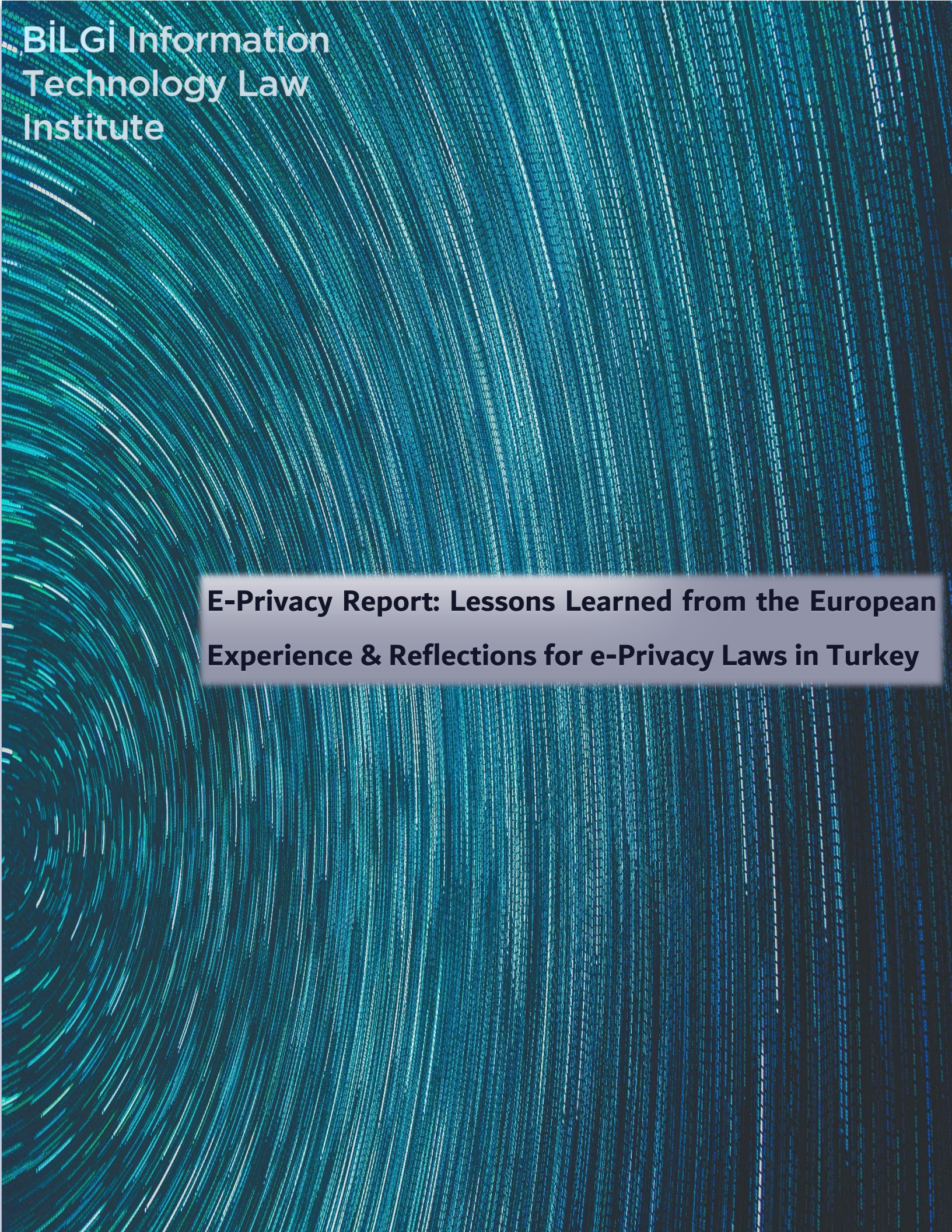

BİLGİ Information Technology Law Institute

E-Privacy Report: Lessons Learned from the European Experience & Reflections for e-Privacy Laws in Turkey

BİLGİ Information Technology Law Institute

E-PRIVACY REPORT v.01: Lessons Learned from the European Experience & Reflections for e-Privacy Laws in Turkey[1]

Authors:

Leyla KESER BERBER

Ayça ATABEY

Ezgi EREN

IT Law Institute

Istanbul Bilgi University

September 2020

BİLGİ Information Technology Law Institute

[1] *This is v.01 (PART I) of the e-Privacy Report. The final version of this Report will consist of a revised version of PART I and PART II.*

E-Privacy Report v.01:

Lessons Learned from the European Experience & Reflections for e-Privacy Laws in Turkey

Introduction 4

Methodology of the Report 7

Scope and objectives 8

PART I 9

Section I: E-privacy Chronology in the EU and Turkey 9

A. Overview of the European Regulatory Framework 9

i. Scope and objectives of the e-Privacy Regulation 10

ii. The interplay between the GDPR and e-Privacy laws 12

iii. The relationship of e-Privacy Regulation with other legislative frameworks 17

iv. The institutional framework of e-Privacy Regulation: duties, powers and coordination 18

v. On the way to the long-awaited e-Privacy Regulation: A brief history of e-Privacy laws in the EU 20

- e-Privacy Directive numbered 2002/58 22

- The introduction of the Cookie Directive numbered 2009/136 and the reasons behind its failure 23

- The Draft e-Privacy Regulation (the new Proposal for the e-Privacy Regulation) 25

B. Challenges faced: a summary of the current debates surrounding the draft e-Privacy Regulation 28

C. Turkey's approach towards e-Privacy 31

i. Legislative History and the Current Regulatory Framework 31

ii. The new e-Privacy Regulation Draft published by ICTA 32

Section II: Location tracking and online identifiers under the draft e-Privacy Regulation: A deep dive into the current approach in the EU 36

A - Online Tracking Technologies 36

i. Cookies 39

ii. Other tracking methods 48

iii. First party/third-party tracking 52

iv. RTB and Micro Targeting 55

v. Alternatives and contextual advertising 65

vi. Analytics 70

vii. Mobile privacy 73

B - Location Tracking 75

i. The State of the Art of Location Tracking 76

ii. Location Tracking and COVID-19 80

iii. Location Tracking and e-Privacy 82

iv. Location tracking in the Draft e-Privacy Regulation 83

C - Next generation profiling tools: Cookie-less tracking 85

D - Debates/Challenges 87

i. Tracking/Cookie Walls and Forced Consent 87

ii. Do-Not-Track signals 94

iii. Introduction of legitimate interests as a ground for processing of electronic communications data, including both content and metadata 97

iv. Online child abuse and e-privacy 100

v. Backdoors and weakened security 103

vi. Data retention 104

vii. Competition and ePrivacy: the CMA report and Google's acquisition of Fitbit 104

Concluding Remarks 109

Bibliography 111

Introduction

With the ubiquity of the internet and ever-advancing technologies, the fundamental rights to data protection and privacy have gained a new dimension. The latest developments in the field of data protection and e-Privacy laws have accordingly become soaring topics globally. The legal framework in the EU with the GDPR and the upcoming e-Privacy Regulation are now widely recognised to be revolutionary defences in the fundamental rights to data protection and privacy in the world. Due to the high standards this framework imposes, it can also be perceived as a threat for industries such as online advertising that live on end-user's data in today's golden age of the data-driven economy.

While the enactment of the GDPR has created a new battlefield for different stakeholders, especially for the tech giants in the online advertising ecosystem, the delays in the enactment of the long-awaited e-Privacy Regulation have resulted in ambiguity among different stakeholders. This ambiguity encapsulates many questions especially with regards to online advertising and the notion of 'consent' which are still expected to be resolved with the enactment of the e-Privacy Regulation. This is mainly because the current e-Privacy regulatory framework has become outdated and fails to keep up with the current issues faced with regard to various topics such as processing of metadata including location data, cookies and other novel technologies used in online advertising, data processing relating to Internet of Things (IoT) devices and machine to machine communications, all of which have a significant place in today's digital economy. In EDPS' 2020-2024 Strategy, there is reference to the increasing backlash against third party cookies and novel methods of identifying individuals and relevant data protection and privacy challenges.[2] Recent developments pave the way for finding alternatives to current tracking technologies and an incline to use cookieless tracking methods.[3]

[2] European Data Protection Supervisor, 'The EDPS Strategy 2020-2024 - Shaping a Safer Digital Future' (2020) 8, 18 <https://edps.europa.eu/sites/edp/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf> accessed 21 August 2020.

[3] See for example, the work of W3C on novel tracking methods, Lara O'Reilly, Interview with Wendy Sletzer, 'A Key Web Standards Group Will Help Decide What Comes after the Third-Party Cookie' (29 January 2020) <https://digiday.com/media/wendy-seltzer-how-w3c-groups-work/>; For technical details, see 'W3c/Web-

All these technological developments increase the need for a new e-Privacy framework in the EU, but also underline how sensitive the balance between the technology and the laws that regulate it is. The recent history of e-Privacy in the EU, as will be detailed in this Report, prove the importance, for regulatory bodies, of keeping up with the technological developments, as well as of having a decent understanding of the technologies they attempt to regulate and the foresight that comes along with it to predict the practical effects of the regulations.

Section I of this Report will start with a comprehensive overview of the European regulatory framework, provide a brief history of the e-Privacy laws, explain its scope and objectives by underscoring the importance of the interplay between the e-Privacy laws and the GDPR, its relationship with the other legislative frameworks, as well as the institutional framework of e-Privacy Regulation explaining the duties, powers and coordination under the current system. An analysis of the e-Privacy Directive numbered 2002/58 will be provided by elaborating on the EU's past framework directives regime pointing out the fact that the e-Privacy Directive was one of the five directives (called framework directives) which shaped collectively the EU's e-communication approach. The comprehensive evaluation will be furthered by explaining the subsequent developments in the EU legal framework and address the discussions stemming from the reasons behind the failure of the e-Privacy Directive, the changes that are brought with the Cookie Directive numbered 2009/136 and the perplexed situation created by the already existing problems which are hoped to be addressed in the final version of the e-Privacy Draft Regulation prior to its enactment.

Following a detailed evaluation of the European regulatory framework, the current laws and provisions in Turkey will also be outlined for comparison purposes while pointing out the current provisions in the e-Privacy Regulation Draft. The scope of these provisions will be discussed by mainly referring to the currently debated challenges that bear the risk to remain unsolved if the necessary amendments are not implemented in the final version before the enactment of the e-Privacy Regulation.

Advertising' <https://github.com/w3c/web-advertising>; See also Timothy C Storm, 'Cookieless Tracking System' <https://patents.google.com/patent/US20080172495>.

Section II of this Report will focus on online identifiers used in advertising, tracking and location data, some of the most problematic topics waiting to be resolved with the new e-Privacy Regulation, and how the draft regulation approaches these topics. The Report will address new developments in tracking technologies, plans for new generation profiling tools and "cookieless tracking", the draft e-Privacy Regulation's position in the face of these new technologies and whether it provides the appropriate standards. Finally, in PART II of this Report, we will try to establish a position regarding the optimum approach for Turkey to balance user privacy and online advertising.

The reason behind such focus on online advertising and tracking methods is that there seems to be an ever evolving conflict between user privacy and the data economy when it comes to these fields, and there is an urgent need to address the question of how a balance could be reached between user privacy and the data economy. Therefore, this report aims to address the various ways the new regulation could provide some relief and the challenges its current draft presents. Another question that will be considered in the report is whether a focus on self-regulation/co-regulation and increasing digital literacy would be able to bring some relief in the face of the long standing conundrum regarding the draft e-Privacy Regulation. In order to provide a thorough understanding of the e-Privacy laws, the upcoming draft regulation and its implications on these topics, the recent developments, academic literature, commentaries from the relevant industries as well as the legal and practical concerns will be addressed while explaining the potential impact the upcoming e-Privacy Regulation will create on different stakeholders, especially in online advertising sector.

The evolving e-Privacy ecosystem in the EU currently prevents this Report from reaching definitive legal conclusions, as any such conclusion is bound to change with the final version of the draft e-Privacy Regulation. Nevertheless, one conclusion that the Report reaches is that the results derived from the comprehensive analysis carried out throughout are of utmost importance for Turkey to learn lessons from the EU's experience in order to adopt the optimal approach where different stakeholders' rights and interests are safeguarded after a careful consideration. Only then can a healthy balance be achieved between these rights and interests to ameliorate the currently existing system.

In PART I of our Report, we explain e-Privacy chronology in the EU, a summary of the current debates surrounding e-Privacy draft Regulation, Turkey's approach towards e-Privacy, location tracking and online advertising and relevant challenges with regards to online advertising technologies and e-Privacy laws. In PART II of the Report, we will aim to provide a road map for adopting e-Privacy laws that are built on the data minimisation principle as well as other core data protection principles which would lead to an advertising world that is more respectful to data privacy. We will aim to discuss current challenges considering the ever-developing novel technologies including already existing ones as well as new ones such as "cookieless tracking" systems and address their legal implications in this context. After presenting the current situation with regards to e-Privacy laws and providing an overview of the existing challenges in PART I, we will provide recommendations to draw a roadmap for Turkey in PART II, which will also contain a small impact and UX assessment concerning analytics cookies based on analysis of different websites and outcomes of the interdisciplinary research we carried out by adopting a multi stakeholder approach.

All in all, this Report aims to address the most debated topics and current challenges regarding the upcoming e-Privacy Regulation in the EU, especially concerning online tracking, cookies, the plans for new "cookieless tracking" schemes and location data. The stalemate faced in the EU points out to the constant conflict between various stakeholders. The upcoming plans for cookieless tracking could decrease the potential effect of the current plans for the new e-Privacy Regulation. All these developments underline how crucial it is for the lawmakers to keep up with the new technologies before taking regulatory action. Moreover, the fast pace of technological developments points to soft laws or different regulatory approaches such as co-regulation/self-regulation as a source of relief in this constant conflict.

Methodology of the Report

This Report looks into different approaches to ePrivacy laws and addresses issues which rotate around the debates relating to ePrivacy regimes and ever developing advertising technologies. This Report presents different perspectives adopted by various stakeholders and compares the existing laws in the EU and Turkey, as well as opinions of relevant academic commentators and policy makers with the purpose of drawing a road map for Turkey. To do so, we analysed national

regulations, policies, policy recommendation papers, opinions of public authorities, academics, and the private sector. We also conducted unstructured interviews with experts from the digital advertising industry and officials. We will aim to reflect the results we inferred from these interviews in PARTI II of our Report in accordance with the anonymity principles. Our research team consists of technologists, lawyers, publishers, advertisers, academics, and experts in the field who shared their experience and valuable opinions with us helping us to analyse the practical issues concerning e-Privacy laws and novelties in the advertising industry. PART I of our Report provides a general framework explaining the chronological advent of e-Privacy laws in Europe and addresses main challenges that have become soaring topics lately. In PART II of our Report we will aim to delve into the business impact to turn off all cookies (except necessary cookies) on websites, the implications of cookieless tracking technologies while addressing the question of how do we balance user privacy and the data economy in the context of online advertising. To do so, we will also look at the legislation aspect and question whether we need strict regulations to protect users or self-regulation/co-regulation and how digital literacy could be seen as a compelling option in enhancing individuals' rights to data protection and privacy. We will try and explore collaboration options within the ecosystem and underscore the role of digital literacy and clear regulations that enhance individuals' rights and freedoms while making sure not to undermine other stakeholders' rights and interests. Lastly, with this setting and possible answers to the mentioned questions, we will try to draw a map for Turkey in an effort to find the optimum approach for Turkey in order to find the right balance between protecting users' right to privacy and supporting transparency, fairness, and innovation in the golden age of online advertising industry.

Scope and objectives

This Report consists of two PARTS and aims to address the most debated topics and current challenges regarding the upcoming e-Privacy Regulation in the EU, with a specific focus on online identifiers and tracking, including new "cookieless tracking" technologies. The Report tries to answer the questions of how to balance user privacy and the data economy in terms of online advertising, as these areas need the most consideration and are most significantly affected from the e-Privacy regulatory reform, and whether strict regulations are needed to protect users or if self-regulation/co-regulation along with improved digital literacy of users could provide much needed relief in this regard. Following these questions, this Report thoroughly evaluates the current

issues rotating around the e-privacy laws while underscoring the importance and the role of ever-advancing "cookieless tracking" technologies in today's golden age of online advertising. Lastly, this Report furthers the discussion by making recommendations to achieve the optimum approach in Turkey in pursuit of protecting different stakeholders and finding the right balance between user privacy and online advertising economy.

PART I

Section I: E-privacy Chronology in the EU and Turkey

A. Overview of the European Regulatory Framework

The European Commission issued a proposal for a new e-Privacy law on January 10, 2017, that sought to replace the existing e-Privacy and Electronic Communications Directive numbered 2002/58,[4] which was enacted in 2002 to oversee privacy regulations across the EU. In the European Union, the General Data Protection Regulation (GDPR)[5] dated 2018 provides comprehensive rules for the processing of personal data. In addition, the EU lawmakers intended to adopt specific rules to protect confidentiality of communications, in a separate e-Privacy Regulation.[6]

Privacy and data protection are fundamental rights that are protected under the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights, through Article 8 of the ECHR (titled 'Right to respect for private and family life') and Articles 7 and 8 of the EU Charter of Fundamental Rights (titled 'Respect for private and family life' and 'Protection of personal data' respectively). The scope of the GDPR only covers Article 8 of the Charter, namely the right to data protection. In other words, the GDPR aims to regulate the rules relating to data

[4] 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) [2002] OJ L 201/37.

[5] 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.

[6] For arguments stating there is no need for such additional rules for communications confidentiality, see Frederik Zuiderveen Borgesius and Wilfred Steenbruggen, 'The Right to Communications Confidentiality in Europe: Protecting Trust, Privacy, and Freedom of Expression' (Social Science Research Network 2018) SSRN Scholarly Paper ID 3152014 <https://papers.ssrn.com/abstract=3152014> accessed 23 August 2020.

protection, not the privacy of communications. In today's digital world, in order to ensure adequate protection of the fundamental rights to privacy and the protection of personal data, the adoption of the proposed e-Privacy Regulation is necessary to fill the gap that exists due to this lack of specific protections aimed towards privacy. The EU's framework cannot be considered complete without an e-Privacy reform.[7]

This Section provides an overview of the European regulatory framework for ePrivacy laws. It starts with providing a summary of e-Privacy Regulation by explaining its scope and objectives. It further provides a general picture for the interplay between the GDPR and e-Privacy laws in the EU. The Section continues with a brief explanation of the relationship of the e-Privacy Regulation with other legislative frameworks and the institutional framework presented by the e-Privacy Regulation, duties and powers of and coordination between different institutions having a role in the observation and enforcement of the e-Privacy Regulation. Afterwards, a brief history of the e-Privacy laws in the EU is presented, starting from the e-Privacy Directive numbered 2002/58, ending on the cancellation of the draft e-Privacy Regulation at the end of 2019 and the most recent work on the draft by the Croatian Presidency.

i. Scope and objectives of the e-Privacy Regulation

The European Commission's proposal for a Regulation on Privacy and Electronic Communications has as its main objective to reinforce trust and security in the Digital Single Market by updating the legal framework on the laws and rules relating to e-Privacy.[8] The EU's e-Privacy Regulation was supposed to take effect alongside the GDPR in May 2018. Yet, as the EU reaches its data protection golden age with the enactment of the GDPR, the e-Privacy Regulation remains in draft. The Commission adopted its proposal for a Regulation on Privacy and Electronic Communications in January 2017.[9] Through this proposal, the main aim is to protect confidentiality of

[7] Giovanni Buttarelli, 'The Urgent Case for a New EPrivacy Law' (*European Data Protection Supervisor - European Data Protection Supervisor*, 19 October 2018) <https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en> accessed 23 August 2020.

[8] European Commission, 'Proposal for an EPrivacy Regulation' (*Shaping Europe's digital future - European Commission*, 10 January 2017) <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation> accessed 23 August 2020.

[9] 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) 010 final 2017.

communications, as provided for in the Charter of Fundamental Rights, but also to ensure the protection of personal data that may be a part of a communication as well as terminal equipment of end users.[10]

The proposed e-Privacy draft Regulation stipulates on and complements the Regulation by setting out particular rules aligned with the GDPR. It aims to modernise the current EU e-privacy rules[11] to mirror technological and legal developments. Moreover, the draft regulation refers to the new Directive (EU) 2018/1972 (European Electronic Communications Code or EECC)[12] for the definition of electronic communications services. This reference is significant as the EECC's definition of electronic communications services now includes, taking into account the most widely used communication technologies of today, services that are functionally equivalent to more traditional communications services, such as Voice over IP (VoIP), e-mail, etc. As a result, the e-Privacy regulation enhances individuals' exercise of their right to privacy through widening the scope of the new rules to also encompass over-the-top communications service providers, thus creating a level playing field for all electronic communications services. As mentioned above, this Report puts emphasis on the draft Regulation's approach towards online tracking and location data, and the widening of the scope of the draft Regulation also allows the inclusion of new technologies used in such contexts.

