Real Time Bidding' (20 June 2019) https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf accessed 21 August 2023, 10 and 11; Liu and Chao (n 9) 334.

17 Michael Veale and Frederik Zuiderveen Borgesius, 'Adtech and real-time bidding under European data protection law' (2022) 2 German Law Journal https://www.cambridge.org/core/journals/german-law-journal/article/adtech-and-realtime-bidding-under-european-data-protection-law/017F027B4E78EBCAE1DCBC1E12B93B9D accessed 21 August 2023, 239

18 Displaying targeted ads related to a product or service (or generally a website) the user has previously viewed is called retargeting. Anja Lambrecht and Catherine Tucker, 'When does retargeting work? Information specificity in online advertising' (2013) 5 Journal of Marketing Research https://journals.sagepub.com/doi/10.1509/jmr.11.0503 accessed 21 August 2023, 562.

19 IAB Europe, 'A Guide to a Post Third Party Cookies Era' (2022) https://iabeurope.eu/wp-content/uploads/2022/03/IAB-Europe-Guide-to-a-Post-Third-Party-Cookie-Era-March-2022.pptx.pdf accessed 21 August 2023, 17.

20 Privacy Sandbox for the Web (*The Privacy Sandbox*) (https://privacysandbox.com/open-web/ accessed 21 August 2023.

21 Tongwei Ren and others, 'An Analysis of First-Party Cookie Exfiltration due to CNAME Redirections' in *Workshop on Measurements, Attacks, and Defenses for the Web* (Internet Society 2021) https://ldklab.github.io/assets/papers/madweb21-cloaking.pdf accessed 21 August 2023, 3.

22 Ha Dao, Johan Mazel and Kensuke Fukuda, 'CNAME cloaking-based tracking on the web: Characterization, detection, and protection' (2021) 3 IEEE Transactions on Network and Service Management https://ieeexplore.ieee.org/abstract/document/9403411/ accessed 21 August 2023, 3882; IAB Europe (Fn. 19), p. 19.

23 Chris Jay Hoofnagle and others, 'Behavioral advertising: The offer you can›t refuse', (2012) 6 Harvard Law & Policy Review 273, 286.

24 Nicolas Hinternesch, 'No Cookies, No Problem – Using ETags For User Tracking' (*Medium*, 17 May 2021) https://levelup.gitconnected.com/no-cookies-no-problem-using-etags-for-user-tracking-3e745544176b accessed 21 August 2023.

25 Hoofnagle (n 23) 283; 'HTML Web Storage API' (*W3 Schools*) https://www.w3schools.com/html/html5_webstorage.asp accessed 21 August 2023.

26 Hoofnagle (n 23) 283.

27 Hoofnagle (n 23) 283.

28 Yinzhi Cao, Song Li and Erik Wijmans, '(Cross-)Browser Fingerprinting via OS and Hardware Level Features' in *Network and Distributed System Security Symposium: Proceedings 2017* (Internet Society 2017) https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-

the user's web browser and device, such as browser type and version, operating system type and version, or screen resolution. This information is to some extent specific to the user's device and can thus form a traceable "fingerprint" of the user.[29] This fingerprint may not be unique with certainty, but the probability of uniqueness may be high.

Web browsers also have dynamic features that can be controlled by scripts embedded in web pages, and the behaviour of these features can vary from device to device, browser to browser, and version to version of the same browser.[30] The use of data that a device actively sends about itself can be referred to as *passive fingerprinting*, and the use of data that must be actively captured by a script can be referred to as *active fingerprinting*.[31] Since fingerprinting is not bound to a specific feature of a web browser that would be limited to the first-party context, it can be used also by third-party domains.

As mentioned above, third-party cookies will soon be blocked by default in all major web browsers, yet they are currently critical to the functioning of the internet advertising ecosystem. Therefore, other technologies have been proposed to replace third-party cookies and enable targeted advertising in a less privacy-intrusive way.[32]

Google, the creator of the most widely used web browser, Google Chrome, proposed two key technologies[33] – *Topics API* for interest-based targeting[34] and *Protected Audience API* (originally named FLEDGE) for targeting users who have visited a specific website.[35] The Topics API is based on a set of tags that web browsers would assign to websites based on their domain name.[36] Based on the user's browsing behaviour, the browser would remember the most visited topics over the past 4 weeks and make them available to websites in a limited way.[37] It can also be used in a third-party context.[38]

Protected Audience API allows websites with ad space to launch an auction in the user's browser for that ad space.[39] The list of potential bidders provided by the website launching the auction is compared with a list of websites that have marked the user's browser as a target for their advertising and have provided logic to learn their bid for the auction.[40] For sites on both lists, the bid is calculated in the browser and the auction winner's ad is retrieved and displayed.[41]

The purpose of the Topics API and Protected Audience API is to enable targeted advertising while reducing the impact on user privacy.[42] However, the Topics API has been criticised by other browser developers and a relevant industry group for not doing enough to reduce the privacy impact.[43] Protected Audience API, in my opinion, has a design flaw.[44] Despite the criticism Google rolled out Topics API to Google Chrome browser in September 2023.[45]

It shows that cookies, as well as other technologies, can be used to track user behaviour online. Currently, third-party cookies are the backbone of the most privacy-intrusive practices, such as cookie synchronisation, which allows data about user behaviour to be shared between websites. Although third-party cookies will soon be blocked in all major web browsers, there will probably still be some browsers that do not have such a strict policy, there will still be techniques to get around this blocking (such as using CNAME cloaking, ETags or fingerprinting), and there will still be technologies that replace third-party cookies. It is therefore still important to regulate cookies and similar technologies.