The need for updating the e-Privacy legislation has come in line with the necessity triggering the European legislation to keep up with the fast pace of development of IT services and products. The European Commission commenced a modernisation process of the data protection framework that was concluded in May 2016 by adopting the new GDPR.[13] In parallel with this change, bringing the e-Privacy legislation into alignment with the new rules that are brought with the enactment of

[10] European Commission, 'Communication from the Commission to the European Parliament and the Council - Data Protection Rules as a Trust-Enabler in the EU and beyond – Taking Stock' <https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/communication_2019374_final.pdf> accessed 24 August 2020.

[11] 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) [2002] OJ L 201/37.

[12] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L 321/36 2018.

[13] European Commission, 'Data Protection' <https://ec.europa.eu/info/law/law-topic/data-protection_en> accessed 24 August 2020.

the GDPR has become a necessity. It is also important to note that both data protection rules that are brought by the GDPR and will be complemented with the e-Privacy Regulation are seen as a trust-enabler in the EU and beyond.

ii. The interplay between the GDPR and e-Privacy laws

This subsection aims to provide a thorough understanding of the contextual and substantive relationship with the GDPR for which subjects GDPR preferred to be silent and just refer to draft e-Privacy Regulation; how e-Privacy draft Regulation completes the GDPR. It particularly focuses on the concept of metadata in the context of the interplay between the GDPR and e-Privacy laws.

As addressed in Article 1 of the GDPR, the GDPR has the objective "*to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*" and to ensure "*the free movement of personal data within the Union*". The rules provided under the GDPR serve to ensure a balance between the (potential) benefits of data processing and the (potential) drawbacks. On the other hand, the existing e-Privacy Directive has the objective to *"[harmonise] the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community"* as stated under Article 1(1) of the e-Privacy Directive.[14]

In the European Data Protection Board (EDPB)'s opinion[15] dated 12 March 2019, the EDPB urged EU legislators to intensify efforts toward adoption of the e-Privacy Regulation and discussed the interplay between the ePrivacy Directive (and MS implementing laws) and the GDPR. The EDPB referred to some important points and mostly debated issues as they concern personal data processing activities that may trigger both the e-Privacy Directive and the GDPR. These issues include but are not limited to the competence, tasks and powers of data protection authorities (DPAs), and how these may be affected when a data processing activity triggers both the e-Privacy

[14] See Article 1(1)-(2) of the ePrivacy Directive, to be read in light of article 94(2) GDPR.

[15] 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' (2019) <https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf> accessed 24 August 2020.

Directive and the GDPR; application of the GDPR's cooperation and consistency mechanism; the extent to which processing can be governed by both the e-Privacy Directive and the GDPR. The EDPB's findings that are relevant for the purposes of this Report are explained below.

The use of cookies is a significant processing activity which falls within the scope of both the e-Privacy Directive and the GDPR. In its opinion on online behavioural advertising, the Article 29 WP stated that "*If as a result of placing and retrieving information through the cookie or similar device, the information collected can be considered personal data then, in addition to Article 5(3), Directive 95/46/EC will also apply*".[16] The CJEU jurisprudence also states that it is possible for processing to fall within the scope of both the e-Privacy Directive and the GDPR.[17]

Although it is possible for the processing to fall within the scope of both legislations, the GDPR does not have targeted rules for the processing of metadata on end-users' devices, especially information used for online behavioural advertising, profiling and microtargeting, as well as more complex tracking methods, increasing the significance of the e-Privacy Regulation, which specifically addresses these topics.

Another critical topic specifically regulated under the e-Privacy Regulation is location data (metadata). Information relating to individuals' location can reveal information which may become sensitive depending on the context. For instance, it is possible to deduct socio-economic status of a person on the basis of the neighbourhood they live, specific health problems they may be having on the basis of health clinics they regularly visit, their religious preferences depending on places of worship they spend time in on a daily or weekly basis or their relationships on the basis of where they spent the night.[18] What makes location data even more important is that it is

[16] Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising (WP 171)' (2010) 9 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf> accessed 24 August 2020; See also Article 29 Data Protection Working Party, 'Opinion 1/2008 on Data Protection Issues Related to Search Engines (WP148)' (2008) 12–13 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf> accessed 24 August 2020; (As cited in 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' [n 15]).

[17] See Wirtschaftsakademie CJEU, C-210/16, 5 June 2018, C-210/16, ECLI:EU:C:2018:388. See in particular paragraphs 33-34.

[18] Jennifer Valentino-DeVries and others, 'Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret' *The New York Times* (10 December 2018) <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html> accessed 20 June 2019; Roger Clarke and Marcus Wigan, 'You Are Where You've Been: The Privacy Implications of Location and

possible to make these deductions for most people by means of only four data points indicating location and time.[19]

It is important to note that the location data can be easily abused. For instance, during the protests in the US following the police killings of Breonna Taylor and George Floyd, many people had their location information unknowingly spied on and analysed by Mobilewalla, a company that profiles users of mobile devices, based on demographics and behaviours, using application and location data obtained from other companies handling vast amounts of data, such as advertisers, data brokers and ISPs.[20] The people whose data were collected most probably did not have any knowledge that this was happening, and there was (and still is) no way of limiting what these companies do with the data, unless proper legal limitations are established as to how such data can be collected and processed. In this context, legal boundaries would help create trust and support the data economy, whereas lack thereof would lead to significant insecurity and chilling effects for both sides of the data economy, namely data subjects/people and data companies. Losing their natural anonymity, people may hesitate to participate in protests, fearing they would be prosecuted afterwards. Accordingly, individuals may avoid sharing their location if they knew it would lead to less favourable outcomes; for instance, if they knew they would be presented with less favourable job opportunities, or worse prices in online shopping.[21]

Due to the sensitivity of location information and the potential it carries within, in order to carry out data processing activities for the purpose of location tracking, explicit consent of the data subject is required. As the EDPB states in its guidelines on contact tracing,

---

Tracking Technologies' (2011) 5 Journal of Location Based Services 138, 150–152; 'Your Morning Commute Is Unique: On the Anonymity of Home/Work Location Pairs' (*33 Bits of Entropy*, 13 May 2009) <https://33bits.wordpress.com/2009/05/13/your-morning-commute-is-unique-on-the-anonymity-of-homework-location-pairs/> accessed 26 June 2019.

[19] Yves-Alexandre de Montjoye and others, 'Unique in the Crowd: The Privacy Bounds of Human Mobility' (2013) 3 Scientific Reports 1.

[20] Caroline Haskins, 'Almost 17,000 Protesters Had No Idea A Tech Company Was Tracing Their Location' (*BuzzFeed News*, 25 June 2020) <https://www.buzzfeednews.com/article/carolinehaskins1/protests-tech-company-spying> accessed 30 June 2020.

[21] Alvin Chang, 'How the Internet Keeps Poor People in Poor Neighborhoods' (*Vox*, 12 December 2016) <https://www.vox.com/2016/12/12/13867692/poor-neighborhoods-targeted-ads-internet-cartoon> accessed 24 August 2020; Privacy International, 'Case Study: Invisible Discrimination and Poverty' (*Privacy International*, 30 August 2017) <http://privacyinternational.org/case-study/737/case-study-invisible-discrimination-and-poverty> accessed 24 August 2020.

> "*location data collected from electronic communication providers may only be processed within the remits of Articles 6 and 9 of the ePrivacy Directive. This means that these data can only be transmitted to authorities or other third parties if they have been anonymised by the provider or, for data indicating the geographic position of the terminal equipment of a user, which are not traffic data, with the prior consent of the users.*"[22]

The EDPB also recalls that for information collected directly from the terminal equipment, Article 5(3) of the e-Privacy Directive applies. This includes location data collected from the end-user's terminal equipment as well. Accordingly, the storing of information on the user's device or gaining access to the information already stored is allowed only on the basis of the user's consent or if "the storage and/or access is strictly necessary for the information society service explicitly requested by the user".[23] The second condition in Article 5(3) of the e-Privacy Directive regarding the strict necessity for the provision of the services explicitly requested by the user would concern, for instance, cookies which keep track of items users pick to purchase later on an e-commerce website or cookies placed by online banking websites which serve to present users with information boxes indicating whether they logged in or out safely.[24] On the other hand, tracking an individual's location through their terminal device in a mall in order to send their devices advertisements about various shops they may like to visit would not fall under this and therefore would require their explicit consent.[25]

Studies show that mobile operating systems, device manufacturers or companies that provide platforms for mobile applications carry out data processing activities and share identifiers such as AdIDs and IdFAs with applications that can be found in App Store and Google Play without obtaining users' consent. Although Apple as well as Google Play have taken considerable steps in terms of privacy gaps and security vulnerabilities that existed in their systems in the context of

---

[22] European Data Protection Board, 'Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak' (2020) para 10 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf> accessed 14 August 2020.

[23] ibid 11.

[24] See the second section regarding online identifiers for further details and discussion.

[25] Ayça Atabey, *Is Google at Odds with the GDPR? Evaluation of Google's Personal Data Collection on Mobile Operating Systems in Light of the Principles of Purpose Limitation, Data Minimisation, and Accountability* (1st edn, Oniki Levha Yayıncılık 2020).

mobile applications, there are still concerns with regards to privacy. One of major concerns and challenges related to mobile applications and protection of data subjects' right to privacy and data protection concern data collection activities carried out by tech giants, more specifically, location data without obtaining users' consent.[26] The issue of processing individuals' location data in exceptional circumstances has especially come under spotlight with the recent discussions that rotate around the COVID-19 tracing apps. It is noteworthy that while the use of such apps is mandatory in some countries, both in the EU and elsewhere,[27] Turkey did not force the use of its COVID-19 tracking app. Later on, the EU also chose the same path: the European Parliament stated that the MSs should not force the use of such apps and the apps should include sunset clauses to ensure they will not be used after the pandemic.[28] The Guidelines published by the MSs on 19 May 2020 and supported by the Commission also emphasize the voluntary nature of the apps to ensure interoperability across the EU.[29]

It needs to be noted at this point that the latest proposal for the e-Privacy Regulation prepared by the Croatian Presidency[30] includes legitimate interests as a legal ground for processing electronic

---

[26] See Douglas C Schmidt, 'Google Data Collection' (Vanderbilt University 2018) <https://static.poder360.com.br/2018/08/DCN-Google-Data-Collection-Paper.pdf> accessed 24 August 2020.

[27] Downloading the tracing app has become mandatory for people who have or may have contracted the virus in Poland as of April 2020. See Costica Dumbrava and European Parliamentary Research Service, 'Tracking Mobile Devices to Fight Coronavirus' 6; and Mark Scott and Zosia Wanat, 'Poland's Coronavirus App Offers Playbook for Other Governments' (*POLITICO*, 2 April 2020) <https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments/> accessed 24 August 2020. Some other countries that have a mandatory tracing app are India (see Patrick Howell O'Neill, 'India Is Forcing People to Use Its Covid App, Unlike Any Other Democracy' [*MIT Technology Review*, 7 May 2020] <https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/> accessed 24 August 2020), Qatar (see Aljazeera News, 'Qatar Makes COVID-19 App Mandatory, Experts Question Efficiency' [*Aljazeera*, 26 May 2020] <https://www.aljazeera.com/news/2020/05/qatar-covid-19-app-mandatory-experts-question-efficiency-200524201502130.html> accessed 24 August 2020), China (see Helen Davidson, 'China's Coronavirus Health Code Apps Raise Concerns over Privacy' [*the Guardian*, 1 April 2020] <http://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy> accessed 24 August 2020); and Taiwan (see Yimou Lee, 'Taiwan Tracking Citizens' Phones to Make Sure They Stay Indoors during Coronavirus Lockdown' [*The Independent*, 20 March 2020] <https://www.independent.co.uk/news/world/asia/coronavirus-taiwan-update-phone-tracking-lockdown-quarantine-a9413091.html> accessed 24 August 2020).

[28] European Parliament, 'Covid-19 Tracing Apps: Ensuring Privacy and Data Protection' (5 June 2020) <https://www.europarl.europa.eu/news/en/headlines/society/20200429STO78174/covid-19-tracing-apps-ensuring-privacy-and-data-protection> accessed 24 August 2020.

[29] Erik Lanne, 'Coronavirus: A Common Approach for Safe and Efficient Mobile Tracing Apps across the EU' (*European Innovation Partnership on Active and Healthy Ageing - European Commission*, 19 May 2020) <https://ec.europa.eu/eip/ageing/news/coronavirus-common-approach-safe-and-efficient-mobile-tracing-apps-across-eu_en> accessed 24 August 2020.

[30] Council 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

communications metadata, which also covers location data (Article 6(b)(e), and Article 8(1)(g) regarding the information on the end-user's terminal device). This inclusion may be considered problematic by some stakeholders and will be discussed in detail below. However, as mentioned in the previous paragraph, according to the e-Privacy Directive, which is currently in force, usually the consent of the end-user will be required to process location data.

iii. The relationship of e-Privacy Regulation with other legislative frameworks

One of the most significant aspects of the EU's e-Privacy overhaul is that the privacy of electronic communications will be regulated with a regulation instead of a directive. The choice of regulating e-Privacy via a regulation instead of a directive brings legal consistency and more efficient harmonisation between the laws of MS, since regulations are directly applicable in the national legal systems, whereas Directives need to be transposed into the national law.

On the other hand, within the scope of this Report, the most significant relationship of the e-Privacy Regulation with legislative frameworks other than the GDPR is with the EECC. As mentioned above, the e-Privacy Regulation adopts the definition provided for the electronic communications services in the EECC (Recital 11 and Article 4(b) of the e-Privacy Regulation). This definition *"encompasses not only internet access services and services consisting wholly or partly in the conveyance of signals but also interpersonal communications services, which may or may not be number-based, such as for example, Voice over IP, messaging services and web-based email services*",[31] leading to the inclusion of many online products and services with a tracking component. The e-Privacy Regulation refers to the EECC, specifically to Article 2 of the EECC, also with regards to the definitions of "electronic communications network", "interpersonal communications service", "number-based interpersonal communications service", "number-independent interpersonal communications service", "end-user" and "call". Another aspect where the EECC is brought up, along with the GDPR concerns the security measures to be adopted: Recital 15aa in the current draft states that "In order to ensure the confidentiality of electronic communications data, providers of electronic communications services should apply security

Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (6543/20)' <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6543_2020_INIT&from=EN> accessed 30 June 2020.

[31] Article 4(b) of the draft e-Privacy Regulation

measures in accordance with Article 40 of Directive (EU) 2018/1972 and Article 32 of Regulation (EU) 2016/679".

Other legislations that the draft regulation makes reference to are Directive 2008/63/EC[32] for the definition of "terminal equipment" (Article 1(1), point (1)) and Directive (EU) 2015/1535[33] with regard to the definition of "information society service" (Article 1(1), point (b)). (Article 4(1)(c-d) of the e-Privacy Regulation).

The current draft text of the e-Privacy Regulation includes a new provision concerning the processing of electronic communications data for the purpose of preventing child sexual abuse in its Article 6(d). This Article refers to Directive 2011/93/EU[34], especially to Article 2(c) of the said directive defining the abusive material, establishing a rather significant connection between the legislative framework for the prevention of child sexual abuse.

iv. The institutional framework of e-Privacy Regulation: duties, powers and coordination

The EDPB elaborates on the issue of whether the fact that certain personal data processing prompts both the GDPR and the e-Privacy Directive could somehow limit a DPA's enforcement authority under the GDPR. The EDPB underlines that, as an initial matter, the DPA's power must derive from the MS's law implementing the e-Privacy Directive – that is, the DPA cannot automatically rely on its powers under the GDPR to enforce national e-Privacy rules. Assuming the relevant MS's law provides the requisite backing, a DPA may scrutinize subsets of processing governed by that law. Accordingly, DPAs can enforce the GDPR even if a part of the problematic processing falls within the scope of the e-Privacy Directive. The EDPB found that DPAs can enforce both the

[32] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Text with EEA relevance) [2008] OJ L 162/20.
[33] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (Text with EEA relevance) [2015] OJ L 241/1.
[34] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 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 (Text with EEA relevance) [2009] OJ L 337/11.

GDPR and the e-Privacy Directive, but the latter must be under the auspices of applicable implementing law.

The Draft proposal for the e-Privacy Regulation originally included a paragraph under Article 18, which stipulated that the DPA's designated pursuant to the GDPR would be responsible for monitoring the application of the e-Privacy Regulation (Article 18(1)). Nevertheless, this paragraph was deleted from the Draft. The intention behind the deletion was to provide more flexibility for the MSs; and, the current version adopts a closer approach to that of the e-Privacy Directive.[35] Accordingly, MSs shall designate "one or more independent public authorities meeting the requirements set out in Articles 51 to 54 of Regulation (EU) 2016/679 to be responsible for monitoring the application of this Regulation" (Article 18(0)).[36] It is also possible for MSs to designate one or more different supervisory authorities for matters that fall under the scope of Chapter III of the Regulation (Articles 12-16), governing end-users' rights to control electronic communications.

In the event where there are more than one authorities responsible for monitoring the application of the e-Privacy Regulation, they are required to cooperate with each other, the DPA designated pursuant to the GDPR and the supervisory authority responsible with the monitoring of the application of the EECC (Article 18, paragraphs (1(b)) and (2)). The supervisory authorities are also required to cooperate with others in the EU as well as with the Commission (Article 20).

The supervisory authorities are bestowed with investigative and corrective powers and may impose administrative fines pursuant to Article 23 of the e-Privacy Regulation (Recital 40, Article 18(1ab)). With regards to the penalties under e-Privacy laws, the e-Privacy Regulation applies the same fine as the GDPR. Anyone found to violate its requirements will be fined up to 20 million Euros or 4% of annual global revenue (Article 23).

---

[35] Council 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) - Progress Report (9351/19)' para 8 <https://data.consilium.europa.eu/doc/document/ST-9351-2019-INIT/en/pdf> accessed 24 August 2020.

[36] See Council 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) (7099/19)' <https://data.consilium.europa.eu/doc/document/ST-7099-2019-INIT/en/pdf> accessed 24 August 2020.

The e-Privacy Regulation also elaborates in its Article 19 the role of the EDPB. The Board is tasked with preparing guidelines, recommendations, best practices regarding the consistent and coherent application of the first three chapters of the Regulation, and promoting cooperation between different supervisory authorities within the EU.

Generally, it can be observed that the initial draft of the e-Privacy Regulation had a more precise approach to ensure full consistency with the GDPR with regards to supervision, while the current version leaves more leeway for MSs to designate supervisory authorities and their respective responsibilities.[37] In the current situation, the approach aiming for full consistency with the GDPR seems to have taken a backseat.

v. On the way to the long-awaited e-Privacy Regulation: A brief history of e-Privacy laws in the EU

On the way to the ePrivacy Regulation, the advent of the data protection and electronic privacy policies and rules in the EU had started in the 70s and early 80s as recommendations[38] and beginning from 90s, rules relating to data protection and electronic privacy appeared in the form of legislation starting with the Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data[39], and continued with Directive 97/66/EC concerning the Processing of Personal Data and the Protection of Privacy in

[37] Frederik Zuiderveen Borgesius and others, 'An Assessment of the Commission's Proposal on Privacy and Electronic Communications' (Social Science Research Network 2017) SSRN Scholarly Paper ID 2982290 <https://papers.ssrn.com/abstract=2982290> accessed 24 August 2020.

[38] See for example European Parliament, 'European Parliament Resolution on the Protection, of the Rights of the Individual in the Face of Technical Developments in Data Processing [1979] OJ C 140/34' <https://resources.law.cam.ac.uk/cipil/travaux/data_protection/1979%20-%20European%20Parliament%20Resolution%20on%20DP.pdf>; European Commission, 'European Commission Recommendation of 29 July 1981 Relating to the Council of Europe Convention for the Protection of Individuals with Regard to Automated Processing of Personal Data [1981] OJ L 246/31' <https://resources.law.cam.ac.uk/cipil/travaux/data_protection/1981%20-%20Commission%20Recommendation%20on%20CoE%20Convention%20OJ%20L246-31.pdf>; and European Parliament, 'European Parliament Resolution on the Protection of the Rights of the Individual in the Face of Technical Developments in Data Processing OJ C 87/39' <https://resources.law.cam.ac.uk/cipil/travaux/data_protection/1982%20-%20Euro%20Parl%20Resolution%20on%20DP%20OJ_C_1982_087%20-%20Final.pdf>.