3. History of cookie regulation in the EU

In the EU, the legislation on access to terminal equipment is part of the legislation on privacy and electronic communications. The current ePrivacy Directive was proposed by the European Commission (hereafter the "Commission") in 2000.[46] Article 5(3) of the ePrivacy Directive regulates the retention of information and access to information already stored in the terminal equipment of a subscriber or user of electronic communications services, including the use of cookies and similar technologies. However, this provision was not included in the

fingerprinting-os-and-hardware-level-features/ accessed 21 August 2023, 1; Hoofnagle (n 23) 285; Article 29 Data Protection Working Party, 'Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting' (WP 224, 25 November 2014) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf accessed 21 August 2023 (hereafter "WP224") 3.

29 For an overview of the relevant data, see WP224 (n 28) 5.

30 WP224 (n 28) 5.

31 Jonathan R. Mayer and John C. Mitchell, 'Third-party web tracking: policy and technology' in *2012 IEEE symposium on security and privacy* (IEEE 2012) https://ieeexplore.ieee.org/document/6234427 accessed 21 August 2023, 421; Cao, Li and Wijmans (n 28), 2; James Konik, 'How Does Canvas Fingerprinting Work?' (*Fingerprint*, 11 July 2021) https://fingerprint.com/blog/canvas-fingerprinting/ accessed 21 August 2023.

32 IAB Europe (n 19) 17 and 65; Commission, 'Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers' (30 January 2023) https://op.europa.eu/en/publication-detail/-/publication/8b950a43-a141-11ed-b508-01aa75ed71a1/language-en accessed 21 August 2023, 176.

33 Privacy Sandbox for the Web (n 20).

34 Sam Dutton, 'The Topics API' (*Chrome Deveopers*, 25 January 2022) https://developer.chrome.com/docs/privacy-sandbox/topics/ accessed 21 August 2023.

35 Sam Dutton and Kevin K. Lee, 'Protected Audience API' (*Chrome Deveopers*, 23 August 2022) https://developer.chrome.com/docs/privacy-sandbox/protected-audience/ accessed 21 August 2023.

36 The relevant part oft he URL adress is called host name. Dutton (n 34).

37 Dutton (n 34)

38 Dutton (n 34)

39 Dutton and Lee (n 35).

40 Dutton and Lee (n 35).

41 Dutton and Lee (n 35).

42 Privacy Sandbox for the Web (n 20).

43 Martin Thomson, 'A Privacy Analysis of Google's Topics Proposal' (6 January 2023) (https://mozilla.github.io/ppa-docs/topics.pdf accessed 21 August 2023; 'Request for Position: Topics API #622' (*GitHub*, 17 March 2022) https://github.com/mozilla/standards-positions/issues/622 accessed 21 August 2023, comment of the user martinthomson form 6 January 2023; 'The Topics API #111' (*GitHub*, 20 December 2022) https://github.com/WebKit/standards-positions/issues/111) accessed 21 August 2023, comment of the user annevk from 20. December 2022; 'Early design review for the Topics API #726' (*GitHub*, 25 March 2023) https://github.com/w3ctag/design-reviews/issues/726#issuecomment-1379908459 accessed 21 August 2023, comment of the user rhiaro from 12 January 2023.

44 It seems that URL adresses used to call the bidding logic and specific services might contain unique identifiers, thus allowing to target individual users. See description of joinAdInterestGroup() function of the Protected Audience API. Sam Dutton and Alexandra White 'Buyer guide: join interest groups and generate bids' (*Chrome Deveopers*, 1 November 2022) https://developer.chrome.com/docs/privacy-sandbox/fledge-api/interest-groups/ accessed 21 August 2023.

45 Anthony Chavez, 'Privacy Sandbox for the Web reaches general availability' (*The Privacy Sandbox*, 7 September 2023) https://privacysandbox.com/news/privacy-sandbox-for-the-web-reaches-general-availability accessed 10 September 2023.

46 Vagelis Papakonstantinou and Paul De Hert, 'The Amended EU Law on ePrivacy and Electronic Communications after Its 2011 Implementation: New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights' (2011) 1 John Marshall Journal of Computer & Information Law, 29, 38.

Commission's draft directive[47] it only appeared for the first time in the proposal resulting from the European Parliament's (hereafter the "Parliament") first reading[48]. The Parliament proposed a regulation requiring *"prior, explicit consent"* for the storage of information and access to information already stored in the terminal equipment of a subscriber or user of electronic communications services.[49]

This proposal met with a strong negative reaction from organisations representing the advertising industry and business in general.[50] Apparently, in response to this opposition, the Council of the EU (hereafter the "Council") replaced the requirement of consent in its common position with a requirement to provide information and the right to refuse.[51] This counter-proposal was eventually reflected in the adopted text of Article 5(3).