[39] 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 [1995] OJ L 281/31.

the Telecommunications Sector,[40] 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) which is amended by Directive 2006/24/EC[41] and Directive 2009/136/EC[42] and finally the 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.

The e-Privacy Regulation is one of nearly thirty legislation of the EU concerning Digital Market Strategy and Digital Europe. Therefore, it has inherent patterns and references to other related laws and regulations, which underpin the EU's digital economy. The European Commission issued a proposal for a new e-Privacy law on January 10, 2017, that sought to replace the existing e-Privacy and Electronic Communications Directive, which was enacted in 2002 to oversee privacy regulations across the EU.[43] In the EU, the GDPR provides comprehensive rules for the processing of personal data. In addition, the EU lawmakers intended to adopt specific rules to protect confidentiality of communications, in a separate e-Privacy Regulation. The European Commission issued a proposal for a new e-Privacy law on January 10, 2017, that sought to replace the existing e-Privacy and Electronic Communications Directive, which was enacted in 2002 to oversee privacy regulations across the EU. In the EU, the GDPR provides comprehensive rules for the processing of personal data. In addition, the EU lawmakers intended to adopt specific rules to protect confidentiality of communications, in a separate e-Privacy Regulation.

[40] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [1997] OJ L 24/1.

[41] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105/54. Note that the Directive 2006/24/EC was declared invalid by Judgment of the Court (Grand Chamber); *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*.

[42] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 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 (Text with EEA relevance) [2009] OJ L 337/11.

[43] For a comprehensive list of sources on transnational European initiatives in data protection and electronic privacy since the 1970s see Centre for Intellectual Property and Information Law, 'European Data Protection and Electronic Privacy: Transnational Resources' <https://www.cipil.law.cam.ac.uk/resources/pan-european-data-protection-and-e-privacy>.

- **e-Privacy Directive numbered 2002/58**[44]

The European Directive 97/66/EC concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector[45] was introduced in 1997; this Directive was later replaced by the European Directive 2002/58/EC on Privacy and Electronic Communications[46] which is also known as "the e-Privacy Directive" and which aimed to safeguard the confidentiality of electronic communications in the EU. The Directive was introduced as part of the 1999 Communications Review and aimed to provide specific data protection rules for the e-communications sector.[47] Yet, the Directive was left out of the Review package and was adopted in 2002 with the objective to address the necessities of ever developing digital technologies.

The e-Privacy Directive was and still is a key legal instrument to protect privacy; it covers specific rules on data protection in the area of telecommunication in public electronic networks. The e-Privacy Directive was one of the five directives that shaped collectively the EU's communication approach. The purpose of e-Privacy Directive was to "complement and particularise" matters that fell within the scope of the general data protection legislation of the EU, Directive 95/46/EC (the 1995 Directive on Data Protection, or the Data Protection Directive, the predecessor of the GDPR).

The e-Privacy Directive complements the general data protection framework and provides more specific privacy rights on electronic communications.[48] It recognises that wider public access to mobile networks and the internet introduces new possibilities for businesses and users, however these possibilities come with new risks to their privacy. Although the e-Privacy Directive is known to complement the general data protection regime, when compared to the Data Protection Directive

[44] 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) [2002] OJ L 201/37.

[45] See Centre for Intellectual Property and Information Law, 'Personal Data and Privacy in Telecommunications Directive 97/66/EC' <https://www.cipil.law.cam.ac.uk/resourceseuropean-travaux/personal-data-and-privacy-telecommunications-directive-9766ec> accessed 24 August 2020.

[46] 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) [2002] OJ L 201/37.

[47] Diego Naranjo, 'Data Protection Reform - Next Stop: E-Privacy Directive' (*EDRi*, 24 February 2016) <https://edri.org/data-protection-reform-next-stop-e-privacy-directive/> accessed 24 August 2020.

[48] See Information Commissioner's Office, 'What Are PECR?' (20 July 2020) <https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/> accessed 24 August 2020.

(95/46/EC), the e-Privacy Directive is regarded as uncertain in many ways. This uncertainty exists because the e-Privacy Directive, different from the Data Protection Directive (95/46/EC), does not have specific provisions which expressly provides its geographical scope of application.[49]

The e-Privacy Directive concerns the processing of personal data and the protection of privacy in the electronic communications sector, and addresses the use of cookies, which was an important inclusion. The provisions provided under the Directive are significant for users to be able to trust in the electronic communications services and technologies they regularly use.

- **The introduction of the Cookie Directive numbered 2009/136 and the reasons behind its failure**

The e-Privacy Directive, in its original Article 5(3) allowed cookies to be set on the end-user's terminal device on the basis of an "informed opt-out".[50] In other words, it allowed cookies to be set on the condition that the end-users were clearly and fully informed and were presented with an option to refuse the setting of cookies. Moreover, Recital 25 of the Directive stated that it was possible to present the end-user with an option to opt-out only once and the choice they make would cover subsequent processing. Unfortunately, this method did not prove effective[51] as the users were being provided only with a link to privacy policies, and as is well-established now, users tend not to read privacy policies, due to inertia as well as the transactions costs for the users arising from the extreme length, difficulty to read and complexity of the privacy policies.[52] Behavioural sciences have established that individuals do not necessarily behave in a rational, expected way all the time, and default options have a strong impact on their choices.[53] With the

[49] See Phil Lee, 'The E-Privacy Directive - When and How Does It Apply Exactly?' (*Fieldfisher*, 11 August 2011) <https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/the-e-privacy-directive-when-and-how-does-it-apply-exactly> accessed 24 August 2020.
[50] Lilian Edwards, 'Data Protection and E-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling', *Law, Policy and the Internet* (1st edn, Hart Publishing 2019) 128.
[51] ibid 128–129.
[52] Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 I/S: A Journal of Law and Policy for the Information Society 543.
[53] F Zuiderveen Borgesius, *Behavioural Sciences and the Regulation of Privacy on the Internet* (Oxford Hart 2015) 17–20 <https://dare.uva.nl/search?identifier=b0052c52-9815-4782-b4b0-b1cabb3624d0> accessed 11 January 2019; Lauren E Willis, 'Why Not Privacy by Default?' (2014) 29 Berkeley Technology Law Journal 61.

addition of the use of dark patterns and nudging, it can be quite difficult for the users to escape the regular cookie consent trap.[54]

After the failure of the e-Privacy Directive to provide better choice to consumers with regard to cookies and online tracking, the Directive (EU) 2009/136[55] (the Cookie Directive) entered the picture, followed by much lively debate,[56] not dissimilar to the current situation concerning the draft e-Privacy Regulation. The Cookie Directive introduced an informed opt-in for the end-users, instead of the previous informed opt-out. According to Article 5(3) of the e-Privacy Directive, as amended by the Cookie Directive, the end-user should give *"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"*. An exception followed this provision, allowing for the storage or access to the electronic communications data *"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*" (Article 5(3)). However, many websites did not follow the informed opt-in consent requirement of the amended Directive and merely provided banners stating that the user would be deemed to have consented to the cookies if they continued to browse the website.[57] Following this, in order to provide clarification and improve the situation in practice, Recital 66 of the Directive was amended again. Accordingly, the choice regarding the cookies could now be made through browser settings. Edwards states that this still did not solve the problem as the inactivity by users and the fact they did not change the default settings was

[54] Norwegian Consumer Council, 'Deceived By Design' (2018) <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> accessed 2 April 2019; See also Matt Burgess, 'We Need to Fix GDPR's Biggest Failure: Broken Cookie Notices' [2020] *Wired UK* <https://www.wired.co.uk/article/gdpr-cookie-consent-eprivacy> accessed 1 July 2020; and Harry Brignull, 'What Are Dark Patterns?' (2018) <https://darkpatterns.org> accessed 20 August 2020.

[55] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 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 (Text with EEA relevance) [2009] OJ L 337/11 (The Cookie Directive).

[56] Edwards, 'Data Protection and E-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' (n 50) 129.

[57] ibid.

considered to constitute consent. The proliferation of tracking/cookie walls did not help the situation either.[58]

Aside from the failure of the amendments brought by the Cookie Directive to relieve the problems faced with regard to consent, the e-Privacy Directive also failed to keep up with the new technologies developed since its entry into force, such as IoT technologies, Over-the-Top (OTT) communications services and the ever more complex online tracking/advertising mechanisms. The e-Privacy Regulation aims to find effective solutions for these new technologies such as machine to machine communications, IoT, OTT services and new tracking methods employed in online advertising. The draft Regulation has the ultimate goal of achieving better harmonisation between the e-Privacy legislation and the GDPR, and therefore, aims to provide better and more efficient protection for the privacy of electronic communications.[59]

- **The Draft e-Privacy Regulation (the new Proposal for the e-Privacy Regulation)**

The proposal for the e-Privacy Regulation was first adopted by the Commission on 10 January 2017. The European Data Protection Supervisor (EDPS) and the European Economic and Social Committee provided their opinions on the proposed text respectively on 24 April 2017 and 5 July 2017. The report prepared by the Civil Liberties Committee (LIBE) on the draft Regulation was adopted by the European Parliament later in October 2017.

As mentioned above, the e-Privacy Regulation was supposed to come into force alongside the GDPR in May 2018. However, since the adoption of the draft Regulation by the European Parliament in October 2017, there has been much discussion and redrafting by the Council.

Overall, the Council has presented various approaches towards the draft Regulation under rotating presidencies (chronologically Austrian, Romanian, Finnish, Croatian to be followed by the German Presidency in July 2020). For instance, the Austrian Presidency introduced a more flexible

[58] ibid 130; Regarding the exceptions to cookie consent under the amended e-Privacy Directive, see Article 29 Data Protection Working Party, 'Opinion 04/2012 on Cookie Consent Exemption (WP 194)' (2012) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf> accessed 24 August 2020; Information Commissioner's Office, 'Guidance on the Use of Cookies and Similar Technologies' (20 July 2020) <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/> accessed 24 August 2020.
[59] Recital 6 of the e-Privacy Regulation.

approach, especially regarding cookies, privacy by default and metadata relating to electronic communications services, which raised concern among various stakeholders. In this context, the EDPB published its opinion on the interplay between the e-Privacy Regulation and the GDPR, urging the Council not to lower the high standards of protection of fundamental rights provided under the GDPR. Since then, throughout the presidencies of Romania, Finland and Croatia, a compromise or an agreement have not been reached, which is not unexpected in light of the stark contrast between the approach favouring more flexibility and the concerns raised by some MSs, the EDPB, civil society and academia.[60]

The draft proposal of the e-Privacy Regulation has been subject to many substantial changes; however, none of the proposed changes have led to a compromise or an agreement. The constant debate culminated in the rejection of the draft Regulation proposed by the Finnish Presidency on 22 November 2019 by the Permanent Representatives Committee of the Council of the EU (COREPER).[61] Following the rejection of the Finnish proposal, the Croatian Presidency proposed a new version of the draft Regulation on 21 February 2020, which was later discussed by the Council Working Party on Telecommunications and Information Society (WP TELE) in March 2020. As will be explained below, the most notable contribution of the Croatian Presidency has been the introduction of legitimate interests as a legal ground to process electronic communications data. Nevertheless, this draft did not lead to an agreement either.[62]

---

[60] 'Legislative Train Schedule - Connected Digital Single Market - Proposal for a Regulation on Privacy and Electronic Communications' (*European Parliament*) <https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform> accessed 24 August 2020; Council 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) - Progress Report (8204/20)' <https://data.consilium.europa.eu/doc/document/ST-9351-2019-INIT/en/pdf> accessed 24 August 2020.

[61] EDRi, 'EPrivacy: EU Member States Push Crucial Reform on Privacy Norms Close to a Dead End' (*EDRi*, 22 November 2019) <https://edri.org/eprivacy-eu-member-states-push-crucial-reform-on-privacy-norms-close-to-a-dead-end/> accessed 24 August 2020; Ella Jakubowska, 'EPrivacy Hangs in the Balance, but It's Not over yet...' (*EDRi*, 20 November 2019) <https://edri.org/eprivacy-hangs-in-the-balance-but-its-not-over-yet/> accessed 24 August 2020; 'EU States Vote on EPrivacy Reform: We Were Promised More Privacy. Instead, We Are Getting a Surveillance Toolkit.' (*Access Now*, 22 November 2019) <https://www.accessnow.org/eu-states-vote-on-eprivacy-reform-we-were-promised-more-privacy-instead-we-are-getting-a-surveillance-toolkit/> accessed 24 August 2020.

[62] 'Legislative Train Schedule - Civil Liberties, Justice and Home Affairs - LIBE - Proposal for a Regulation on Privacy and Electronic Communications' (*European Parliament*) <https://www.europarl.europa.eu/legislative-train/theme-civil-liberties-justice-and-home-affairs-libe/file-jd-e-privacy-reform> accessed 24 August 2020.

The Croatian Presidency has reached the end of its mandate in June 2020 and the German Presidency has taken over on the 1st of July to stay until the end of 2020. It is not clear what their attitude will be towards the draft Regulation; however, according to a promising report by Kayali of PoliticoEurope, the German Presidency seems to be aiming "for a political agreement on #ePrivacy by December".[63]

The German Presidency's agenda was published on 30 June 2020.[64] Accordingly, German Presidency seeks to adopt a "general approach" and an agreement by December 2020, by following two general principles, namely, protecting the privacy of electronic communications according to the Charter of Fundamental Rights and "*[ensuring] the preservation and advancement of innovative business models in the digital world*" with providing support for European SMEs and start-ups in the face of global competition.[65]

On 6 July 2020, in its Proposal, the German Presidency underscored their willingness to discuss various topics during its mandate.[66] Firstly, the Presidency stressed that, taking the COVID-19 pandemic into account, there is need to consider "*whether provisions on the permission to process electronic communications metadata for the protection of vital interests as set out in the latest compromise text 6543/20 are still supported by Member States, or whether further alignment to the GDPR is needed*".[67] Secondly, Article 6b(1)(e) and Article 6b(2) – 'legitimate interest'/'statistical counting' - were brought under spotlight by pointing out that as a general principle, to be able to achieve legal clarity, processing of electronic communications data shall be based on a clear and unequivocal objective for as long as it is undertaken without obtaining the

---

[63] Laura Kayali, 'Laura Kayali on Twitter' (*Twitter*, 16 June 2020) <https://twitter.com/LauKaya/status/1272940587893821440> accessed 24 August 2020.

[64] Council of the European Union, 'Draft Agendas for Council Meetings, during the Second Semester of 2020 (the German Presidency) (9250/20)' <https://data.consilium.europa.eu/doc/document/ST-9250-2020-INIT/en/pdf> accessed 24 August 2020.

[65] Council 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) - Presidency Discussion Paper (9243/20)' 2 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9243_2020_INIT&from=EN> accessed 24 August 2020.

[66] Council 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) - Presidency Discussion Paper (9243/20)' (n 65).

[67] ibid 2.

consent of the end-user. In addition Article 8 - legitimate interest and security of the end-user's device and Article 6d – 'detection of child abuse imagery' were stressed by underscoring the need to further discussion on these topics and that the options provided under this Proposal[68] needs careful consideration. The Presidency further made a call for MSs by asking "*with regard to the other provisions and recitals of the Regulation, for example Article 2 and the related recital 8aa or Article 6c, to indicate where they see a need for further discussion in order to clear the way for a General Approach*".[69]

This bewildering and long-lasting legislative process has still not reached to an end. There are still issues that require further clarification and challenges that call for agreement. Further improvements with regards to reaching an agreement is expected by the end of 2020.[70]

B. Challenges faced: a summary of the current debates surrounding the draft e-Privacy Regulation

One of the main concerns among the actors of the online data economy is the complexity of rules in the context of online advertising in the latest Proposal. The actors of the sector place the emphasis on the need for clear rules in online advertising and not putting the burden on stakeholders' shoulders in trying to figure out how to implement such rules into practice. The strong lobbying by the actors in the sector of online advertising and publishing, such as Google, Facebook and Axel Springer, is one of the reasons, among many others, why the e-Privacy Regulation is still on hold.[71] Moreover, varying opinions and suggestions with regards to the upcoming e-Privacy Regulation do not only come from the corporations. Various stakeholders find

[68] Council 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) - Presidency Discussion Paper (9243/20)' (n 65).
[69] ibid 7.
[70] ibid.
[71] Chloé Berthélémy, 'Captured States - e-Privacy Regulation Victim of a "Lobby Onslaught"' (*EDRi*, 23 May 2019) <https://edri.org/coe-eprivacy-regulation-victim-of-lobby-onslaught/> accessed 24 August 2020; Corporate Europe Observatory, 'Shutting down EPrivacy: Lobby Bandwagon Targets Council' (4 June 2018) <https://corporateeurope.org/en/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targets-council> accessed 24 August 2020; for a more detailed look at the impact of corporate lobbying on the EU, see Vicky Cann and Belén Balanyá, 'Captured States: When EU Governments Are a Channel for Corporate Interests' (Corporate Europe Observatory (CEO) 2019) <https://corporateeurope.org/sites/default/files/ceo-captured-states-final_0.pdf> accessed 24 August 2020.

the latest proposal bewildering and suggestions to legislators are made towards taking into account the lessons learnt from the GDPR.[72] According to Massé, global data protection lead of the digital rights NGO Access Now, commercial and law enforcement access to data needs to be separated.[73] Ustaran opines that the e-Privacy proposal had an ineffective approach to promote innovation while ensuring that users' privacy is protected.[74] Similarly, a report on the draft e-Privacy Regulation criticizes the Regulation on the basis that it lacks the flexibility and the risk-based approach provided under the GDPR, as it limits the legal grounds for processing.[75] Though it should be noted that the report was prepared on the basis of the text proposed during the Finnish Presidency (doc. 14054/19), meaning that it does not refer to the inclusion of legitimate interest as a legal ground, which was brought about by the Croatian Presidency in 2020. Although it is also highly debated, the introduction of the legitimate interest may alleviate these concerns.

On the other hand, publisher groups including Digital Content Next (DCN) support the draft e-Privacy Regulation on the grounds that it will help weaken the duopoly of Facebook and Google on the online advertising markets and strengthen the position of consumers as well as publishers in the long term.[76]

Some of the most significant debates regarding the e-Privacy Regulation so far focus specifically on the cookie consent mechanisms and tracking/cookie walls, whether forced consent and tracking/cookie walls shall be banned, Do-Not-Track Signals, micro-targeting and RTB, new provisions regarding metadata, including location data, introduction of legitimate interests as a ground for processing of electronic communications data, both including content and metadata. These debates will be addressed below, in Section II of this Report.

---

[72] Jasper Juinen, 'EU May Overhaul EPrivacy Plan After Nations Criticize It' (3 December 2019) <https://news.bloomberglaw.com/privacy-and-data-security/eu-may-overhaul-eprivacy-plan-after-nations-criticize-it> accessed 24 August 2020.

[73] ibid.

[74] ibid.

[75] Hogan Lovells, 'Study of Proposal for an E-Privacy Regulation' (2019) <https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2019/2019_11_25_study_eprivacy_regulation.pdf?la=en> accessed 24 August 2020.

[76] Jack Marshall, Interview with Jason Kint, 'GDPR Is "a Significant Risk to Facebook and Google": A Digiday+ Slack Town Hall with DCN's Jason Kint' (19 April 2018) <https://digiday.com/media/gdpr-significant-risk-facebook-google-digiday-slack-town-hall-dcns-jason-kint/> accessed 24 August 2020.

It is also important to note that usage of online tracking technologies that are used in the advertising ecosystem have serious legal implications which show to have the potential to undermine individuals' fundamental rights and freedoms. Castello argues that the ad tech industry has considerably undermined individuals' rights and freedoms and that their practices pose a threat for users' individual autonomy while having serious detrimental implications for rule of law.[77] He also underscores that the existing laws are insufficient to protect users' right to privacy and to provide adequate safeguards for rule of law,[78] which is one of the bedrock principles of constitutional law and is crucial for advancing democracy and protecting fundamental rights and freedoms.[79] Moreover, in the context of affinity profiling[80] and online behavioural advertising, there are challenges related to privacy, and non-discrimination, as well as group level protection.[81] Unfortunately, the current legal framework both in the EU[82] nor in Turkey do not adequately address these challenges and fail to provide adequate protection to protect individuals' right to privacy. A thorough analysis of the reasons why the current legal framework is not sufficient to protect individuals' rights, prevent discrimination, and ensure protection for individuals' autonomy as well as the rule of law in a democratic society will be discussed in detail in PART II of this Report.

[77] Róisín Áine Costello, 'The Impacts of AdTech on Privacy Rights and the Rule of Law' [2020] Technology and Regulation 11.
[78] ibid.
[79] See for example Massimo Tommasoli, 'Rule of Law and Democracy: Addressing the Gap Between Policies and Practices' (*United Nations UN Chronicle*) <https://www.un.org/en/chronicle/article/rule-law-and-democracy-addressing-gap-between-policies-and-practices> accessed 24 August 2020; and Sumit Bisarya and W Elliot Bulmer, 'Rule of Law, Democracy and Human Rights: The Paramountcy of Moderation' in Anne Meuwese, Ernst Hirsch Ballin and Maurice Adams (eds), *Constitutionalism and the Rule of Law: Bridging Idealism and Realism* (Cambridge University Press 2017) <https://www.cambridge.org/core/books/constitutionalism-and-the-rule-of-law/rule-of-law-democracy-and-human-rights-the-paramountcy-of-moderation/A0519089C517185986BC2165F622CF0F> accessed 24 August 2020.
[80] 'Affinity profiling - grouping people according to their assumed interests rather than solely their personal traits - has become commonplace in the online advertising industry.' See Sandra Wachter, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising' (Social Science Research Network 2019) SSRN Scholarly Paper ID 3388639 1 <https://papers.ssrn.com/abstract=3388639> accessed 9 October 2019.
[81] Wachter (n 80).
[82] ibid 1, 12–13.

C. Turkey's approach towards e-Privacy

i. Legislative History and the Current Regulatory Framework

In Turkey, the Information Technologies and Communication Authority ("ICTA") has been the responsible authority for e-Privacy since 2004. The ICTA transposed the e-Privacy Directive into national law in 2004 and published a bylaw called the Regulation on the Processing of Personal Data and the Protection of Privacy in the Telecommunication Sector,[83] which included provisions regarding, *inter alia*, notification requirements in the event of a security breach, privacy of telecommunications and conditions for processing traffic and location data.

In 2008, the Electronic Communications Code (ECC)[84] entered into force. This Code originally authorized ICTA to determine the procedures and principles regarding processing of personal data and privacy protection for activities concerning the electronic communications sector under Article 51. In 2012, using the authority given to it by Article 51 of the ECC, to replace the previous regulation of 2004 ICTA enacted a new regulation, namely the Regulation Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communication Sector[85] (the 2012 Regulation), which was in line with the e-Privacy Directive (as amended by Directive 2009/136/EC).

However, in 2014, the 2012 Regulation lost its legal footing after the Constitutional Court annulled Article 51 of the ECC,[86] based on Article 20(3) and Article 13 of the Turkish Constitution. According to Article 13, "fundamental rights and freedoms may be restricted only by law and in conformity with the reasons mentioned in the relevant articles of the Constitution without infringing upon their essence".[87] Pursuant to Article 20(3), data protection is one of the fundamental rights and personal data can be processed only in cases envisaged by law.

---

[83] The Regulation on the Processing of Personal Data and the Protection of Privacy in the Telecommunication Sector, published in the Official Gazette dated 6 February 2004, numbered 25365.

[84] Electronic Communications Code dated 5 November 2008, numbered 5809, published in the Official Gazette dated 10 November 2008, numbered 27050 (ECC).

[85] Regulation Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communication Sector, published in the Official Gazette dated 24 July 2012, numbered 28363 (the 2012 Regulation).

[86] *Constitutional Court judgment of 9 April 2014, numbered E 2013/122 and K 2014/74, published in the Official Gazette dated 26 July 2014 and numbered 29072*.

[87] The Constitutional Court of the Republic of Turkey, 'Translation of the Turkish Constitution' <https://www.anayasa.gov.tr/en/legislation/turkish-constiution/> accessed 18 September 2020.

After the Constitutional Court's decision to annul Article 51 of the ECC, ICTA replaced Article 51 with a new provision with the Law No. 6639 Amending Some Laws and Decree Laws.[88] Compared to the older version, the new Article 51 includes more detailed provisions regarding the protection of personal data and privacy in electronic communications.

Pursuant to the current Article 51(1) of the ECC No. 5809, the Authority is entitled to determine the procedures and principles towards the processing of personal data and the protection of its privacy regarding the electronic communications sector.[89] Article 51(7) of the ECC provides further important details regarding the limitation of the processing of traffic data. It also needs to be noted that the Constitutional Court rendered a relevant judgment regarding traffic data in 2014[90] and found unlawful the indiscriminate and unrestrained collection, retention and sharing of traffic data by the Telecommunications Communication Presidency (TİB) with other authorities upon court decisions.[91]

While Article 51 of the ECC No. 5809 has a significant importance in the regulation of electronic communications, it is not consistent with the Turkish data protection regulatory framework, since it was enacted long before the current data protection laws. Therefore, there is a growing need for a new e-Privacy Regulation in Turkey, to resolve the discrepancies between Article 51 of the ECC and the rest of data protection laws.

ii. The new e-Privacy Regulation Draft published by ICTA

Based on Article 51 of the e-Communication Law, the ICTA prepared a draft Regulation in collaboration with all related stakeholders. However, taking into consideration new developments and discussions on the draft e-Privacy Regulation in the EU, the ICTA did not publish the new regulation and preferred to observe the situation in the EU.

---

[88] Law no. 6639 Amending Some Laws and Decree Laws, dated 27 March 2015, published in the Official Gazette dated 15 April 2015, numbered 29327.
[89] Electronic Communications Code dated 5 November 2008, numbered 5809, published in the Official Gazette dated 10 November 2008, numbered 27050.
[90] *Constitutional Court Judgment of 2 October 2014, numbered E 2011/149 and K 2014/151, published in the Official Gazette dated 1 January 2015, numbered 29223*.
[91] Elif Küzeci, *Kişisel Verilerin Korunması* (4th edn, Oniki Levha Yayıncılık 2020) 525–526.

The latest published version of the new e-Privacy Regulation drafted by ICTA for public consultation aims was published on 17 March 2020 .[92] As opposed to the current provision under the ECC, the scope of ICTA's draft e-Privacy Regulation does not specifically address personal data but simply refers to "data", which is defined as "traffic data, location data, subscriber/user identity and other related information".

The definition of traffic data as well as of location data under the Turkish e-Privacy Regulation draft (Article 4(1)(ı) and 4(1)(l)) follows the definition of traffic and location data provided under the e-Privacy Directive (Article 2(b) and 2(c)), with a small difference regarding the definition of location data: the Turkish version specifies location information as data sent from end-users' terminal device with the help of satellite navigation systems. The e-Privacy Directive can be understood to cover this type of location data as well, thanks to the definition under Article 2(c).

According to Article 5(1) of ICTA's draft regulation, operators are required to prepare a security policy regarding the processing of personal data, in line with the principles stipulated in Article 51 of the ECC No. 5809. They also need to provide technical and organizational measures in line with national and international standards to protect the personal data they hold and the services they provide, to answer all types of risks, within the bounds of technical possibilities.

Article 5(3) of the draft regulation provides for a data retention requirement. Accordingly, "process records documenting access to personal data and other related systems"[93] shall be time-stamped and kept for a time of two years.

The draft regulation goes on to state in its Article 5(4) that the operator shall ensure the privacy, security, completeness, accessibility of the data it processes, and also comply with the purpose limitation principle. The third parties th.at the operator authorizes are also required to comply with

[92] Information and Communication Technologies Authority, 'Public Consultation Regarding the Draft Regulation on the Processing of Personal Data and Protection of Privacy in the Electronic Communications Sector' <https://www.btk.gov.tr/uploads/boarddecisions/kamuoyu-gorusu-alinmasi-elektronik-haberlesme-sektorunde-kisisel-verilerin-islenmesi-ve-gizliligin-korunmasina-iliskin-yonetmelik/77-2020-web.pdf> accessed 18 September 2020; BTS & Partners, 'ICTA Launches A Public Consultation On The Draft EPrivacy Regulation' (18 May 2020) <https://www.bts-legal.com/publication-detail/ICTA%20Launches%20A%20Public%20Consultation%20On%20The%20Draft%20ePrivacy%20Regulation > accessed 24 August 2020.

[93] BTS & Partners (n 92).

these requirements. This is in line with the provisions of the Turkish data protection law, which stipulates joint liability for data controllers and data processors regarding data security.

One noteworthy point in the draft Regulation is that the wording used in the law has changed and all the provisions that include consent are replaced with 'explicit consent'. In addition, the conditions for obtaining a valid consent are provided under Article 7. The conditions in question are in parallel with the definitive conditions for explicit consent under the Law No. 6698: *"(i) provided for a specific subject, (ii) provided upon being adequately informed, (iii) freely given, and thus, adopt an equivalent protection regime for subscribers/users".*[94] In line with these conditions under the Law No. 6698, the draft Regulation stipulates that explicit consent shall be obtained in advance of the processing activity and for a specific subject (Article 7(1)(a)), the subscriber/user shall be adequately informed, the subscriber/user shall not be forced to provide consent, in other words, consent shall be freely given. Moreover, Article 7 stipulates that the provision of basic electronic communications services or products shall not be made conditional on the explicit consent of the subscriber/user. (Article 7(1)(b)).

The operators are required to provide information on "*(i) the types of personal data and the types of traffic and location data to be processed, (ii) the scope of processing, (iii) the purpose of processing, and (iv) the period of processing, in a clear and comprehensible manner*"[95] before obtaining explicit consent (Article 7(1)(c)). Moreover, the draft Regulation introduces requirements for the consent to be deemed explicit: for instance, if to be provided in writing, such information shall be at least 12 points size (Article 7(1)(c)). Moreover, when obtaining the explicit consent through electronic media, the statement of consent is required to be time-stamped (Article 7(1)(ç)).

It is important to underscore that the draft Regulation introduces a distinct scheme for personal data transfers to third parties (excluding data transfers to public bodies to which data transfers are allowed under the Law). Under Article 7(1)(d), operators are required to ensure that they give information on "(i) the scope of data to be transferred, (ii) the name and address of the recipient entity, (iii) purpose and period of transfer and (iv) how data will be destructed by the end of the

[94] ibid.
[95] BTS & Partners (n 92).

period, before obtaining explicit consent for such transfer". The article in question adds a further requirement for operators in cases where a change occurs in the above-given information. In such circumstances, operators are required to obtain explicit consent for the transfer.

According to Article 7(1)(e) of the draft Regulation, when the data is transferred to third parties, it shall be processed only by the third parties which are included in the information that is provided to the subscriber/user when obtaining their explicit consent. This requirement may be interpreted as a restriction according to which the third parties that the data is transferred to cannot use sub-processors.[96]

In terms of obligation to inform concerning traffic and location data, Article 8 of the draft Regulation provides that operators need to ensure that their obligation to inform is complied with, in cases where traffic and location data are processed for the purposes aimed under the relevant legislation or case law, which as a result, do not require obtaining 'explicit consent'. Accordingly, in such circumstances, the draft Regulation sets out obligations for operators to ensure that general information is provided to subscribers/users on "*(i) the types of traffic and location data to be processed, (ii) purposes, (iii) period, and (iv) methods for processing*".[97]

The current Regulation has a strict approach regarding data localization, and it prohibits cross-border transfers. Yet, as it can be concluded from Article 7(1)(d) of the draft Regulation, it shall be possible to transfer personal data to third parties even if they are not in Turkey upon obtaining explicit consent, as long as the subscribers/recipients are informed regarding "*(i) the country to which data will be transferred, (ii) the purpose and period for retention abroad, (iii) the corresponding legislation and practice in the recipient country*".[98] It is noteworthy to state that the draft Regulation does not refer to the cross-border transfer regime provided under the Law No. 6698.

Furthermore, additional rights and protections are provided for subscribers. According to Article 13(1) of ICTA's Draft Regulation, operators are required to provide information regarding how explicit consent can be withdrawn, and to make sure that withdrawing consent is made equally

[96] ibid.
[97] ibid.
[98] ibid.

easy with giving it. Article 13(2) further sets out that, on a yearly basis, operators are required to provide information to subscribers/users whose personal data are processed. The Article adds that personal data processing cannot continue unless the said information is provided to the subscriber/user in a standardized manner.

Section II: Location tracking and online identifiers under the draft e-Privacy Regulation: A deep dive into the current approach in the EU

This Section aims to provide an overview of the online tracking technologies and briefly address their legal implications. It first starts with providing a summary of online tracking technologies and briefly explains how online tracking occurs. To do this, the below sub-sections delve into different topics such as first party and third-party tracking, RTB and micro-targeting, alternatives and contextual advertising, analytics, and mobile privacy. After providing a general overview of the online tracking technologies, this Section moves on to location tracking and underscores important issues and debates that rotate around the e-Privacy laws.

A - Online Tracking Technologies

Tracking involves "the targeting and retargeting of users through the use of cookies for advertising purposes".[99] Online tracking can occur in different ways. Websites, apps, and smart devices include trackers for carrying out data processing activities. Firstly, apps, websites or smart devices including but not limited to mobile phones, tablets, and smart TVs[100] collect data themselves. Secondly, the data collection can be carried out on behalf of the third parties. As a result of these tracking and data collection practices, very granular data can be collected in great amounts, about individuals who browse the web or use an app on their mobile devices. This data can then reveal very private or personal details about the lives, personalities, and preferences of these individuals

[99] CMS, 'Tracking under the EPrivacy Regulation' <https://cms.law/en/deu/insight/e-privacy/tracking-under-the-e-privacy-regulation> accessed 24 August 2020.
[100] Ayça Atabey and Leyla Keser Berber, 'Addressable TV and Consent Sequencing' (2020) 1 Global Privacy Law Review <https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/1.1/GPLR2020004> accessed 21 September 2020.

and as a result can be used to manipulate or influence them.[101] Therefore it is crucial to address these tracking practices.

Browsing the internet involves a two-sided communication between the user's computer and the website they are viewing. It is not only the user's computer who requests information about the website they are looking to visit, but the website also requests information about who visits them. The material that is communicated during this exchange is not limited to what the user views on their screen, but also includes background information about the user. For instance, information about the user's browser settings is sent to the website to enable the website display its content in a manner that is suitable to the user's browser and for the user to have a better browsing experience. Websites receiving information about the user and about their behaviour online is what we call, in its most basic form, "online tracking".

In online tracking, some examples of data that are collected are "data that enables users to log in into the web service for authentication and customization purposes, IP addresses, user identifiers, timestamps, URLs of the visited pages and other parameters that enable the user to be singled-out"[102] and cookies. Are they personal data? It seems like, at a first glance, that such information may not be capable of pointing out to an individual person. However, the GDPR's definition of personal data is wider than data that can directly point to an individual person. According to the GDPR, personal data is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4(1) of the GDPR).

---

[101] See Privacy International, 'I Asked an Online Tracking Company for All of My Data and Here's What I Found' (*Privacy International*, 7 November 2018) <http://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found> accessed 16 September 2020. For an example where data obtained from online advertising was used to influence the parliamentary elections in Poland in 2019, through specifically targeting LGBTQ+ individuals, see Johnny Ryan, 'Submission to Irish Data Protection Commissioner' 5 <https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2020/09/JohnnyRyanDocumnet.pdf> accessed 22 September 2020 This is one of many examples showing that data obtained in online advertising ecosystem is not fully anonymised and can be used to target specific individuals.

[102] 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' 9 <https://hal.inria.fr/hal-02875447/document> accessed 24 August 2020.

Moreover, the purpose of data processing[103] does not matter. As long as the data can identify the users, in other words "when identification of users is likely",[104] it is personal data. It does not matter "whether they are meant or used to track the online activity of such users".[105]

In this sense, an e-mail address consisting of the name and surname of a person would be an example of where the related individual can be directly identified. On the other hand, a unique cookie identifier or an IP address would be examples of data where the individual is indirectly identifiable.

Even though the bits of data collected in online tracking may not be capable of directly identifying an individual, they can easily be combined with other information to identify or single-out individuals, to target them and to create their profiles. The ease of combination with other data can be seen more clearly when the extremely wide scope of online tracking is considered. As a result, in light of the GDPR's definition of personal data, the data that is processed within the scope of online tracking methods explained here are, in most cases, personal data.

Recital 30 of the GDPR clarifies this point:

> "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them".[106]

Additionally, data from other sources and insights that are inferred about the individual are also personal data collected within the scope of online tracking activities as long as they can be linked to the individual.

---

[103] The term "processing" is used throughout the report in the meaning that is conferred to it under the GDPR, which is: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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;" according to Article 4(2) of the GDPR.

[104] Santos, Bielova and Matte (n 102) 9.

[105] ibid.

[106] Recital 30 of the GDPR.

Online tracking practices need to comply with the e-Privacy Directive. However, when personal data is concerned, GDPR is also applicable. Therefore, the data processing practices where personal data is processed shall comply with both the GDPR and the e-Privacy Directive. The specific requirements of the GDPR and the e-Privacy Directive will be explained below, after explaining the cookies more in detail.

i. Cookies

Within the context of online tracking, websites send small text files named "cookies" that allow them to store information on the user's computer, describing the user and their browser to them so that the website can recognise the user next time they visit it.[107] There are numerous types of cookies such as session cookies, persistent cookies, flash cookies, and zombie cookies etc. Session cookies are cookies that store information which the data subject (user) has put in and such cookies "track the movements of the user within the website".[108] A session cookie which is also known as a transient cookie contains information that is stored in a temporary memory location and then subsequently deleted after the session is completed or the web browser is closed.[109] This cookie stores information that the user has input and tracks the movements of the user within the website. If a cookie does not contain an expiration date, it is considered a session cookie and when the browser session ends, the cookie is permanently lost from this point on.[110] If the cookie contains an expiration date, then, it is a persistent cookie. The session cookies are never stored in a disk and are rather in-memory cookies while for persistent cookies, on the date specified in the expiration, the cookie will be removed from the disk.[111] Another type is flash cookies, which is a local shared

[107] See also *Follow the Cookie Trail - Computerphile* (2013) <https://www.youtube.com/watch?v=LHSSY8QNvew> accessed 24 August 2020; and *EXTRA BITS - Follow the Cookie Trail - Computerphile* (2013) <https://www.youtube.com/watch?v=_d0G6FZ_kR4> accessed 24 August 2020.

[108] 'What Is Session Cookie? - Definition from Techopedia' (*Techopedia.com*) <http://www.techopedia.com/definition/4910/session-cookie> accessed 24 August 2020; See also Data Protection Commission, 'Guidance Note: Cookies and Other Tracking Technologies' (2020) <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf> accessed 24 August 2020.

[109] See Data Protection Commission (n 108).

[110] 'What Are Cookies? What Are the Differences between Them (Session vs. Persistent)?' (*Cisco*, 17 July 2018) <https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117925-technote-csc-00.html> accessed 24 August 2020.

[111] ibid.

object and is a data file that can be created on a user's computer by the sites the user visits.[112] These are usually used to enhance users' browser experience. Zombie cookies occur when third-party cookies are placed outside of a user's web browser's designated cookie storage; moreover, third-party cookies and flash cookies may work together to create zombie cookies.[113]

Web tracking based on cookies remains an important problem for the privacy of Web users. Even after the GDPR's enactment, third party companies continue tracking users with various sophisticated techniques based on cookies without their consent. According to Fouad et al.'s study, 91.92% of websites incorporate at least one type of cookie-based tracking.[114]

The legal framework concerning cookies, specifically the cookie banners on websites

As explained above, cookies function via storing and accessing small text files on the computer or other electronic device of an end-user. This is regulated under Article 5(3) of the e-Privacy Directive, according to which

> "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 any technical storage or access for the

[112] 'How to Delete Flash Cookies, Permacookies, and Zombie Cookies' (*ReputationDefender*, 12 April 2018) <https://www.reputationdefender.com/blog/privacy/how-to-delete-flash-cookies-permacookies-and-zombie-cookies> accessed 24 August 2020.

[113] ibid.