Further developments in the law were probably influenced by the Sony/BMG music publishing case.[52] Some of this label's music CDs automatically installed software on the user's PC that limited the number of copies of the music CDs that could be made. However, the software was installed surreptitiously and, due to its inappropriate design, increased the computer's vulnerability to malware.[53] Sony/BMG's conduct fell outside the scope of the original wording of Article 5(3) of the ePrivacy Directive – it did not involve access to a terminal in connection with the use of an electronic communications service.

In 2007, the Commission presented a proposal for a directive amending the ePrivacy Directive.[54] This proposal included an amendment to Article 5(3) so that the scope of the provision was not linked to electronic communications services (to cover cases such as Sony/BMG).[55] It was only during the negotiations in the European Parliament that a provision requiring consent to store information and access information already stored on the terminal equipment was added to the draft amendment.[56] In the Parliament's first reading, this proposal was accompanied by the wording *"taking into account that the browser settings constitute prior consent"*.[57] Following a rejection by the Commission[58], a consent regime was again proposed in the second reading in the Parliament, but without this addendum.[59]

Both the Commission and the Council subsequently accepted the Parliament's proposal for a consent regime without specific justification[60] and the amendment was issued in Directive 2009/136/EC. The amended Article 5(3) reads as follows:

> *Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent*

47 Commission, 'Proposal for a Directive of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the electronic communications sector' COM/2000/0385 final - COD 2000/0189 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52000PC0385 accessed 21 August 2023.

48 Parliament, 'Second report on the proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector ((COM(2000) 385 – C5-0439/2000 – 2000/0189(COD))' A5-0374/2001, Amendment 26 (https://www.europarl.europa.eu/doceo/document/A-5-2001-0374_EN.pdf?redirect accessed 21 August 2023

49 Parliament (n 48).

50 Eleni Kosta, 'Peeking into the cookie jar: the European approach towards the regulation of cookies' (2013) 4 International Journal of Law and Information Technology https://academic.oup.com/ijlit/article-abstract/21/4/380/730901 accessed 10 September 2023, 387; Sylvia Mercado Kierkegaard, 'How the cookies (almost) crumbled: Privacy & lobbyism' (2005) 4 Computer Law & Security Review https://www.sciencedirect.com/science/article/abs/pii/S0267364905001184 accessed 21 August 2023, 321.

51 Council, 'Common position (EC) No 26/2002 adopted by the Council on 28 January 2002' https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2002:113E:0039:0053:EN:PDF accessed 21 August 2023.

52 Kosta (n 50) 384.

53 SunnComm MediaMax Security Vulnerability FAQ (*Electronic Frontier Foundation*, 19 July 2007) https://www.eff.org/pages/sunncomm-mediamax-security-vulnerability-faq accessed 21 August 2023. It was subsequently discovered that other Sony/BMG CDs contained a similar tool, MediaMax-3, which suffered from very similar flaws. Kosta (n 50) 384.

54 Commission, 'Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users› rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation {SEC(2007) 1472} {SEC(2007) 1473}' /* COM/2007/0698 final - COD 2007/0248 */ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52007PC0698 accessed 21 August 2023.

55 Commission (n 54).

56 Parliament, 'European Parliament legislative resolution of 24 September 2008 on the proposal for a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users› rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation (COM(2007)0698 - C6-0420/2007 - 2007/0248(COD))' https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52008AP0452 accessed 21 August 2023.

57 Parliament (n 56).

58 Commission, 'The amended proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users› rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation of 6.11.2008, COM/2008/0723 final - COD 2007/0248' https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2008%3A0723%3AFIN accessed 21 August 2023.

59 Parliament, 'European Parliament legislative resolution of 6 May 2009 on the Council common position for adopting a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users› rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (16497/1/2008 - C6-0068/2009 - 2007/0248(COD))' https://www.europarl.europa.eu/doceo/document/TA-6-2009-0360_EN.html accessed 21 August 2023.

60 Commission, 'Opinion pursuant to Article 251(2), third subparagraph, point (c) of the EC Treaty, on the European Parliament›s amendments to the Council›s common position regarding the proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users› rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No .... 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, amending the Commission proposal pursuant to Article 250(2) of the EC Treaty of 29.7.2009, COM/2009/0421 final - COD 2007/0248' https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009PC0421 accessed 21 August 2023; Kosta (n 50) 390.

> *any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.*

It is also worth noting that, before the final approval of the Directive by the European Parliament and the Council, 13 Member States issued an opinion that Article 5(3) is not intended as a change to the existing requirement where consent can be exercised as a right to refuse cookies or similar technologies used for legitimate purposes.[61] In this opinion, they rely on Recital 66 of Directive 2009/136/EC, which refers to storing information and gaining access to information already stored on a terminal device, but surprisingly does not refer to consent but to the right to refuse such activities.[62]

The EU law on cookies was therefore first proposed in 2000 and adopted in 2002, but it is only since 2009 that the consent requirement has been included. Also, the requirement was first proposed with the idea that it could be expressed through default web browser settings, and this was the position taken by many EU member states when the consent requirement was enacted in 2009. It is also notable that the stricter law was probably not prompted by the advent of the internet and online tracking but by a case of surreptitious software installation.