[114] Imane Fouad and others, 'Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels' (2020) 2020 Proceedings on Privacy Enhancing Technologies 499. The submission by Johnny Ryan to Irish Data Protection Commissioner in September 2020 exemplifies such breaches of the GDPR which are still going on. For more information, see Ryan (n 101); Following an inquiry into the online advertising sector focusing on real time bidding, which will be addressed in this report, British data protection watchdog Information Commissioner's Office also published reports and raised concerns regarding the systematic breaches of the law in online advertising. For more information, see Information Commissioner's Office, Update Report into Adtech and Real Time Bidding (2019) <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf> accessed 22 September 2020; The Irish Data Protection Commissioner also found that many data controllers in online advertising were also in breach of the law. See Data Protection Commission, 'Report by the Data Protection Commission on the Use of Cookies and Other Tracking Technologies - Following a Sweep Conducted between August 2019 and December 2019 (Revised on 15 April 2020)' (2020) <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Data%20Protection%20Commission%20cookies%20sweep%20REVISED%2015%20April%202020%20v.01.pdf> accessed 22 September 2020.

> 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.".

Accordingly, there are three possible legal grounds to store or access a cookie on the end-user's device:

- either the consent of the end-user shall be obtained,
- the access or storage shall be undertaken for the sole purpose of carrying out the transmission of a communication over an electronic communications network: meaning that the transmission of the communication would not be possible without the access or storage, like in the case of a load-balancing cookie, [115]
- or the access or storage shall be "strictly necessary" to provide the service requested by the user or the subscriber.

Here, according to Art 29 WP, strictly necessary means that the service would not function without the access or storage.[116] Santos et al. explain this point as follows: "In this regard, the choice of a certain functionality that relies on [browser-based tracking technology] is not enough to justify the strict necessity if the web publisher has a different implementation choice that would work without a [browser-based tracking technology]".[117] In line with this narrow interpretation, according to both the Art29WP and DPAs, "'advertising, and use of the data for marketing, research and audience measurement' are not strictly necessary to deliver a service that is requested by a user"[118] and do require consent.

As for the standards that the consent shall comply with, Article 5(3) of the e-Privacy Directive refers to Directive 95/46/EC. After the entry into force of the GDPR, this reference to Directive

[115] Santos, Bielova and Matte (n 102) 11.
[116] Article 29 Data Protection Working Party, 'Opinion 04/2012 on Cookie Consent Exemption (WP 194)' (n 58) 3–4.
[117] Santos, Bielova and Matte (n 102) 11–12.
[118] Article 29 Data Protection Working Party, 'Opinion 03/2016 on the Evaluation and Review of the EPrivacy Directive (2002/58/EC) (WP 240)' (2016) <https://www.pdpjournals.com/docs/88612.pdf>; (as cited in Santos, Bielova and Matte [n 102] 12).

95/46/EC has been replaced with a reference to the GDPR (see Article 94(2) of the GDPR). Therefore, currently, cookie consent shall comply with the consent rules under the GDPR, listed under Article 4(11) and Article 7.

The Directive does not specify how that consent shall be obtained in practice, however, in practice, most of the websites use cookie banners. Whether these banners are compliant with the existing consent requirements under the GDPR, as well as with other binding and non-binding legal sources is an extremely important question. Although it seems like the answer to the consent requirements concerning the cookie banners should not be too complicated, this issue has been causing problems for some time.

- **Cookie Wars**

As explained above in Section I of this Report, the e-Privacy Directive has undergone some changes since it first came into force, in order to answer the problems regarding cookies faced in practice.

In its original version, before amendments, the e-Privacy Directive allowed cookies to be set on the end-user's terminal device on the basis of an "informed opt-out".[119] This meant that cookies could be set if the end-users were clearly and comprehensively informed and were also presented with an option to refuse the setting of cookies. Recital 25 of the Directive added to this; accordingly, it was possible to present the end-user with an option to opt-out only once and the choice they make would cover subsequent processing. However, this method failed to reach its goal of making users make an active choice regarding their cookie preferences[120] because first the users were being provided only with a link to privacy policies. Secondly, the users tend not to read privacy policies, due to widespread inertia as well as the transaction costs for the users arising from the extreme length, difficulty to read and complexity of the privacy policies.[121] Third reason for the failure can be the use of dark patterns and nudging. These are practices which make it much

[119] Edwards, 'Data Protection and E-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' (n 50) 128.
[120] ibid 128–129.
[121] McDonald and Cranor (n 52).

more difficult for the users to reject the setting of cookies on their devices and influence them, in a covert manner, to remain passive and not to select privacy-friendly options.[122]

In this context, the e-Privacy Directive had clearly failed to provide better choice to consumers for cookies and online tracking. As a result, the Directive (EU) 2009/136[123] (the Cookie Directive) entered the picture; however, at first it was not received well and was followed by extensive debate.[124] The Cookie Directive introduced an informed opt-in for the end-users, instead of the previous informed opt-out. According to the thus amended Article 5(3) of the e-Privacy Directive, the end-user shall give *"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"*. As explained above, an exception follows this provision, allowing for the storage or access to the electronic communications data *"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"* (Article 5(3)). The goal of this amendment was notable; yet, it failed significantly, as many websites did not follow the informed opt-in consent requirement. They merely provided banners stating that the user would be deemed to have consented to the cookies if they continued to browse the website.[125]

Following this failure, to provide clarification and improve the situation in practice, Recital 66 of the Directive was amended again and the choice regarding the cookies could now be made through browser settings. As stated by Edwards, this did not suffice to solve the problem, as the inactivity by users and instances where they did not change the default settings were considered to constitute

[122] Norwegian Consumer Council (n 54); See also Burgess (n 54); and Brignull (n 54).
[123] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 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 (Text with EEA relevance) [2009] OJ L 337/11 (the Cookie Directive).
[124] Edwards, 'Data Protection and E-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' (n 50) 129.
[125] ibid.

consent. The proliferation of tracking/cookie walls did not help the situation either,[126] which will be addressed under the following sub-heading.

Currently, while we are still waiting for the upcoming e-Privacy Regulation, cookie consent is regulated through the e-Privacy Directive. Though, due to clashing approaches adopted by various stakeholders, the situation in online tracking is still not as clear as it should have been. To help alleviate the situation, Art49WP, EDPB and European DPAs have since been publishing their own guidelines. For instance, ICO's position, which can be said to be somewhat unique as it is rather flexible compared to other DPAs, can be seen in the table below:

ICO's Guidance on Exceptions to Cookie Consent Requirements:[127]

Activities likely to fall within the exception	**Activities unlikely to fall within the exception**
A cookie used to remember the goods a user wishes to buy when they proceed to the checkout or add goods to their shopping basket	Cookies used for analytical purposes to count the number of unique visits to a website for example
Certain cookies providing security that is essential to comply with the security requirements of the seventh data protection principle for an activity the user has requested – for example, in connection with online banking services	First and third-party advertising cookies

[126] ibid 130; Regarding the exceptions to cookie consent under the amended e-Privacy Directive, see Article 29 Data Protection Working Party, 'Opinion 04/2012 on Cookie Consent Exemption (WP 194)' (n 58); Information Commissioner's Office, 'Guidance on the Use of Cookies and Similar Technologies' (n 58).

[127] Information Commissioner's Office, 'Guidance on the Use of Cookies and Similar Technologies' (n 58); (as cited in Edwards, 'Data Protection and E-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' [n 51] 132).

Some cookies help ensure that the content of your page loads quickly and effectively by disturbing the workload across various computers.	Cookies used to recognise a user when they return to a website so that the greeting they receive can be tailored.

Figure as cited in Edwards, 'Data Protection and E-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' [n 51] 132.

Recently, the CJEU clarified the issue of cookie consent in its Planet49 judgment[128], in line with previous guidance provided by supervisory authorities. Accordingly, the e-Privacy Directive was found to be applicable to all data stored on the end-user's terminal device, regardless of whether the data is personal data or not, as long as it enters the end-users' private sphere.[129] Moreover, pursuant to the e-Privacy Directive, pre-ticked boxes cannot be used to obtain valid consent from the end-users for tracking via cookies and other technologies such as browser fingerprinting or tracking pixels explained in the previous chapter.[130] Additionally, in the event there is a need to obtain consent from end-users pursuant to the e-Privacy Directive, the notion of consent shall be interpreted in light of the GDPR's definition of consent, as well as of the relevant recitals under the GDPR.[131]

In Planet49, the CJEU interpreted the notion of consent in the e-Privacy Directive according to the notion of consent under the GDPR. This is not surprising, considering the direct reference to the Directive 95/46/EC in the e-Privacy Directive; however, the CJEU's judgment is still important as it clarifies how the notion of consent provided under the GDPR shall be interpreted and applied when it comes to consent practices in online tracking.

The interpretation of consent in Planet49 applies not only to the e-Privacy Directive, but also to the e-Privacy Regulation, since the e-Privacy Regulation explicitly refers to the GDPR for consent

[128] Case C-673/17 *Planet49* ECLI:EU:C:2019:801 [2019].
[129] ibid 71.
[130] ibid 57, 63, 65.
[131] ibid 60–63; See also Osborne Clarke, 'Planet49: CJEU Rules on Consent Requirements for Cookies' (*Osborne Clarke*, 7 October 2019) <https://www.osborneclarke.com/insights/planet49-cjeu-rules-consent-requirements-cookies/> accessed 24 August 2020.

in Article 4 a of the current draft (consolidated text of the draft e-Privacy Regulation dated 6 March 2020). As a result, the notion of consent under the upcoming e-Privacy Regulation shall be interpreted pursuant to the notion of consent provided in Article 4(11) and Article 7 as well as the relevant recitals of the GDPR.

- **A Systematic Approach**

In light of the problems that the cookie banners have been causing in practice, the issue has been examined by Santos, Bielova and Matte in their article titled "Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners". Accordingly, after examining the binding legal sources, i.e. the GDPR, the e-Privacy Directive and the CJEU decisions, as well as the non-binding legal sources, ie the guidelines published by the EDPB and national DPAs, they determined that there are 22 requirements for obtaining valid consent for cookie banners. They divided these as high-level and low-level requirements. Accordingly, the requirements for consent to be deemed valid are depicted in the Table below, which is a simplified version of Santos, Matte and Bielova's contribution:[132]

Requirements	
High-Level Requirements	**Low-Level Requirements**
Prior	"R1 Prior to storing an identifier"
	"R2 Prior to sending an identifier"
Free	"R3 No merging into a contract"
	"R4 No tracking walls"
Specific	"R5 Separate consent per purpose"
Informed	"R6 Accessibility of information page"

[132] Santos, Bielova and Matte (n 102) 15.

	"R7 Necessary information on [browser-based tracking practices]"
	"R8 Information on consent banner configuration"
	"R9 Information on the data controller"
	"R10 Information on rights"
Unambiguous	"R11 Affirmative action design"
	"R12 Configurable banner"
	"R13 Balanced choice"
	"R14 Post-consent registration"
	"R15 Correct consent registration"
Readable and accessible	"R16 Distinguishable"
	"R17 Intelligible"
	"R18 Accessible"
	"R19 Clear and plain language"
	"R20 No consent wall"
Revocable	"R21 Possible to change in the future"
	"R22 Delete 'consent cookie' and communicate to third parties"

Simplified version of the figure cited in Santos, Bielova and Matte (n 102) 15.

It has to be noted that these requirements do not take into account certain aspects which are excluded from the scope of the assessment that Santos, Bielova and Matte conducted, for various reasons.[133] Namely, the study excludes the requirement of explicit consent, since a double-layer verification approach was needed which would require additional verification effort; the cases concerning unbalanced power in the assessment of freely given consent (Recital 43); whether the consent is informed in the sense that the meaning of the purposes presented in the cookie banners; consent expressed through browser settings; children's consent; and exceptions specified in the GDPR.[134]

The 22 requirements listed above, as clarified by Santos, Bielova and Matte, need to be complied with, in order for the consent to be lawfully obtained through cookie banners. Unfortunately, currently, many websites do not comply with these requirements and are therefore breaching the applicable legal framework.[135]

The esteemed work of Santos, Bielova and Matte is one of many, where great efforts are directed towards fixing the breaches of the law observed in the use of cookies in the online advertising sector. This work lists and examines very clearly the requirements under the existing legal framework, for the consent to be legally obtained through cookie banners. Although guidances explaining the substance of the law did not suffice to fix the violations of the legal framework until now, this is thought to be mainly due to inaction and lack of resources by national data protection authorities. Hopefully, systematic, granular and very clear pieces of work like this article of Santos, Bielova and Matte will be able to make an effective positive contribution.

ii. Other tracking methods

There are also methods other than cookies that enable online tracking, such as tracking pixels, browser fingerprinting, SDKs, and Canonical Name (CNAME) Cloaking. Tracking pixels are invisible images placed on a website, an app, or the body of an email that the user is viewing. When the user requests to view the page, the pixel, which is hosted on an external server, is also loaded. Loading the pixel means that the user's browser sends information about the user to the

[133] ibid 8.
[134] ibid.
[135] See, for example, Data Protection Commission (n 114); and Information Commissioner's Office (n 114).

external server where the pixel is stored. If the pixel is Facebook's tracking pixel, then the information about the user will be sent to Facebook. The information sent may include various types of information, such as the IP address of the users and the specific location that the users are looking at on the web page or the email they are viewing.

Browser fingerprinting refers to identification of the end-users on the basis of the unique combination of the settings of their browser, such as the language of the browser, the IP address, the operating system, the fonts that the user has installed on their operating system, screen resolution etc.[136] While these bits of information are not capable of pointing to the user on their own, their combination is usually unique so the users can be tracked across the web just on the basis of this "fingerprint" of their browser, without resorting to cookies or other tracking methods. The more unique the combination of the settings, the easier it becomes to identify a specific user who visits the website.[137]

Software Development Kits, or "SDKs" are tools used by software developers which allow them to develop apps for a specific platform or operating system. For example, to allow users to log into an app with their Facebook accounts, the developers use SDKs developed by Facebook. The SDKs, which are in many cases developed by someone other than the developer of the app, contain trackers for various purposes. In the end, these tools can be used by third parties to track users throughout different applications they use, can be easily misused,[138] and as opposed to tracking conducted on mobile or desktop web browsers, tracking via SDKs is quite difficult to block.[139]

---

[136] See Pierre Laperdrix and others, 'Browser Fingerprinting: A Survey' [2019] arXiv:1905.01051 [cs] <http://arxiv.org/abs/1905.01051> accessed 24 August 2020.

[137] The website ('AmIUnique' <https://amiunique.org/> accessed 24 August 2020) allows users to see if their browser fingerprint is unique and therefore can be tracked across the web accurately by trackers.

[138] For a recent example, where a company named MobiBurn paid app developers to integrate its SDKs into the apps they develop in exchange for money and then unlawfully collected vast amounts of data from end-users' devices through the integrated SDKs, including their call-logs, email addresses and location information, sold the data to various data brokers, and is sued by Facebook for its conduct, see Wolfie Christl, 'Wolfie Christl on Twitter on MobiBurn' (*Twitter*, 28 August 2020) <https://twitter.com/WolfieChristl/status/1299287573370724353> accessed 30 August 2020.

[139] 'How Do Tracking Companies Know What You Did Last Summer?' (*Privacy International*, 21 May 2019) <http://privacyinternational.org/explainer/2976/how-do-tracking-companies-know-what-you-did-last-summer> accessed 24 August 2020.

It is also important to address CNAME cloaking,[140] which is a new technique that involves hiding third-party trackers under first party trackers or disguising them as first-party trackers: *"It misleads web browsers into believing that a request for a subdomain of the visited website originates from this particular website, while this subdomain uses a CNAME to resolve to a tracking-related third-party domain. This technique thus circumvents third-party targeting privacy protections"*.[141]

In other words, in CNAME Cloaking, if a user is visiting the website bbc.com, this website uses, instead of "google.adsense.com", another address such as "axwt.bbc.com", for calling third party trackers. This address looks like it originates from the bbc.com website that the user is visiting; however, it leads to a third-party tracker, such as "google.adsense.com". Adblockers cannot block tracking when this technique is used, because adblockers usually work by blocking domain names. For instance, an adblocker can easily block "google.adsense.com". However, it is not possible for the adblocker to predict that "axwt.bbc.com" will take the user to "google.adsense.com"; therefore, it will not block "axwt.bbc.com". Some browsers and adblockers have developed innovative solutions that can fight against CNAME cloaking, for instance Firefox and uBlock Origin can block CNAME cloaking.[142] Still, considering how most browsers are still unable to block CNAME cloaking, to protect themselves from tracking via CNAME cloaking, the users may have to resort to more intricate applications which are capable of DNS-level blocking.[143]

Another problematic aspect of online tracking is that the users cannot be really anonymous because platforms and tech companies that rely on data use the same hash function to anonymise the data.[144] This is because when the anonymised profile data is shared, for instance, personal data such as email addresses are not shared, but the hashed versions of these email addresses are shared. However, while sharing hashed versions of such data, the same hash function is used. Hence, the

---

[140] Ha Dao, Johan Mazel and Kensuke Fukuda, 'Characterizing CNAME Cloaking-Based Tracking on the Web' [2020] IFIP 9; Ha Dao, 'Characterizing CNAME Cloaking-Based Tracking' (*APNIC Blog*, 4 August 2020) <https://blog.apnic.net/2020/08/04/characterizing-cname-cloaking-based-tracking/> accessed 24 August 2020.

[141] Dao (n 140).

[142] Romain Cointepas, 'CNAME Cloaking, the Dangerous Disguise of Third-Party Trackers' (*Medium - NextDNS*, 22 November 2019) <https://medium.com/nextdns/cname-cloaking-the-dangerous-disguise-of-third-party-trackers-195205dc522a> accessed 24 August 2020.

[143] ibid.

[144] Wolfie Christl, 'Corporate Surveillance in Everyday Life' (Cracked Labs 2017) 69–70 <https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf> accessed 24 August 2020; 'Wolfie Christl on Twitter - Anonymized Data' (*Twitter*, 29 July 2020) <https://twitter.com/WolfieChristl/status/1288229191759081472> accessed 24 August 2020.

hashing results in the same output, in other words, the data that is the result of hashing is the same. This means that even though the email address is not shared in the ecosystem, it is still possible to identify and target specific individuals and monitoring can still take place in today's digital ecosystem. As Christl puts it, calling this kind of personal data sharing anonymized is corporate misinformation, and unfortunately, a powerful industry lives on this illusion created by themselves.[145] Moreover, since the same hash function is used by everyone, everyone gets the same output, therefore whether the hash can be reversed is not relevant in the discussions. Yet, it is important to note that hashed IDs can also be based on other relevant data including phone numbers and using more complex versions such as hashing the hashes or using salted hashes. However, as Christl points out, sharing/matching personal data through hashing email addresses and turning them into hashed pseudonymous identifiers is merely sharing/matching personal data. Yet, in many cases the hashing practices are quite simple, as described above. Sharing/matching personal data by converting email addresses into hashed pseudonymous identifiers across companies is just: sharing/matching personal data.[146] Many companies use misleading statements when they make statements that personal data converted in this manner which can be linked together and synchronised with user profiles remain private.[147] For instance, Oracle states that all IDs derived from personally identifiable information must be hashed before being sent to their platform and implies that the hashed versions of these IDs remain private.[148] Making statements suggesting or implying that sharing data in a hashed format ensures maintaining privacy is highly misleading. In addition to hashing, data platforms such as Oracle refer to various mechanisms, implying that such mechanisms are good practice for the purposes of ensuring data minimisation. Put differently, such mechanisms can be used to suggest "only minimum personal data sharing, from 'querying' to 'verifying' to 'matching' etc".[149] There are many arguments revolving around whether or not data can be "deanonymized"; yet, before discussing deanonymization, it would be

[145] 'Wolfie Christl on Twitter - Anonymized Data' (n 144).
[146] Christl, 'Corporate Surveillance in Everyday Life' (n 144) 69.
[147] 'Oracle Data Cloud Platform Help Center' <https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/IDManagement/sending_ohashes.html> accessed 24 August 2020; Christl, 'Corporate Surveillance in Everyday Life' (n 144) 61, 69.
[148] 'Oracle Data Cloud Platform Help Center' (n 147).
[149] See 'Wolfie Christl on Twitter - Anonymized Data' (n 144); See also Christl, 'Corporate Surveillance in Everyday Life' (n 144).

more appropriate if the discussions underscored when data is not anonymized in the first place, specifically when personal data sharing based on pseudonymous identifiers is in question.[150]

In addition to the above-mentioned tracking methods, it is also reported that websites will be enabled to do advanced network connections soon. Although granting this ability to websites may have benefits, it may also enable persistent tracking.[151] Another tracking method to be mentioned involves Internet Protocol version 6, or IPv6, which can be used "to embed a network device's Ethernet MAC address in an IPv6 address"[152] and thus to uniquely identify each device, raising concerns regarding end-users' privacy. Still, alternative solutions to alleviate such concerns are developed, for instance methods involving randomisation and temporary addresses are suggested to protect end-user's privacy.[153]

iii. First party/third-party tracking

There are two main ways through which online tracking takes place: first-party tracking and third-party tracking. First-party tracking simply means that the users are being tracked by the website they are visiting or the app they are using, and their data is not being sent to third parties. Third-party tracking on the other hand involves the user data being sent to third parties via, among other means, ad exchanges. Third-party tracking is highly risky compared to first-party tracking: In practice, third-party tracking means that the data will be shared with lots of third parties unknown to the user and it becomes extremely difficult to exert control over data once it is shared in this manner. As a result, in third-party tracking, it is difficult to comply with the GDPR's requirements, and especially requirements concerning information and consent practices. Ad exchanges, as will be explained in the following sub-section, are some of the most prominent mediums where the data is shared with third parties.

---

[150] 'Wolfie Christl on Twitter - Anonymized Data' (n 144).

[151] See Lukasz Olejnik, 'Lukasz Olejnik on Twitter - 20 August 2020' (*Twitter*, 20 August 2020) <https://twitter.com/lukOlejnik/status/1296471401147305986> accessed 24 August 2020; See also 'WICG/Raw-Sockets' (*GitHub*) <https://github.com/WICG/raw-sockets> accessed 24 August 2020.

[152] Mathew J Schwartz, 'Facing the Privacy Implications of IPv6' (9 September 2011) <https://iapp.org/news/a/2011-09-09-facing-the-privacy-implications-of-ipv6/> accessed 30 August 2020.

[153] Lukasz Olejnik, 'Lukasz Olejnik on Twitter on IPv6' (*Twitter*, 27 August 2020) <https://twitter.com/lukOlejnik/status/1299012058386780161> accessed 30 August 2020; Suresh Krishnan and others, 'Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6' (26 August 2020) <https://tools.ietf.org/html/draft-ietf-6man-rfc4941bis-10> accessed 30 August 2020.

Due to third-party tracking becoming increasingly frowned upon and Safari and Firefox developing technical ways to block third-party tracking, some workarounds have been developed. For instance, some third-party trackers disguise themselves as first-party trackers via an advanced tracking method called "redirect tracking" or "bounce tracking".[154] In this technique, the user is taken to the website of the third party for a very brief, imperceptible moment and then redirected to their actual destination. This way, the third party is able to act as a first party, since the user has had a stopover on its website, and place its tracker as a first-party tracker.[155] This enables the third parties that engage in redirect tracking to bypass technologies that block third-party tracking, but it is possible to prevent redirect tracking as well.[156]

Third-Party identifiers

In August 2019, Google announced that it was planning to develop a new model where the internet users will have more privacy and in which the third-party cookies will become obsolete. In line with this plan, Google announced a new initiative (known as Privacy Sandbox)[157] to develop a set of open standards to fundamentally enhance privacy on the web.[158] Google stated that its goal for this open source initiative is to make the web more private and secure for users, while also supporting publishers.[159] Allowing third party trackers depends on the company's policy; for instance, Safari and Firefox's cookie/tracking policies do not allow third party trackers. Chrome has allowed it so far but Google is planning to ban third party trackers on Chrome gradually in the

[154] Steven Englehardt, 'Firefox 79 Includes Protections against Redirect Tracking' (*Mozilla Security Blog*, 4 August 2020) <https://blog.mozilla.org/security/2020/08/04/firefox-79-includes-protections-against-redirect-tracking> accessed 26 August 2020.
[155] Mozilla, 'Redirect Tracking Protection' (*MDN Web Docs*) <https://developer.mozilla.org/en-US/docs/Mozilla/Firefox/Privacy/Redirect_tracking_protection> accessed 24 August 2020.
[156] Selena Deckelmann, 'Latest Firefox Rolls out Enhanced Tracking Protection 2.0; Blocking Redirect Trackers by Default' (*The Mozilla Blog*, 4 August 2020) <https://blog.mozilla.org/blog/2020/08/04/latest-firefox-rolls-out-enhanced-tracking-protection-2-0-blocking-redirect-trackers-by-default> accessed 24 August 2020.
[157] 'Chrome Cookie Tracking Changes 2020' (*YIELDKIT*, 31 January 2020) <https://www.yieldkit.com/news/chrome-cookie-tracking-changes-2020/> accessed 24 August 2020.
[158] Meera Narendra, '#Privacy: Google Announces Plans to Make Third Party Cookies Obsolete' (*PrivSec Report*, 15 January 2020) <https://gdpr.report/news/2020/01/15/privacy-google-announces-plans-to-make-third-party-cookies-obsolete/> accessed 24 August 2020.
[159] '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 24 August 2020.

next 2 years.[160] However, Google has rolled back one of the first stages of its cookie action plan and the enforcement of SameSite cookie rules.[161]

Removing third party identifiers will, at the first stage, prevent tracking people across the web, across different websites and platforms. Moreover, it is expected to strengthen the position of big data companies that have access to/are capable of collecting first-party data, such as Google, Facebook and Amazon.[162] For instance, removing third-party identifiers from Chrome, Google will easily strengthen its position as one of the most prominent first-party trackers in the online ecosystem, along with other platforms that have their own platforms or "walled-gardens". It is also argued that removing third-party identifiers would not hurt tech giants such as Google's businesses much, as they are already capable of collecting vast amounts of data through their own services and within their own walled gardens/platforms. On the other hand, publishers and advertisers that depend on third-party tracking may suffer a lot, having to adapt their business models to a completely new environment and suffering big losses in the meanwhile. However, even though some stakeholders in the online advertising ecosystem may suffer unfairly, there is no doubt that removing third-party identifiers will strengthen user privacy.

It is also important to note that such a big change made for deleting third-party cookies from the Chrome browser is likely to have equally big effects on different stakeholders as there could be major changes from attribution modelling to personalization initiatives and conversion analytics.[163] There are potential benefits in blocking third party cookies such as preventing ad fraud, where most of the ad budget is lost in the middle layers of the ecosystem, to publishers'

[160] ibid; Frederic Lardinois, 'Google Wants to Phase out Support for Third-Party Cookies in Chrome within Two Years' (*TechCrunch*, 14 January 2020) <https://social.techcrunch.com/2020/01/14/google-wants-to-phase-out-support-for-third-party-cookies-in-chrome-within-two-years/> accessed 24 August 2020; Megan Graham, 'Google Plans to Kill Support for Third-Party Cookies That Track You All over the Internet' (*CNBC*, 14 January 2020) <https://www.cnbc.com/2020/01/14/google-chrome-to-end-support-for-third-party-cookies-within-two-years.html> accessed 24 August 2020.

[161] 'Chrome Cookie Tracking Changes 2020' (n 157).

[162] ibid.

[163] Raquel Rosenthal, 'A 5-Step Path to Cookieless Digital Marketing' (*SmartBrief*, 7 May 2020) <https://www.smartbrief.com/original/2020/05/5-step-path-cookieless-digital-marketing> accessed 24 August 2020; 'Cookieless Web: 3 Areas To Watch In The Second Half Of 2020' (*AdExchanger*, 26 May 2020) <https://www.adexchanger.com/data-driven-thinking/cookieless-web-3-areas-to-watch-in-the-second-half-of-2020/> accessed 24 August 2020.

disadvantage, through traffic and ad views generated by bots and other fraudulent methods.[164] In addition, blocking third party cookies can be beneficial for preventing cross-site forgery attacks.[165]

Recently, in August 2020, class action lawsuits were announced in the Netherlands and the UK for Oracle and Salesforce regarding cookie tracking consent.[166] The suits will contend that "mass surveillance of Internet users to carry out real-time bidding ad auctions cannot possibly be compatible with strict EU laws around consent to process personal data".[167] The Privacy Collective announced that it claims compensation for the wrongful use of internet users' personal data and brought action against Oracle and Salesforce for breaking consent rules and for illegally sharing users' personal data through third party tracking cookies and other adtech technologies.[168]

iv. RTB and Micro Targeting

Real-Time Bidding (RTB), also called "programmatic advertising" is a significant part of today's online advertising ecosystem. When a website or an app uses RTB, it means that advertisers compete to give the highest bid for the "impression" of the user who is about to see an advert on the advertising space provided by the website or the app.

The RTB system works as follows: Websites and apps dedicate certain spaces within their infrastructure, to display ads. For instance, while Instagram displays ads in the form of a story or as sponsored posts on its users' feeds, a website may have banners for adverts. The users are tracked throughout the web and various information including the pages they are browsing, their

---

[164] For further details, see Adform, 'What Is Ad Fraud and How Can It Be Prevented' (2019) 4–6 <https://iabeurope.eu/wp-content/uploads/2019/11/what-is-ad-fraud-and-how-can-it-be-prevented.pdf> accessed 24 August 2020.

[165] 'Cross-Site Request Forgery', , *Wikipedia* (2020) <https://en.wikipedia.org/w/index.php?title=Cross-site_request_forgery&oldid=972395753> accessed 24 August 2020.

[166] Natasha Lomas, 'Oracle and Salesforce Hit with GDPR Class Action Lawsuits over Cookie Tracking Consent' (*TechCrunch*, 14 August 2020) <https://social.techcrunch.com/2020/08/14/oracle-and-salesforce-hit-with-gdpr-class-action-lawsuits-over-cookie-tracking-consent/> accessed 24 August 2020; Carly Page, 'Oracle And Salesforce Hit With $10 Billion GDPR Class-Action Lawsuit' (*Forbes*, 14 August 2020) <https://www.forbes.com/sites/carlypage/2020/08/14/oracle-and-salesforce-hit-with-10-billion-gdpr-class-action-lawsuit/> accessed 24 August 2020.

[167] Lomas, 'Oracle and Salesforce Hit with GDPR Class Action Lawsuits over Cookie Tracking Consent' (n 166).

[168] ibid; 'The Privacy Collective | Because Privacy Matters' <https://theprivacycollective.eu/en/> accessed 24 August 2020; see also Natasha Lomas, 'Mental Health Websites in Europe Found Sharing User Data for Ads' (*TechCrunch*, 4 September 2019) <https://social.techcrunch.com/2019/09/04/mental-health-websites-in-europe-found-sharing-user-data-for-ads/> accessed 24 August 2020.

IP address and location, information about their device and unique advertising identifiers are collected by various actors, as explained above in the previous sub-section. This data is then used to infer these individuals' interests, personality, sexuality, political and religious views so that ads that suit their interest better can be displayed.[169] This data can be and has been systematically used for other purposes as well, such as product development and political micro-targeting.[170]

When an individual visits a website or uses an app, within milliseconds, the information about the individual is first sent to Supply Side Platforms[171] (also called Sell-Side Platforms or monetisation platforms[172]) (SSPs). SSPs help publishers market their user portfolios and ad spaces to ad exchanges and marketers.[173] After receiving the information from the website, the SSP sends an ad request to ad exchange platforms, which are made up of a number of different ad networks and which "*help publishers manage advertising requests from many advertisers*".[174] When an ad exchange receives the ad request, it broadcasts the data it receives via this request to Demand Side Platforms (DSPs) and sends bid requests to these DSPs.

DSPs are platforms that act on behalf of marketers who want to advertise their products and services. If the marketer wants to target the user who is about to see the ad, in other words, if the individual fits with the target audience of the marketer, the DSP sends an automatic bid to the ad exchange. The DSP that sends the highest bid wins the auction and gets to display the marketer's advert on the website or the app that the targeted individual is viewing. Within this context, the

[169] It was observed by Ryan that one data broker using Google's RTB system profiles individuals in categories such as "Substance abuse", "Diabetes", "Chronic Pain" and "Sleep Disorders". On the other hand, one data broker using IAB's RTB system categorises individuals in categories such as "AIDS & HIV", "Incest & Abuse Support", "Brain Tumor", "Incontinence", "Depression" (Ryan [n 101] 6); Other categories used by data brokers using RTB systems include 'Infertility', 'STD' and 'Conservative', which refers to the political views of the profiled individual (ibid 13–15).

[170] For an example where data obtained from online advertising was used to influence the parliamentary elections in Poland in 2019, through specifically targeting LGBTQ+ individuals, see Johnny Ryan, 'Submission to Irish Data Protection Commissioner' (n 101) 5.

[171] Johnny Ryan, 'Report from Dr Johnny Ryan – Behavioural Advertising and Personal Data' (2018) 5 <https://brave.com/wp-content/uploads/2018/09/Behavioural-advertising-and-personal-data.pdf> accessed 24 August 2020.

[172] Norwegian Consumer Council, 'Out of Control' (2020) 35, fn 83 <https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf> accessed 24 August 2020.

[173] Christl, 'Corporate Surveillance in Everyday Life' (n 144) 45.

[174] ibid.

marketers pay for each "impression", i.e. each time their ad is displayed on the website.

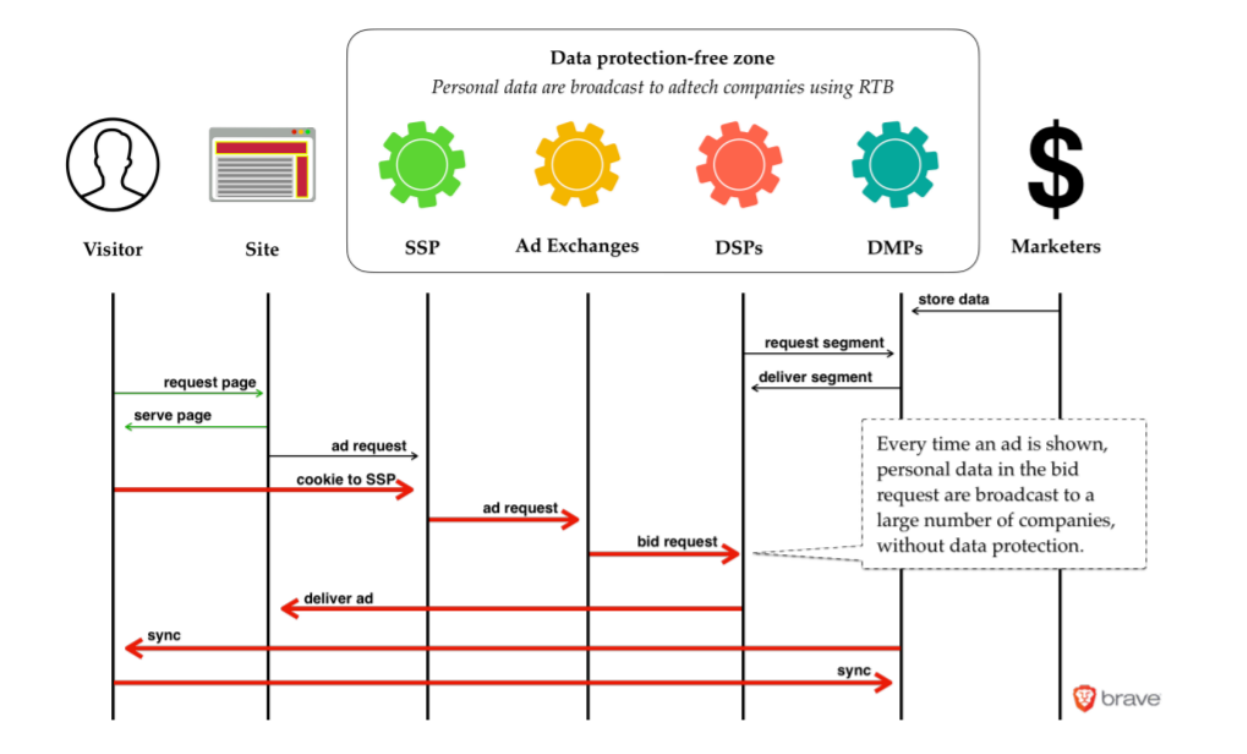

Figure depicting information exchanges in RTB (simplified), by Johnny Ryan, 'Report from Dr Johnny Ryan – Behavioural advertising and personal data' https://brave.com/wp-content/uploads/2018/09/Behavioural-advertising-and-personal-data.pdf[175]

Another type of actor that partakes in the RTB mechanism and generally in online advertising are Data Management Platforms (DMPs). DMPs "*can perform a "sync" that uses this personal data to contribute to their existing profiles of the person. In it worth noting that this sync would not be possible without the initial bid request".*[176] Cambridge Analytica, the main actor of the Cambridge Analytica-Facebook scandal,[177] is an infamous example of such DMPs.

It needs to be noted that the RTB schemes are not always described in the same manner, sometimes different terms are used to describe the same actors. Moreover, the roles of the different actors

[175] Ryan, 'Report from Dr Johnny Ryan – Behavioural Advertising and Personal Data' (n 171) 5.
[176] ibid.
[177] Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' *The Guardian* (17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 17 September 2020.

described above are not always clear cut. As stated by Chirstl, "*[t]he lines between the different kinds of vendors, such as ad exchanges, SSPs, or DSPs, are often overlapping and blurred*".[178]

There are different types of auction mechanisms in RTB. For instance, open auctions are auctions where there is no limitation regarding the participants, whereas in private auctions only certain participants can bid, depending on whether the publisher allows them based on criteria they determine. On the other hand, certain advertisers and publishers may choose a scheme where they do not use auctions and instead have an agreement between themselves, fixing the price and conditions of the advertisement, called a "preferred deal".[179] Depending on the type of auction mechanism chosen, the data of the individual person who is about to view the ad may be shared with hundreds or even thousands of actors in the RTB mechanism.

There are two main RTB schemes that are being used today: OpenRTB, an RTB system developed by the Interactive Advertising Bureau (IAB)s[180] and Google's proprietary scheme "Authorized Buyers".[181] As a result of this dual structure, the standards set by Google and IAB determine the nature and functioning of the whole RTB mechanism. In a way, it can be said that these two actors are capable of actively regulating the whole ecosystem.

The below figure depicts data collection practices on individuals, by adopting a comparative approach towards the developments which took place in the recent years.

[178] Christl, 'Corporate Surveillance in Everyday Life' (n 144) 45.

[179] Norwegian Consumer Council (n 172) 34–35.

[180] 'OpenRTB (Real-Time Bidding)' (*IAB*) <https://www.iab.com/guidelines/real-time-bidding-rtb-project/> accessed 26 August 2020.

[181] 'Introducing Authorized Buyers - Authorized Buyers Help' (*support.google.com*) <https://support.google.com/authorizedbuyers/answer/9070822?hl=en> accessed 24 August 2020. Google's Authorized Buyers scheme distributes the data to a striking number of more than 900 data companies in the RTB system, see Johnny Ryan, 'Submission to Irish Data Protection Commissioner' (n 101) 2 and Appendix F.

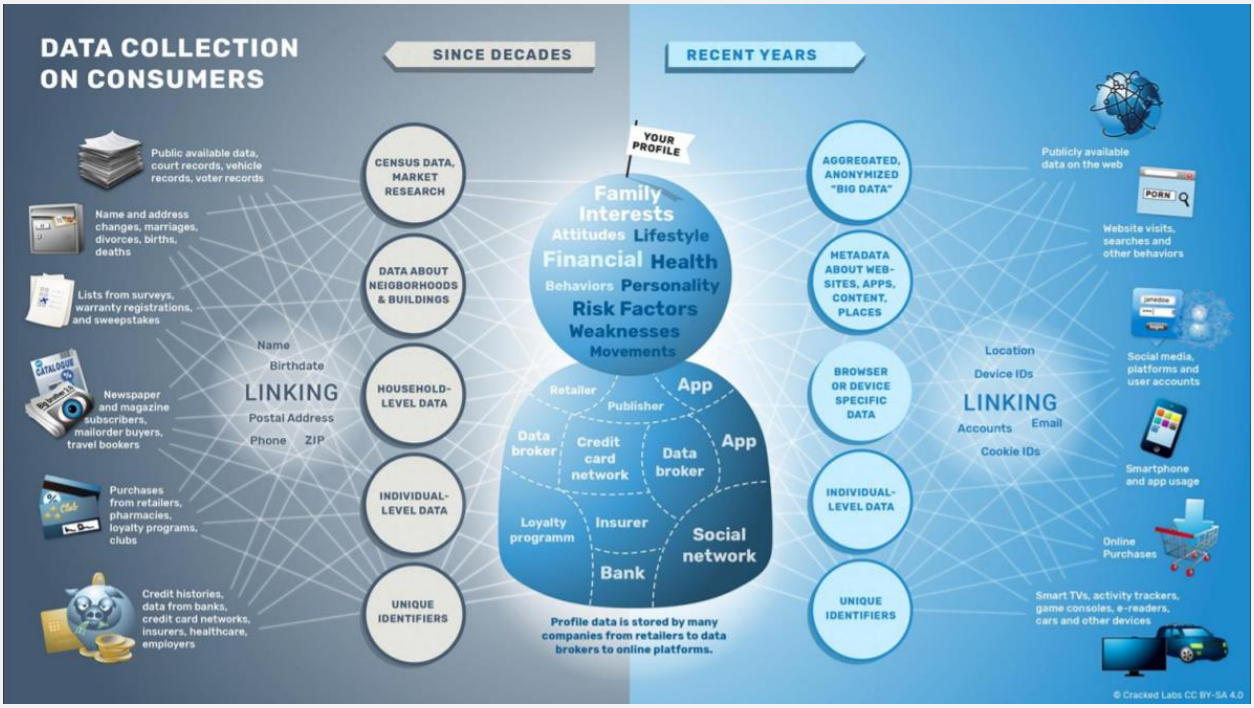

Figure as appears in Cracked labs, Wolfie Christl, 'Corporate Surveillance in Everyday Life', 2017, p. 65, Figure 5[182]

As explained above and depicted in the above figure, huge amounts of data are collected on an incredibly high number of individuals[183] and there are many different actors in the RTB ecosystem. The number can go up to thousands,[184] which leads to one of the biggest pitfalls of RTB: each actor partaking in this ecosystem is technically capable of sharing the data with other third parties. There are no technical limitations to stop them. As a result of this structure, it is technically impossible to know the final destination of the data or the identity of data controllers and processors that receive the data.[185] This results in an unknown number of advertisers receiving the information about the individual who is about to see an ad. The legal requirements regarding online

[182] Christl, 'Corporate Surveillance in Everyday Life' (n 144) 65, Figure 5.