4. Current EU cookie law

Concerning cookies and similar technologies that allow for the storage of data on the user's device, such as ETags and web storage, Article 5(3) implies a requirement to obtain consent for the storage of cookies on the end device and their subsequent reading, except in cases where these cookies or similar technologies are necessary for the functioning of a website, such as a shopping cart in an online shop.[63] This requirement also applies to Protected Audience API, as it requires the information about the user being relevant for targeting by a website to be stored in the user's browser (along with information about the website's bidding logic).

The application of Article 5(3) to fingerprinting is less clear. According to the opinion of the Article 29 Data Protection Working Party (hereafter "WP29")[64], Article 5(3) of the ePrivacy Directive applies to these techniques *"[i]f the fingerprint is created by storing or accessing information stored on the end user's device."*[65] Unfortunately, the Opinion does not clarify what data the WP29 considers to be obtained by accessing information stored on the user's terminal and what data considers do not correspond.

This issue should be considered in light of Recital 24 of the ePrivacy Directive, which states that the terminal equipment is part of the user's private sphere. In my view, it would be an exaggeration to imply that the data that a device actively transmits about itself in the HTTP header of a request to access a web page is also part of that private sphere.[66] Conversely, this private sphere includes data that must be requested by a script running on the user's device.

While this data is not strictly stored on the device in the same structured way as, for example, cookies or data in web storage, it is stored as an attribute on the device and can therefore be queried by running scripts. At the same time, as WP29 points out, the notion of access to data stored on the terminal does not only refer to data stored on the terminal by a particular website but also to previously stored data.[67] I am therefore of the opinion that Article 5(3) does not apply to passive fingerprinting, but it does apply to active fingerprinting. As the use of the Topics API requires a website to actively query the web browser's API, it falls within the scope of Article 5(3) of the ePrivacy Directive.

The consent requirement itself must then be interpreted in accordance with the consent requirements set out in General Data Protection Regulation (GDPR)[68] – the ePrivacy Directive provides in its Article 2(f) that *"'consent' by a user or subscriber corresponds to the data subject›s consent in Directive 95/46/EC*", which has been repealed and replaced by the GDPR. The GDPR then provides in its Article 94(2)

61 Council, 'Appendix to footnote ‹I/A› Adoption of the proposal for a Directive (EC) No 1308/2006 of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and services and 2002/20/EC on the authorisation of electronic communications networks and services (LA+S) (third reading) of 18.11.2006. 2009, 2007/0247 (COD), 15864/09 ADD 1 REV 1, as amended by Corrigendum to footnote ‹I/A› Adoption of the proposal for a Directive (EC) No. 1308/2006 of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and services and 2002/20/EC on the authorisation of electronic communications networks and services (LA+S) (third reading) of 19.11.2009, 2007/0247' (COD), 15864/09 ADD 1 https://data.consilium.europa.eu/doc/document/ST-15864-2009-ADD-1/en/pdf accessed 21 August 2023.

62 Council (n 61).

63 On which cookies can be considered necessary and which not, see WP194 (n 12) 6.

64 The WP29 was the body that brought together the various supervisory authorities of the Member States under the legislation preceding EU General Data Protection Regulation (GDPR): 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), OJ 2016 L 119/1 – EU Directive 95/46: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

65 WP224 (n 28) 7. This conclusion is also confirmed by the Statement of the European Data Protection Board 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. 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' (5 May 2018) https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_en.pdf accessed 21 August 2023.

66 This is information about the user›s web browser and operating system, including their versions, contained in the *User-Agent* field. Internet Engineering Task Force, 'Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content' (2014) https://datatracker.ietf.org/doc/html/rfc7231#section-5, Article 5.1. accessed 21 August 2023. For example, this field may take the form *"Mozilla/5.0 (iPhone; CPU iPhone OS 12_0 like Mac OS X) AppleWebKit/605.1" for Apple iPhone devices and the Safari web browser.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1"* or for a computer running Microsoft Windows 10 and the Chrome web browser *"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.3"*.

67 See WP224 (n 28) 8.

68 EU General Data Protection Regulation (GDPR): 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), OJ 2016 L 119/1.

that references to Directive 95/46/EC shall be deemed to be references to the GDPR.[69] This means that consent must be, in accordance with Article 4(11) of the GDPR, a *"freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*.

The details of obtaining consent for the use of cookies are addressed in the opinions of several EU member state supervisory authorities.[70] Freedom of consent in the context of cookies means first and foremost that consent cannot be enforced by preventing access to a website or mobile application if consent is not given (through so-called *cookie* or *tracking walls*).[71] Specificity is reflected in the requirement to specify the purposes for which cookies are used, and the user must be able to decide whether or not to give consent for each purpose.[72] Informed consent means, in particular, the obligation to provide information about the identity of the data subject, the scope and purposes of the processing, and the right to withdraw consent at any time.[73] Concerning cookies, information about cookie expiration and third parties that may store cookies on the user's device or read them based on consent is important.[74] The requirement for unambiguous consent precludes consent being given by, for example, simply continuing to browse the website.[75] Deceptive practices should also be avoided when obtaining consent.[76]

Current EU cookie law, therefore, requires consent (beyond technical necessity) for the use of cookies (both third-party and first-party), similar technologies such as ETrackers and web storage, and the proposed Protected Audience API technology. The requirement also extends to active fingerprinting, which includes the use of the proposed Topics API.