[183] See also Wolfie Christl, 'Wolfie Christl on Criteo' (*Twitter*, 31 August 2020) <https://twitter.com/WolfieChristl/status/1300528762153586688> accessed 17 September 2020.

[184] For instance, Google's Authorized Buyers scheme distributes the data to a striking number of more than 900 data companies in the RTB system, see Johnny Ryan, 'Submission to Irish Data Protection Commissioner' (n 101) 2 and Appendix F.

[185] Johnny Ryan, 'New Evidence to Regulators: IAB Documents Reveal That It Knew That Real-Time Bidding Would Be "Incompatible with Consent under GDPR".' (*Brave Browser*, 20 February 2019) <https://brave.com/update-on-gdpr-complaint-rtb-ad-auctions/> accessed 24 August 2020.

tracking were detailed above, in the subheading "Cookies", and considering those, it is important to note that this is incompatible with the core principles set out under the GDPR.

The problems of the RTB mechanism and extensive tracking online is not limited to sharing of data with a great number of unknown parties. The existence of a great number of participants, and the impossibility of limiting further sharing of data with outside actors create security vulnerabilities as well. In the past, there have been instances where vulnerabilities in ad networks were exploited to serve malware to the viewers who receive the ad, a practice dubbed "malvertising".[186]

Another problem that the RTB and online tracking could cause is the misuse of data, for instance for computational political microtargeting and influencing voters. Such a misuse of data to influence the democratic processes took place in the Cambridge Analytica scandal and could happen also via the RTB mechanism. Taking these risks into account, some online platforms have limited the possibility of micro targeting on their services, for instance Facebook and TikTok allow micro-targeting of a minimum 1000 users (and these measures can still be bypassed).[187] Furthermore, the European Parliament recently called for a ban on micro-targeted ads and suggested that the platforms shall provide more transparent information to their users regarding their advertising practices.[188]

There are concerns with regards to risks of advertising, automated decision making including profiling, online manipulation techniques including micro-targeting, and social sorting since they can have serious implications for individuals in a democratic society where individuals' freewill

[186] Alex Hern, 'Major Sites Including New York Times and BBC Hit by "ransomware" Malvertising' (*the Guardian*, 16 March 2016) <http://www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising> accessed 24 August 2020; Brian Prince, 'Sophisticated Malvertising Campaign Targets US Defense Industry' (*Dark Reading*, 17 October 2014) <https://www.darkreading.com/attacks-breaches/sophisticated-malvertising-campaign-targets-us-defense-industry-/d/d-id/1316753> accessed 24 August 2020.

[187] Lukasz Olejnik, 'European Parliament Calls to Ban Micro-Targeted Ads. Now What?' (*Security, Privacy & Tech Inquiries*, 26 June 2020) <http://blog.lukaszolejnik.com/european-parliament-calls-to-ban-micro-targeted-ads-now-what/> accessed 24 August 2020.

[188] European Parliament, 'European Parliament Resolution of 18 June 2020 on Competition Policy' (18 June 2020) para 105 <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0158_EN.html> accessed 24 August 2020; See also Olejnik, 'European Parliament Calls to Ban Micro-Targeted Ads. Now What?' (n 187).

and fundamental rights should be respected.[189] It is argued that with massive data collection carried out in the advertising ecosystem, data subjects' rights are undermined and they are treated as commodities.[190] This treatment has compelling implications for being regarded as a threat to society.[191] This is because through massive data collection practices,[192] companies become more capable of influencing and controlling as "they can be used to deliver deceitful, or aggressive messages, or generally messages that bypass rationality by appealing to weaknesses and emotions".[193] These points are not merely relevant in the RTB context, but have strong implications and high relevance in a more general sense in the context of online advertising.

In the RTB context, it is also important to refer to the recent developments with regards to a new FTC investigation.[194] A group of members of Congress has asked the FTC to start an investigation into the mobile advertising and RTB industry's practice of covertly tracking users by using digital display ads.[195] In their request, there is an overt reference to RTB ecosystem and privacy violations of the private sector in the ad tech industry, and the letter also mentions MobileWalla, and data collection carried out during the Black Lives Matter protests.[196] This request is significant as it illustrates the increasing awareness regarding the problematic aspects of the RTB ecosystem.

---

[189] For further discussion see Giovanni Sartor and others, *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence: Study* (2020) 22–25 <http://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> accessed 24 August 2020.

[190] See for example Federal Trade Commission, 'FTC's Use of Its Authorities to Protect Consumer Privacy and Security' (2020) <https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf>; and Federal Trade Commission, 'Opinion of the Federal Trade Commission in the Matter of Cambridge Analytica, LLC, a Corporation' <https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_opinionpublic.pdf> accessed 24 August 2020; and Lee Mcguigan, 'Selling The American People: Data, Technology, And The Calculated Transformation Of Advertising' <https://repository.upenn.edu/cgi/viewcontent.cgi?article=4945&context=edissertations>.

[191] See for example Anthony Nadler, Matthew Crain and Joan Donovan, 'Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech' (Data & Society).

[192] Criteo is a striking example that illustrates the massive data collection practices of adtech companies. According to the company's Q2 2020 Earnings Call document, their ID Graph scheme has '2.5 billion unique users globally, of which 98% have persistent 152 identifiers beyond cookies'. See Christl, 'Wolfie Christl on Criteo' (n 183).

[193] Sartor and others (n 189) 28–29.

[194] Byron Tau and Patience Haggin, 'Lawmakers Urge FTC Probe of Mobile Ad Industry's Tracking of Consumers' *Wall Street Journal* (31 July 2020) <https://www.wsj.com/articles/lawmakers-urge-ftc-probe-of-mobile-ad-industrys-tracking-of-consumers-11596214541> accessed 25 August 2020.

[195] ibid.

[196] Sara Merken, 'Lawmakers Ask FTC to Probe Online Ad Industry, Pointing to "widespread" Violations' *Reuters* (1 August 2020) <https://www.reuters.com/article/adtech-privacy-ftc-idUSL2N2F22OL> accessed 25 August 2020;

With regards to micro-targeting, Gary and Soltani argue that restricting or lessening the ability to micro target ads would be more effective, when compared to any law policing online discourse contending that it will raise considerably less free speech issues.[197] On the other hand, Edelman points out that in a scenario where a law had passed and companies were banned from doing any ad micro-targeting business, people might come to understand that micro-targeting had supercharged advertisers' ability to discriminate, even when they were not trying to and that it would be correct to think that the ads users come across might be for products they are less likely to buy.[198] Yet, he also points out that in such a scenario, banning targeted advertising would not necessarily mean that the personalization would come to an end.[199] Therefore, it can be concluded that banning targeted advertising and micro targeting would not mean that automated decision making including profiling and personalization techniques would perish nor that it would significantly decrease.

On the other hand, CNIL's decision against the French company Vectuary in 2018 triggered discussions with regards to ameliorating or in fact remaking the ad tech industry for good.[200] In the decision, emphasis was put on the notion of consent. To elaborate, CNIL underscored that the rules prescribed by Article 7 were not fulfilled just because it was assumed that a contractual clause ensured having carried out data processing activities, more specifically, data collection by obtaining valid initial consent. Vectuary was held accountable for not being able to demonstrate that the company carried out its data processing activities in compliance with the rules related to

Allison Schiff, 'Lawmakers Call RTB An Unfair And Deceptive Business Practice In Letter To The FTC' (*AdExchanger*, 4 August 2020) <https://www.adexchanger.com/privacy/lawmakers-call-rtb-an-unfair-and-deceptive-business-practice-in-letter-to-the-ftc/> accessed 25 August 2020.

[197] See Jeff Gary and Ashkan Soltani, 'First Things First: Online Advertising Practices and Their Effects on Platform Speech' (*Knight First Amendment Institute at Columbia University*, 21 August 2019) <https://knightcolumbia.org/content/first-things-first-online-advertising-practices-and-their-effects-on-platform-speech> accessed 25 August 2020.

[198] See Gilad Edelman, 'Why Don't We Just Ban Targeted Advertising?' [2020] *Wired* <https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising/> accessed 25 August 2020.

[199] ibid.

[200] Natasha Lomas, 'How a Small French Privacy Ruling Could Remake Adtech for Good' (*TechCrunch*, 21 November 2018) <https://social.techcrunch.com/2018/11/20/how-a-small-french-privacy-ruling-could-remake-adtech-for-good/> accessed 25 August 2020.

consent; more specifically, Vectuary failed to show the validity of the expressed consent for its data processing activities.[201]

CNIL revealed that Vectuary was holding "the personal data of a staggering 67.6 million people when it conducted an on-site inspection of the company in April 2018".[202] Although Vectuary was not given a fine for this, CNIL ordered the company to delete all data it had not already deleted, as it decided that data collection activities were not carried out in compliance with the relevant rules under the GDPR. Accordingly, CNIL decided that the obtained consent was not valid, and finally, ordered Vectuary to cease processing data without consent,[203] raising concerns among various actors of the ad tech industry.

In addition to CNIL's Vectuary decision, another very important complaint was filed in 2018 with the Irish Data Protection Commission, and the UK's ICO raised concerns as it addressed the ad tech industry and more specifically targeted the RTB system itself.[204] There are other examples worth mentioning, in different places in Europe. For instance, the mentioned complaint is followed by complaints in Poland[205] by Panoptykon, and later in Belgium, the Netherlands, Spain and Luxembourg, targeting RTB practices.[206]

The data protection and privacy concerns with regards to data processing activities carried out in the advertising industry have increasingly become a soaring topic with a specific focus on RTB.[207] Another concern with regards to RTB relates to ad frauds, which can happen in different ways., for instance, when "bots with automated scripts visit webpages and/or watch videos or click ads".[208] As a result of this type of fraud, AdTech companies and publishers end up paying for

---

[201] *Décision n° MED 2018-042 du 30 octobre 2018 mettant en demeure la société VECTAURY*.

[202] Lomas, 'How a Small French Privacy Ruling Could Remake Adtech for Good' (n 200).

[203] ibid.

[204] ibid.

[205] Natasha Lomas, 'Google and IAB Ad Category Lists Show "Massive Leakage of Highly Intimate Data," GDPR Complaint Claims' (*TechCrunch*, 28 January 2019) <https://social.techcrunch.com/2019/01/27/google-and-iab-ad-category-lists-show-massive-leakage-of-highly-intimate-data-gdpr-complaint-claims/> accessed 25 August 2020.

[206] Natasha Lomas, 'GDPR Adtech Complaints Keep Stacking up in Europe' (*TechCrunch*, 20 May 2019) <https://social.techcrunch.com/2019/05/20/gdpr-adtech-complaints-keep-stacking-up-in-europe/> accessed 25 August 2020.

[207] ibid.

[208] Norwegian Consumer Council (n 172) 55; For a recent example where malicious code was found in an SDK, see John Koetsier, 'Malicious Chinese SDK In 1,200 IOS Apps With Billions Of Installs Causing "Major Privacy Concerns To Hundreds Of Millions Of Consumers"' (*Forbes*, 24 August 2020)

showing ads to bots rather than individuals; this can be the case on publisher sites and also in apps.[209]

It is possible to see the most complicated ad frauds, where technically intricate and complex methods are used, in the financial scheme's context. These methods are used to design "to generate and push revenue through AdTech services, in order to get paid by ad networks and publishers for that traffic".[210] Different methods and tactics used in the RTB ecosystem allows considerable amounts of money to be funnelled towards bad actors mostly without detection. Thus, it can be concluded that tech giants that are involved in advertising are "still funnelling ad dollars towards hate and disinformation".[211]

Digital Content Next's letter[212] underscored the importance of RTB and emphasised that the current system disadvantaged publishers' different ways. Firstly, it enables "real-time data leakage" which became a big concern since the third party intermediaries are allowed to "collect data about publishers' audiences and target those audiences cheaper elsewhere".[213] Secondly, the letter points out that "real-time revenue leakage sees 80%-55% of publisher revenue captured by AdTech companies".[214] The final point in the Digital Content Next's letter concerns ad frauds, where the emphasis on diverting revenue from publishers are highlighted. Consequently, such a

<https://www.forbes.com/sites/johnkoetsier/2020/08/24/malicious-chinese-sdk-in-1200-ios-apps-with-billions-of-installs-causing-major-privacy-concerns-to-hundreds-of-millions-of-consumers/> accessed 26 August 2020; and Alyssa Miller, 'SourMint: Malicious Code, Ad Fraud, and Data Leak in IOS | Snyk' (24 August 2020) <https://snyk.io/blog/sourmint-malicious-code-ad-fraud-and-data-leak-in-ios/> accessed 26 August 2020.

[209] Norwegian Consumer Council (n 172) 55.

[210] ibid.

[211] Branded, 'So *that's* How Breitbart Is Still Making Money' (22 July 2020) <https://branded.substack.com/p/so-thats-how-breitbart-is-still-making> accessed 25 August 2020; See also Zach Edwards, 'Breitbart.Com Is Partnering with RT.Com & Other Sites via Mislabeled Advertising Inventory' (*Medium*, 23 July 2020) <https://medium.com/@thezedwards/breitbart-com-is-partnering-with-rt-com-other-sites-via-mislabeled-advertising-inventory-6e7e3b5c3318> accessed 25 August 2020.

[212] Johnny Ryan, 'Major Publisher Group DCN Tells Regulators "the Sky Won't Fall" If RTB Switches to Safe, Non-Personal Data.' (*Brave Browser*, 19 June 2019) <https://brave.com/dcn-letter-rtb/> accessed 25 August 2020.

[213] ibid.

[214] ibid; See also Keach Hagey, 'Behavioral Ad Targeting Not Paying Off for Publishers, Study Suggests' *Wall Street Journal* (29 May 2019) <https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-for-publishers-study-suggests-11559167195> accessed 25 August 2020.

practice might result in the loss of advertisers' trust and reluctance for investing money on digital advertising.[215]

v. Alternatives and contextual advertising

As explained above, online behavioural advertising involves profiling individuals and targeting them, and has so far been widely detrimental to individuals' right to privacy and data protection. The RTB mechanism has many pitfalls in this regard. A brief look into the recent history of online advertising may tell the onlookers that the online advertising ecosystem is synonymous with behavioural advertising and RTB. This view considers behavioural advertising in its current form to be an inevitable business model. However, it is also argued that the technological developments up to this point will not necessarily determine the future of the online advertising ecosystem and that it is possible to change its course, through regulation, strategic litigation and an emphasis on alternative technologies.[216]

Indeed, online behavioural advertising is not the only viable method to generate meaningful income on the Internet. Some alternative advertising approaches developed in response include removing personal data from online advertising through choosing other types of advertising such as contextual, or by removing sensitive personal data from real-time bidding specifications. The publishers' group DCN and Brave suggest that removing personal data would benefit publishers, even though it may negatively affect ad tech companies.

> *"Removal of personal data from bid requests would negatively impact adtech companies who collect and use data across the web but, ultimately, value would likely shift towards other ways to target advertising which do not require personal data to be shared with all parties such as* ***targeting based on context, non-personal data, localized or 1st party data and other new and old ways to predict and measure advertising relevance****. It would direct new innovation in adtech which we can't predict*".[217]

[215] Ryan, 'Major Publisher Group DCN Tells Regulators "the Sky Won't Fall" If RTB Switches to Safe, Non-Personal Data.' (n 212).
[216] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power* (Profile Books 2019).
[217] Ryan, 'Major Publisher Group DCN Tells Regulators "the Sky Won't Fall" If RTB Switches to Safe, Non-Personal Data.' (n 212).

Contextual advertising is suggested as a strong alternative to the RTB ecosystem. As the name of this practice suggests, contextual advertising involves displaying to the user's advertisements related to the contents of the web page they are viewing. For instance, if a user is viewing a news article about cats, they may be shown an advertisement about a cat product. Although it is possible to develop more complex models of contextual advertising through machine learning and other technologies,[218] the type of contextual advertising that could provide a solution to the problems of today's online advertising ecosystem would ideally not involve personal data or user profiles and would instead centre around the content of the website visited or app used.[219]

An important question at this point is whether contextual advertising would prove to be as lucrative as behavioural advertising for various actors in the online advertising ecosystem, and different studies have reached different conclusions. For instance, a study by Google reached the conclusion that without cookies, publishers would suffer a loss of advertising revenue of more than 50 percent.[220] On the other hand, another research concluded that in the event cookies were disabled the publishers would suffer a loss of only 4 percent.[221] Within this context, the results obtained by publishers who tried contextual advertising could shed a light to the impact of switching to contextual advertising: two significant examples that illustrate such impact are those of the New York Times and the Dutch national broadcaster Nederlandse Publieke Omroep (NPO).

After the entry into force of the GDPR, the New York Times switched to contextual advertising for its European pages. As a result of this switch, the newspaper has not suffered any loss of profits and even continued to grow its online advertising business.[222] It has to be noted that the NYT has a big reader base, which is an advantage not every publisher can have. If the size of the reader base

---

[218] Norwegian Consumer Council (n 172) 16, fn 21. See also, for instance, 'How to Build Better Contextual Bandits Machine Learning Models' (*Google Cloud Blog*) <https://cloud.google.com/blog/products/ai-machine-learning/how-to-build-better-contextual-bandits-machine-learning-models/> accessed 25 August 2020.

[219] Norwegian Consumer Council (n 172) 16.

[220] Deepak Ravichandran and Nitish Korula, 'Effect of Disabling Third-Party Cookies on Publisher Revenue' (2019) <https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf> accessed 25 August 2020.

[221] Veronica Marotta, Vibhanshu Abhishek and Alessandro Acquisti, 'Online Tracking and Publishers' Revenues: An Empirical Analysis' (2019) <https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf>.

[222] Jessica Davies, 'After GDPR, The New York Times Cut off Ad Exchanges in Europe - and Kept Growing Ad Revenue' (*Digiday*, 16 January 2019) <https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/> accessed 25 August 2020.

has an impact on the amount of revenue to be generated through contextual advertising, then it would be difficult to predict the results of abandoning online behavioural advertising for publishers with various reader bases.