Despite the position of some member states in 2009 mentioned above in Part 3, the standard for the consent is high and the consent cannot be expressed by default settings of a web browser. An informed and active indication of the user's wishes, such as a specific click, is required.

5. What the future holds: the ePrivacy Regulation

The Commission presented its proposal for an ePrivacy Regulation in January 2017.[77] In October 2017, Parliament's competent committee adopted a number of amendments to it, which became Parliament's official position for negotiations with the Commission and the Council.[78] In parallel, discussions took place in the Council,[79] resulting in a common Council position for negotiations with the Parliament in February 2021.[80]

The Commission proposal addresses the protection of information stored on and related to user devices in relation to cookies in Article 8(1). Article 10 of the Commission proposal then sets out requirements for web browser settings relating to cookies and similar technologies.

This wording, in contrast to Article 5(3) of the ePrivacy Directive, makes it clear that the legislation applies not only to technologies that consist in storing data in the user's web browser, such as cookies or web storage but also to technologies that deal with data that can be retrieved from the terminal and that are indicative of its hardware or software, such as fingerprinting. In my view, it does not cover passive fingerprinting, which would fall under the less strict notice regime of Article 8(1) of the proposal.

The only substantive change to the mainly consent-based regime of Article 8(1) of the Proposal compared to Article 5(3) of the ePrivacy

69 On the relationship between the ePrivacy Directive and the GDPR, see 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' (12 March 2019) https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en.pdf accessed 21 August 2023; Etteldorf, Christina. 'EDPB on the Interplay between the ePrivacy Directive and the GDPR' (2019) 2 European Data Protection Law Review https://edpl.lexxion.eu/article/EDPL/2019/2/12) accessed 21 August 2023.

70 For example, see Commission nationale de l›informatique et des libertés, 'Délibération n° 2020-092 du 17 septembre 2020 portant adoption d›une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs «' (17 September 2020) https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf accessed 21 August 2023.; Information Commissioner›s Office, 'How do we comply with the cookie rules?' (https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/ accessed 21 August 2023.

71 Veale and Borgesius (n 16) 236.

72 Veale and Borgesius (n 16) 236.

73 GDPR, rec. 42

74 European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (13 April 2021) https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf accessed 21 August 2023, para 72ff; Veale and Borgesius (n 16) 236.

75 European Data Protection Board, 'Report of the work undertaken by the Cookie Banner Taskforce' (17 January 2023) https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf) accessed 21 August 2023.

76 European Data Protection Board (n 75).

77 Commission proposal (n 6).

78 Parliament, 'Report on the 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)' A8-0324/2017 https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html accessed 21 August 2023 (hereafter the "Parliament's position").

79 For a summary of developments at different stages, see Council, '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) - Progress report. 2017/0003(COD), 13106/20' (23 November 2020) https://data.consilium.europa.eu/doc/document/ST-13106-2020-INIT/en/pdf accessed 21 August 2023; Council, '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). 2017/0003(COD), 5008/2' (5 January 2021) https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf accessed 21 August 2023. For an overview of all versions, see the history of the proposal at the website of the Publications Office of the European Union, '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). 2017/0003(COD)' 52017PC0010 https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0010 accessed 21 August 2023.

80 See Council, '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) - Mandate for negotiations with EP. 2017/0003(COD)' 6087/21 (10 February 2021) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT accessed 21 August 2023 (hereafter the "Council's position").

Directive is that consent should not be required for "*website traffic measurement*" (under certain conditions). The proposed obligations for web browser developers under Article 10 are rather soft, essentially requiring just the ability to block cookies and similar technologies.[81]

Compared to the Commission's proposal, the Parliament's position has namely added a provision specifically prohibiting cookie walls from preventing access to a website when consent is not given.[82] Also, the obligations of web browser developers have been significantly revised in Parliament. Newly, web browsers would have to block cookies and similar technologies by default, except for those that are technically necessary, offer the user the option to agree to or change this default setting upon installation, also offer the option to choose to block cookies and similar technologies for measuring traffic, and offer the option to give specific consent through settings of the browser.[83] Parliament's position also extends the consent requirement to passive fingerprinting where it serves other than technical or statistical purposes.[84]

The parallel and subsequent discussions in the Council were complicated – they lasted more than 4 years and produced at least 12 different versions of the proposal containing partial amendments concerning Article 8 and related recitals.[85] At the outset of the discussions, some Member States expressed the need to find a balanced solution to the problem of "*consent fatigue*", i.e. the overload of users with multiple consent requirements.[86] The technical and economic characteristics of the internet advertising ecosystem were also an important topic of discussion.[87]

Concerning cookies and similar technologies, in the final version of the Council's position, Article 8(1) does not differ substantially from the original text proposed by the Commission.[88] A requirement to consent to passive fingerprinting for non-statistical purposes was then added to Article 8(2), similar to the Parliament's position.[89]

The main changes concern the Recitals of the proposal and Articles 9 and 10. In Recital 20aaaa, it has been added that access to a website without direct payment may be made conditional on consent to the storage and reading of cookies without depriving the user of his free choice, provided that the user is clearly informed about the use of cookies and is given the choice between a consent service option and an equivalent offer that does not require consent.[90] At the same time, however, Recital 21aa states that the use of cookies may be necessary in the case of a website that is predominantly funded by advertising provided that the user is adequately informed about the purposes of the use of cookies and has accepted such use.[91]

Articles 9 and 10 were then recast in Article 4a, which however contains the minimum of the Commission's original proposal in terms of requirements for web browser functionality. Thus, the article only provides that consent can be given via a web browser.[92] However, it is now added that this consent should override the software settings and, if given by the user for a particular service, should be reflected immediately.[93]

The substance of the original Article 10 is then moved to Recital 20a, which states that end-users face frequent requests for consent to use cookies, which can lead to end-users being overloaded and not reading consent requests, and this can result in a reduction in the level of protection provided. Therefore, it would be useful to be able to give specific and informed consent for one or more purposes through the browser settings, for example by means of a list of providers that will be allowed to use certain types of cookies. The rationale encourages web browser developers to create such options, but this is not a legally binding obligation. In addition, the Recital adds that "*directly expressed*" consent (presumably meaning consent in relation to a specific website) should always take precedence.[94]

In summary, the positions of the Commission, Parliament and Council differ. The Commission proposes are rules largely similar to the current Article 5 of the ePrivacy Directive, with minor changes and a basic obligation for web browser developers. The Parliament proposes strict rules based on mandatory granular consent settings in web browsers and technical signals of consent binding on websites. The Council reduces all obligations for web browser developers and opens the way to impose the use of cookies as a condition for access to free content and services. Consent plays a key role in all versions of the proposal.

6. Critique of the consent-based approach

The approach to regulating cookie use based on user consent is a manifestation of a control-based approach to privacy that has a long history. In 1890, Warren and Brandeis saw the essence of the right to privacy as "*the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others*".[95]

This approach to privacy has not lost its relevance in modern times. Similarly, Alan Westin's widely cited work *Privacy and Freedom* defines privacy as *"the claim of individuals, groups or institutions to determine*

81 Commission proposal (n 6) arts. 10(1) and (2).
82 Parliament's position (n 80) amendment 92.
83 Parliament's position (n 78) amendments 106 to 109. This individual setting should probably also be initiated by the individual website. See Parliament's position (n 78) amendment 116. At the same time, these settings of consents and objections to processing within the meaning of Article 21 GDPR should be reflected in the technically specified signals sent to websites. These signals should then be binding for the websites concerned. See Parliament's position (n 78) amendments 103 and 111 to 115.
84 Parliament's position (n 78) amendments 95 to 99.
85 Publications Office of the European Union (n 79).
86 Council, '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) - Discussion on possible compromise solutions. 2017/0003(COD)' 5934/19 (4 February 2019) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5934_2019_INIT) accessed 21 August 2023, 3
87 Council, '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) - Presidency note. 2017/0003 (COD)' 10866/17 (3 July 2017) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10866_2017_INIT accessed 21 August 2023, 4.
88 Council's position (80).
89 Council's position (80) art. 8(2).
90 Council's position (80) rec. 20aaaa. This rule should not be applicable in the case of a significant imbalance between the end-user and the service provider, for example in the case of services provided by public institutions and service providers in a dominant position on the market.
91 Council's position (80) rec. 21aa.
92 Council's position (80) art. 4a(2).
93 Council's position (80) art. 4a(2aa).
94 Council's position (80) rec. 20a.
95 Samuel. D. Warren / Louis D. Brandeis, 'The Right to Privacy' (1890) 5 Harvard Law Review 193, 198.

for themselves when, how, and to what extent information about them is communicated to others."[96] Warren and Brandeis are followed in thought by Adam D. Moore, who defines privacy through the content of the right to privacy, describing it as the right to control access to one's person and information about one's person.[97] Similarly, Roger Clark defines privacy as *"the interest that individuals have in sustaining 'personal space', free from interference by other people and organisations."*[98] Clark's definition is based on Morison, who describes privacy as the state of an individual being free from interference with their intimate interests.[99]

However, the control-based approach to privacy is struggling with the way we use the web. Every time a user opens a website, complex processing of information about him or her starts, often including multiple parties and processes. Considering the number of websites an active user may potentially view a day, he can hardly meaningfully exercise his control over all these processes. In the words of Woodrow Hartzog, control is not a *"bottomless well"*.[100]

As rightly stated in Recital 20a of the Council's position, Internet users are frequently asked to consent to the use of cookies, which can lead to user overload and users not reading consent requests.[101] For example, according to a study by 2020, which looked at the top five consent collection tools used on the 10,000 most visited websites in the UK, the median number of third parties listed in the consent dialogue was 315. The text describing these third parties averaged 7,985 words, which would mean that a reader reading 250 words per minute on each website would spend an average of over 31 minutes reading information about the third parties covered by the consent they were being asked to provide.[102]

According to a 2008 study, the average American would have to spend an average of 201 hours in a year to quickly go through all the privacy policies he or she encounters.[103] However, this number would likely be significantly higher today, given the empirically observable increase in the scope of privacy policies, brought about among other things by the adoption of the GDPR, as well as the greater number and complexity of services and websites that an individual encounters. As a result, the time and cognitive effort required to exercise control over one's personal data is enormous.

Even if the user were to read all the relevant policies and information, he or she would likely face an information asymmetry, as data processing processes related to the use of cookies and similar technologies are generally complex and the privacy policy cannot contain all the information available to the website operator.[104] The complexity of these processes is also linked to the complexity of the choices presented. Consent to the use of cookies and similar technologies must comply with the requirements of the GDPR, which means that the request for consent must relate to all the purposes of the processing, and the user must be able to decide on the purposes individually.[105] It is therefore not sufficient to make a single decision concerning a single website, but several such decisions are required (even if they ultimately result in a single act of consent for all purposes).[106]

Furthermore, control through tools such as cookie consent is based on the assumption that users make rational decisions about the choices presented to them. However, this assumption does not correspond to reality. When an individual is faced with choices that are highly uncertain over time (such as the long-term consequences of a single disclosure of personal information), lack information, and generally lack cognitive resources, their decision is not fully rational. Instead, people use what is known as heuristics or shortcuts when making decisions.[107] For example, overestimating the likelihood of phenomena you observe in your environment (as opposed to those you have not encountered) can be considered a heuristic.[108] This can lead to an underestimation of negative privacy impacts because these negative impacts are not common in the population and are difficult to observe. The method of making decisions using heuristics is called "*bounded rationality*".[109]

In addition to heuristics, cognitive and behavioural biases prevent people from making rational decisions.[110] Unlike heuristics, these biases apply as systematic errors in judgement or action to all decisions, regardless of their complexity.[111] An example of an error in judgement is hyperbolic discounting, where an individual underestimates the long-term negative consequences of an action in light of its immediate benefits.[112]

In addition to bounded rationality and biases, decision-making in the exercise of control is influenced by the user interface in which the individual exercises control. This influence is commonly referred

96 Westin, A. *Privacy and Freedom* (Ig Publishing 2018) 24.
97 Adam, D. Moore, *Privacy rights: moral and legal foundations* (Penn State Press 2010) 16.
98 Roger Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' (*Roger Clarke›s Web-Site,* 24 July 2016) http://www.rogerclarke.com/DV/Intro.html#Priv accessed 21 August 2023.
99 William Loutit Morison, 'Report on the law of privacy' (1974) 1.
100 Woodrow Hartzog, *Privacy's blueprint* (Harvard University Press 2018) 63.
101 Regarding users not reading consent requests, see also Oksana Kulyk and others, 'Has the GDPR hype affected users' reaction to cookie disclaimers?' (2020) 1 Journal of Cybersecurity 1/2020, https://academic.oup.com/cybersecurity/article/6/1/tyaa022/6046452 accessed 21 August 2023, 11.
102 Midas Nouwens and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' in Regina Bernhaupt and others, *Proceedings ´20 CHI conference on Human Factors in Computing Systems* (Association for Computing Machinery 2020) https://arxiv.org/abs/2001.02479 accessed 21 August 2023, 4 and 6.
103 Aleecia Mcdonald and Lorrie Faith Cranor, 'The cost of reading privacy policies', (2008) 3 I/S: A Journal of Law and Policy for the Information Society 543, 563.
104 See Alessandro Acquisti and others, 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online' (2017) 3 ACM Computing Surveys https://dl.acm.org/doi/abs/10.1145/3054926 accessed 21 August 2023, 4; Eoin Carolan and Rosario Castillo-Mayen, 'Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws' (2015) 2 Virginia Journal of Law & Technology 324, 380; Ignacio N. Cofone, 'The way the cookie crumbles: online tracking meets behavioral economics', (2017) 1 International Journal of Law and Information Technology https://academic.oup.com/ijlit/article-abstract/25/1/38/2567087 accessed 21 August 2023, 51.
105 See Part 4.
106 Not to mention the cases where the website operator proactively enables decision-making about individual third parties, as required for example by the IAB TCF 2.0 standard. IAB Europe, 'IAB Europe Transparency & Consent Framework Policies', (5 May 2023) https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/ accessed 21 August 2023. Appendix B, Part C, point c.iii. In such cases, there may be dozens of choices.
107 Acquisti (n 104) 2.
108 Acquisti (n 104) 6.
109 Acquisti (n 104) 5.
110 Acquisti (n 104) 6.
111 Acquisti (n 104) 6.
112 Acquisti (n 104) 8.

to as *nudging*.[113] Nudging users of an interface can be done both consciously and unconsciously by its creator. Nudging can be used as a manipulative technique to influence a user towards a decision with negative privacy implications.[114]

Thus, the practical implementation of website consent requests does not lead to greater user awareness of cookies or similar technologies or greater motivation to obtain information.[115] On the contrary, such requests may give users a (not necessarily well-founded) sense of improved privacy protection and motivate them to share more information.[116] At the same time, users often find the requests annoying.[117]

This leads to the conclusion that the consent-based approach to regulating cookies is fundamentally flawed. While consent has its place in regulating invasions of privacy, it must not be overused, and the idea of a user giving complex but meaningful consent on every website is not realistic. This leaves us with the task of finding a way to reduce the number and complexity of the necessary consents to an acceptable level while maintaining or improving the level of privacy protection provided by Article 5(3) of the ePrivacy Directive. My aim here is not to provide a final solution but to suggest possible approaches that should be explored in further research. These suggestions are made in the context of the likely purposes behind Article 5(3), which were to protect users from unauthorised and surreptitious software installations (and more generally from surreptitious tampering with device settings).

First, there are some cases where there is no room for user choice because the technologies involved are too invasive. This is the case with third-party cookies and similar technologies that can be used in a third-party context. Because they can be used to create common identifiers and subsequently share data between websites, they should be blocked by default in all web browsers. This is a measure already implemented by many major web browsers and planned by the rest. To be implemented in all web browsers, it should be mandated by law.

Second, even if third-party cookies are blocked, there are ways to get around this blocking using ETags, fingerprinting or CNAME cloaking. In my opinion, web browser developers should implement state-of-the-art measures to detect and prevent such abuses of these technologies for surreptitious user tracking.

Third, the remaining technologies that could only be used in a first-party context pose such a low risk to web users' privacy that it would make more sense to exempt them from the consent requirement. If they were subsequently used for user tracking, this would still be covered by the GDPR, which would provide the relevant protections but would also offer other legal bases in addition to consent.

Fourth, the law should remain open but cautious towards new technologies such as Protected Audience API and Topics API. Proposals for these technologies currently appear to have shortcomings that make it questionable whether they offer much improvement in terms of privacy compared to third-party cookies. However, later proposals for these or similar technologies may offer more substantial improvements while maintaining their contribution to targeted advertising on websites. Each of these technologies (its specification and prototype) should be carefully assessed. If a reduced privacy impact is demonstrated, the technology should be allowed to be used with reduced requirements for user control. This could mean that the technologies are enabled by default in web browsers, with the user being prompted to confirm that the technology is enabled the first time they use the browser.

7. Conclusion

Cookies and other technologies can be used to track user behaviour online. Third-party cookies are used for privacy-intrusive practices such as cookie synchronisation, which allows data about user behaviour to be shared between websites. Cookies will soon be blocked in all major web browsers, but there are likely to be other browsers that do not have such a strict policy. There are also techniques to get around this blocking, such as using CNAME cloaking, ETags or fingerprinting, and there will continue to be technologies that replace third-party cookies, such as Topcis API and Protected Audience API.

Since 2009, EU law has required consent for the use of cookies and similar technologies that are not technically necessary for the website to function. The strict law was probably not prompted by the advent of the internet and online tracking but by a case of surreptitious software installation.

The current EU cookie law requires consent (beyond technical necessity) for the use of cookies (both third party and first party), similar technologies such as ETrackers and web storage, and the proposed Protected Audience API technology. Active fingerprinting, which includes the use of the proposed Topics API, is also covered by the provision.

The standard for the consent is high and it cannot be expressed by default settings of a web browser. An informed and active indication of the user's wishes, such as a specific click, is required.

Regarding the ePrivacy Regulation, the positions of the Commission, Parliament and Council differ. The Commission proposes rules broadly similar to the current Article 5 of the ePrivacy Directive (with minor changes and a basic obligation for web browser developers).

The Parliament proposes strict rules, including mandatory granular consent settings in web browsers and mandatory technical signals of consent on websites. The Council reduces all obligations for web browser developers and paves the way for imposing the use of cookies as a condition for access to free content and services. Consent plays a key role in all versions of the proposal.

However, the consent-based approach is flawed because it relies on control that cannot be exercised over the number and complexity of data processing operations triggered by a user's browsing. Simply familiarising oneself with the relevant information would be extremely time-consuming and would still leave the user in a position of information asymmetry. In addition, consent decisions could be influenced by heuristics, cognitive biases and nudging.

113 Acquisti (n 104) 10.
114 European Data Protection Board, 'Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them' (14 March 2022) https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf accessed 21 August 2023. However, nudging can also be used as a tool to mitigate the control problems described above. Acquisti (n 104) 25.
115 Cofone (n 104).
116 Carolan (n 104) 378.
117 Kulyk (n 101) 32.

I, therefore, believe that it should be mandatory for web browser developers to block third-party cookies by default. They should also be required to implement state-of-the-art measures to detect and prevent techniques such as CNAME cloaking or the use of ETags and fingerprinting. In addition, first-party cookies could be exempted from the consent requirement, and for technologies that replace third-party cookies, the consent requirement could be reduced to confirming the activation of the technology upon first use of the web browser, provided that the technology is evaluated and its reduced privacy impact is demonstrated.

Aknowledgements

This article was written within the project "Law and Technology XI", MUNI/A/1293/2022. The author would like to thank Matěj Myška, Jakub Míšek, Vladan Rámiš and František Nonnemann for their feedback on the ideas behind the text. Any errors are the sole responsibility of the author.