Even though it is difficult to reach a definitive conclusion on the basis of the NYT's example, the example of the Dutch broadcaster NPO supports the idea that contextual advertising may indeed compete with behavioural advertising.[223] When the GDPR entered into force in 2018, NPO adopted a new cookie consent mechanism on its websites, where users who continued browsing without actively consenting to the setting of cookies were deemed to not have consented and opted out of tracking. As a result of this choice, 90 percent of visitors opted out of tracking and were subjected to contextual advertising. Such a high percentage of users opting out may not be deemed surprising, in line with the idea of user inertia and the power of defaults, however, the results regarding the advertising revenue were quite surprising. The contextual ads served to the visitors who opted out brought in "as much or more money as ads served to users who opted in"[224] which was so impressive that at the beginning of 2020 NPO decided to completely switch to contextual advertising. Since January 2020, NPO does not track any of its visitors and has since experienced a dramatic increase in its online advertising revenue. According to the reports, even the Covid-19 pandemic has not made a negative impact on NPO's digital advertising business.[225]

Moreover, NPO's experience sheds some light on the question whether smaller publishers would still be able to make as much revenue as they do with online behavioural advertising. A smaller size of reader base may be thought to bring less ad revenue and without behavioural advertising, smaller publishers may not be able to generate as much income. However, NPO's experience successfully disproves this idea and shows that even much smaller NPO branches report huge increases in their advertising revenue thanks to the switch to contextual advertising. For instance, Omroep MAX, which is an NPO publication for people over 50 years of age and ranks in the 4000s in website rankings in Netherlands, has experienced an increase of 92 percent in its ad revenue.

---

[223] Gilad Edelman, 'Can Killing Cookies Save Journalism?' [2020] *Wired* <https://www.wired.com/story/can-killing-cookies-save-journalism/> accessed 25 August 2020.
[224] ibid.
[225] Johnny Ryan, 'New Data Shows Publisher Revenue Impact of Cutting 3rd Party Trackers' (*Brave Browser*, 1 July 2020) <https://brave.com/npo/> accessed 25 August 2020; Johnny Ryan, 'Update (Six Months of Data): Lessons for Growing Publisher Revenue by Removing 3rd Party Tracking' (*Brave Browser*, 24 July 2020) <https://brave.com/publisher-3rd-party-tracking/> accessed 25 August 2020; Edelman (n 223).

Another one of NPOs websites, funx.nl ranks around 1200s in the Netherlands and reported a revenue increase of 80 percent.[226] Of course not only websites with small audiences, but also most popular ones benefited from the switch to contextual advertising: Nos.nl, the third most popular news website of the Netherlands reported an increase of 86% in its advertising revenue.[227]

One contributing factor to the success of contextual advertising is thought to be the fact that online behavioural advertising methods involve many intermediaries who share the revenue and contextual advertising effectively removes them from the picture. The experiment conducted by Guardian supports this point: when Guardian purchased its own ad space through RTB, only 30 percent of the revenue made it back to Guardian, indicating a loss of 70 percent that goes to various actors within the RTB scheme.[228] Another evidence supporting this point is,

> *"a report*[229] *by the Incorporated Society of British Advertisers [which] found that fully half the money spent by advertisers was getting sucked up by various ad tech companies before it got to the publishers running the ads. Even Google publicly states*[230] *that when an advertiser and publisher both use Google's platforms to buy and sell programmatic ads, Google takes more than 30 percent of the money*".[231]

The presence of many other actors within the RTB scheme, as well as the fraudulent behaviour observed throughout, explained in the previous subsection, lead to a significant loss of profit for publishers.

Although these examples are a clear indication of the potential of contextual advertising, it is not straightforward for publishers to switch to contextual advertising. As stated by Jason Kint, the CEO of the major publishers' group Digital Content Next (DCN), the publishers need to move

---

[226] Ryan, 'Update (Six Months of Data)' (n 225).
[227] ibid.
[228] David Pidgeon, 'Where Did the Money Go? Guardian Buys Its Own Ad Inventory' (4 October 2016) <https://mediatel.co.uk/news/2016/10/04/where-did-the-money-go-guardian-buys-its-own-ad-inventory> accessed 25 August 2020.
[229] Abi Gibbons, 'Time for Change and Transparency in Programmatic Advertising' (*ISBA*, 6 May 2020) <https://www.isba.org.uk/news/time-for-change-and-transparency-in-programmatic-advertising/> accessed 25 August 2020.
[230] Sissie Hsiao, 'How Our Display Buying Platforms Share Revenue with Publishers' (*Google Ad Manager*) <https://blog.google/products/admanager/display-buying-share-revenue-publishers> accessed 25 August 2020.
[231] Edelman (n 223).

together, in a concerted manner, since *"there would be a first mover disadvantage to a single publisher that removes personal data from bid requests if its competitors have not done so [...] because an advertiser could simply purchase other advertising "inventory" from alternative publishers who had not done so"*.[232] This is especially the case in the US, where there is a lack of a strict privacy law which could have the effect of forcing publishers to simultaneously switch to contextual advertising.

Online advertising had a considerable negative impact on journalism. Publishers gain revenue mainly from advertising, and in the online advertising ecosystem, they must share their revenue with and are losing most of it to big platforms, such as Google, Facebook, and Amazon. As stated by Aram Zucker-Scharff, the Director for Ad Engineering in The Washington Post's Research, Experimentation and Development group, and reported by Wired,

> *"one of the key reasons why journalism has experienced a decade of brutal layoffs and bankruptcies is that its financial foundation—advertising—has been diverted toward companies that specialize in using data to track people online. According to a 2019 eMarketer report,*[233] *Amazon, Facebook, and Google account for nearly 70 percent of US digital ad revenue*".[234]

Zucker-Scharff's account shows how sensitive the economic situation is for the publishers and emphasizes the need for simultaneous action among publishers towards contextual advertising.

On the other hand, from advertisers point of view, online behavioural advertising and RTB may help advertisers as it allows them to display ads to potential consumers/buyers anywhere on the web, relieving them from the obligation to pay higher prices for ad spaces on more popular publishers' websites. OBA allows them to buy ad space on a less known, even obscure website rather than having to pay much higher prices for the ad spaces on the website of a well-known newspaper. This seems beneficial to boost competition among publishers who provide ad spaces

---

[232] Ryan, 'Major Publisher Group DCN Tells Regulators "the Sky Won't Fall" If RTB Switches to Safe, Non-Personal Data.' (n 212).
[233] Nicole Perrin, 'Facebook-Google Duopoly Digital Ad Spending Forecast Estimates 2019' (*eMarketer*, 4 November 2019) <https://www.emarketer.com/content/facebook-google-duopoly-won-t-crack-this-year> accessed 25 August 2020.
[234] Edelman (n 223).

on their websites. However, in the long run, it may negatively affect the quality of the online content. This is because the OBA ecosystem benefits the websites that manage to gather more clicks, regardless of the content they provide. For instance, a news site that frequently publishes junk news content, i.e. content that is aimed to grab the attention of readers with striking titles which may not be linked to the facts, would manage to gain huge profits due to the clicks they attract. On the other hand, publishers who provide higher quality content may not always be as striking and as a result not as many visitors see their content. In the long run, they may be pushed to adopt a similar style to the junk news websites to attract more readers. Even if the higher quality content providers and publishers are not negatively affected, the competition may be tipped against them as a result of the ecosystem that simply benefits websites that draw more clicks regardless of the quality of content.

vi. Analytics

Analytics services and products constitute an important part of the advertising industry.[235] Tracking for analytics purposes refers to practices where a website analytics monitor the activity of a website. Through analytics tracking, it is possible to monitor the activity on a website, know details about website visitors' location, browser usage, entrance and exit pages and many more. Analytics are used to provide a deeper understanding of how a company's SEO and marketing efforts are doing in terms of performance and further help companies with business decision making since it allows them to track visitors and make deductions in accordance with the results obtained from using analytics tools. Companies can use and apply analytics to data that can be used to make predictions for enhancing the business and improving business performance.[236] The legality of tracking activities conducted for analytics purposes depends first of all on which type

[235] See for example, Louis Columbus, 'Analytics Are Defining The Future Of Digital Advertising' (*Forbes*, 18 January 2018) <https://www.forbes.com/sites/louiscolumbus/2018/01/18/analytics-are-defining-the-future-of-digital-advertising/> accessed 25 August 2020.

[236] See Helen Mayhew, Tamim Saleh and Simon Williams, 'Making Data Analytics Work for You--Instead of the Other Way around | McKinsey' (7 October 2016) <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/making-data-analytics-work-for-you-instead-of-the-other-way-around> accessed 25 August 2020; Jake Frankenfield, 'How Data Analytics Work' (*Investopedia*, 1 July 2020) <https://www.investopedia.com/terms/d/data-analytics.asp> accessed 25 August 2020; See also Christl, 'Corporate Surveillance in Everyday Life' (n 144).

of tracking is used, as this will determine the legal position of the parties that conduct the tracking activity pursuant to the relevant legal framework.

Different DPAs in Europe have developed different approaches to the question of whether analytics tracking can be deemed necessary or not within the scope of the e-Privacy legal framework. With regards to strictly necessary cookies, the Article 29 WP states that the private sector's reliance on their assertion that the use of first party analytics are strictly necessary is irrelevant for companies to offer a functionality that is specifically requested by the data subject in an explicit way since the data subject can also "access all the functionalities provided by the website when such cookies are disabled".[237] Accordingly, in such circumstances, these cookies cannot be regarded to fall under the exemption of consent if they are not limited to the website owner.[238] Furthermore, the ICO provides that it is "unlikely that priority for any formal action would be given to uses of cookies where there is a low level of intrusiveness and low risk of harm to individuals".[239] In the ICO Guidance, the first party analytics cookies are given to exemplify cookies which are potentially low risk.[240] Similarly, recently, the German DPA found that third party analytics are not strictly necessary.[241] Although the German DPA did not specify which tracking tools can be justified on the basis of legitimate interests and therefore do not require consent, similar to ICO's approach, its Guidelines provides that this particularly could be the case for analytics tools that are used with the mere objective of "analyzing website usage or measuring the range of usage and for tools that do not exchange data with third parties or at least do not allow the third party to use the collected information for own purposes, namely to merge it with own

[237] See Santos, Bielova and Matte (n 102) 12; Article 29 Data Protection Working Party, 'Opinion 04/2012 on Cookie Consent Exemption (WP 194)' (n 58) 10.
[238] Santos, Bielova and Matte (n 102) 12.
[239] Information Commissioner's Office, 'Guidance on the Use of Cookies and Similar Technologies' (n 58) s 'What else do we need to consider'.
[240] Santos, Bielova and Matte (n 102) 12; Information Commissioner's Office, 'ICO on the Guidance on the Use of Cookies and Similar Technologies' (3 July 2019) <https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf> accessed 25 August 2020.
[241] Wiebke Jakob, 'Conference of German Data Protection Authorities Issues Guidance on Tracking and Cookies' (*IPT Germany*, 3 May 2019) <https://blogs.dlapiper.com/iptgermany/2019/05/03/conference-of-german-data-protection-authorities-issues-guidance-on-tracking-and-cookies/> accessed 25 August 2020; Datenschutzkonferenz, 'Konferenz Der Unabhängigen Datenschutzaufsichtsbehörden Des Bundes Und Der Länder - Orientierungshilfe Der Aufsichtsbehörden Für Anbieter von Telemedien' <https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf> accessed 25 August 2020.

information".[242]. Moreover, the Greek DPA held that consent is required because third-party analytics trackers are not strictly necessary.[243] Google is not a mere processor but a joint-controller, as it processes the data collected via its analytics tools not only for the purposes determined by the relevant website, but for its own purposes as well.[244] As a result, websites and Google Analytics need an agreement in line with Article 28 of the GDPR instead of Article 26.[245]

Analytics tracking is not always as innocent. Security vulnerabilities created through web skimming, via Google Analytics codes.[246] Web skimming is a known class of attacks usually targeted at online shoppers. This attack occurs once the malicious code is injected into the compromised site. This site collects and then sends data that is put by the user himself/herself to a cybercriminal source. After this process, if the attack succeeds, the cybercriminals gain access to shoppers' payment information. To make the data flow to a third-party resource less apparent, fraudsters generally register domains resembling the names of popular web services.[247]

Another important issue which has come more under spotlight during the COVID-19 crisis[248] concerns the relationship between the online advertising ecosystem and dissemination of junk

---

[242] Jakob (n 241).

[243] See ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ, 'ΔΕΛΤΙΟ ΤΥΠΟΥ - Συστάσεις Για Τη Συμμόρφωση Υπευθύνων Επεξεργασίας Δεδομένων Με Την Ειδική Νομοθεσία Για Τις Ηλεκτρονικές Επικοινωνίες' <http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=84,221,176,170,98,24,72,223>; (as cited in Santos, Bielova and Matte [n 102] 12).

[244] 'Beschluss Der Konferenz Der Unabhängigen Datenschutzaufsichtsbehörden Des Bundes Und Der Länder - 12.05.2020 - Hinweise Zum Einsatz von Google Analytics Im Nicht-Öffentlichen Bereich' <https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf> accessed 25 August 2020.

[245] Dr Carlo Piltz and Johannes Zwerschke, 'DSK Adopts Minimum Requirements for the Use of Google Analytics' (June 2020) <https://www.reuschlaw.de/en/news/dsk-adopts-minimum-requirements-for-the-use-of-google-analytics/> accessed 25 August 2020; 'Beschluss Der Konferenz Der Unabhängigen Datenschutzaufsichtsbehörden Des Bundes Und Der Länder - 12.05.2020 - Hinweise Zum Einsatz von Google Analytics Im Nicht-Öffentlichen Bereich' (n 244).

[246] Victoria Vlasova, 'Web Skimming with Google Analytics' (*Kaspersky Securelist*, 22 June 2020) <https://securelist.com/web-skimming-with-google-analytics/97414/> accessed 25 August 2020.

[247] ibid.

[248] Note that another important issue raised during COVID-19 crisis concerns contact tracing apps and their privacy implications. In this context, Veale's commentary on Apple-Google decentralised contract tracing is worth mentioning. See Michael Veale, 'Privacy Is Not the Problem with the Apple-Google Contact-Tracing Toolkit' (*the Guardian*, 1 July 2020) <http://www.theguardian.com/commentisfree/2020/jul/01/apple-google-contact-tracing-app-tech-giant-digital-rights> accessed 25 August 2020.

news and disinformation.[249] Taylor et al. conducted a research by comparing professional versus junk news and disinformation sources. The research findings show that the top junk news and disinformation sources achieve extremely "high key SEO factors and are optimised for distribution on search and social media".[250] Moreover, it was found that "major high-prestige, high-trust sites inadvertently boost junk news and disinformation promoting their online reputation and visibility"; while the considerable majority of junk news and disinformation domains is seen to rely on major advertising platforms to monetize their pages and more than half of these use Google ads.[251]

vii. Mobile privacy

Contrary to what the current online advertising ecosystem would lead one to believe, it is not impossible for developers to implement privacy by design and default principles. For instance, Apple has introduced new features aligned with these principles with the new version of its mobile operating system iOS 14. Accordingly, user tracking for advertising purposes will become an opt-in feature and privacy "nutrition labels" will be used throughout the system to provide users a better understanding of how they are being tracked.[252]

As a first step, the users will be provided with information regarding the data collection and privacy practices of an app presented to the users in the app store. This information includes "the data types an app may collect, and whether the information is used to track [the users] or is linked to their identity or device"[253] as well as if any third-party advertising or analytics SDKs are used and information about the data collection practices of those SDKs. Apple uses the term "tracking" to describe the practices where the data about the user or their device is shared with data brokers or where the data collected via the app is combined with the data collected from other media. This

[249] Emily Taylor and others, 'Follow the Money: How the Online Advertising Ecosystem Funds COVID-19 Junk News and Disinformation' 8.
[250] oiiadmin, 'Follow the Money: How the Online Advertising Ecosystem Funds COVID-19 Junk News and Disinformation' (*The Computational Propaganda Project*) <https://comprop.oii.ox.ac.uk/research/covid19-disinfo-seo/> accessed 25 August 2020; See also Taylor and others (n 249).
[251] Taylor and others (n 249); oiiadmin (n 250).
[252] 'User Privacy and Data Use - App Store' (*Apple Developer*) <https://developer.apple.com/app-store/user-privacy-and-data-use/> accessed 25 August 2020; See also Lukasz Olejnik, 'Lukasz Olejnik on Twitter - 22 June 2020' (*Twitter*, 22 June 2020) <https://twitter.com/lukOlejnik/status/1275142030629523457> accessed 25 August 2020; and Lukasz Olejnik, 'Lukasz Olejnik on Twitter - 22 June 2020' (*Twitter*, 22 June 2020) <https://twitter.com/lukOlejnik/status/1275158957376536579> accessed 25 August 2020.
[253] 'User Privacy and Data Use - App Store' (n 252).

includes common practices such as "displaying targeted advertisements [...] based on user data collected from [third parties]", "sharing device location data or email lists with a data broker" and "sharing a list of emails, advertising IDs, or other IDs with a third-party advertising network that uses that information to retarget those users in other developers' apps or to find similar users".[254] Through the AppTracking Transparency framework of iOS 14, the apps are required to inform users about the described data practices and obtain their consent. Consent requirement through the AppTracking Transparency framework is removed only when the data does not leave the device in a way where the user or the device can be identified or when the data is shared with and used by the data brokers "solely for fraud detection, fraud prevention, or security purposes, and solely on your behalf. For example, using a data broker solely to prevent credit card fraud".[255]

Apple has its own advertising identification methods, one of which is the ID for Vendors (IDFV). IDFV remains the same for the apps provided by the same vendor on the same device, so it allows tracking users across these apps but not allow across apps from different providers and on different devices unless the user allows such tracking. A new privacy-friendly feature that Apple has introduced with iOS 14 is SKAdNetwork, which is an advertising framework enabling registered advertising networks to measure the efficiency of advertising campaigns without sharing user data.[256] SKAdNetwork is expected to leave CPA and other advertising metrics out of the picture.[257] Another important feature that Apple has revealed is "*an intelligent privacy report feature in the Safari browser that will clearly show who is tracking you"*.[258]

---

[254] ibid.
[255] ibid.
[256] ibid.
[257] Anupam Chugh, 'Apple Is Killing A Billion-Dollar Ad Industry With One Popup' (*Medium*, 10 July 2020) <https://medium.com/macoclock/apple-is-killing-a-billion-dollar-ad-industry-with-one-popup-2f83d182837f> accessed 25 August 2020.
[258] ibid. For a first impression of how this feature works, see John Koetsier, 'Apple's New Browser Blocked 90 Web Trackers In 5 Minutes' (Forbes, 17 September 2020) <https://www.forbes.com/sites/johnkoetsier/2020/09/17/apples-new-browser-blocked-90-web-trackers-in-5-minutes/> accessed 20 September 2020. This article clearly shows the excessive amount of trackers browsers try to place on end-users' devices and hence, the scope and intrusiveness of online tracking. For a similarly striking depiction of the intrusiveness of online tracking, see Privacy International, 'I Asked an Online Tracking Company for All of My Data and Here's What I Found' (Privacy International, 7 November 2018) <http://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found> accessed 16 September 2020.

iOS 14 will also implement "privacy nutrition labels". These are information pop-up boxes which indicate at the point of data collection what types of data are collected about and linked to the user and how the users are tracked across different apps and websites through the said data collection.[259]

The new privacy features that Apple has introduced with iOS 14 are a huge step towards better user privacy, as they would ensure that users will be better informed about when, how and by whom they are being tracked on their mobile devices for advertising purposes and as they will be provided with a straightforward control mechanism to prevent such tracking from taking place once and for all, which would relieve the consent fatigue problem. Moreover, thanks to the ad tracking being made into an opt-in feature, users' tendency to stick with default options will not lead to unwanted tracking. Apple seems to closely follow privacy by design and default principles, which will hopefully influence the rest of the mobile ecosystem. On the other hand, these developments were not received positively by all actors in the online advertising ecosystem. For example, iOS 14's privacy friendly features were met with criticism from Facebook,[260] which stated that the updates will "disproportionately affect [its] Audience Network" and "may render Audience Network so ineffective on iOS 14 that it may not make sense to offer it on iOS 14".[261] Accordingly, Facebook is expecting iOS 14 to decrease its Audience Network's revenue more than 50%.[262]

B - Location Tracking

Online tracking does not only involve tracking via cookies, browser fingerprinting etc. Identifiers on the web, identifiers on mobile devices, real world identifiers (credit card readers, license plate

---

[259] Jules Polonetsky, 'Jules Polonetsky on Twitter' (*Twitter*, 22 June 2020) <https://twitter.com/JulesPolonetsky/status/1275154348918607872> accessed 25 August 2020.

[260] Tim Bradshaw, 'Facebook Attacks Apple for Curbing Personalised Ads' (26 August 2020) <https://www.ft.com/content/1a72d3d7-f2ec-4bb1-9f61-d65afba41821> accessed 30 August 2020; Salvador Rodriguez, 'Facebook Warns Apple's IOS 14 Could Shave More than 50% from Audience Network Revenue' (*CNBC*, 26 August 2020) <https://www.cnbc.com/2020/08/26/facebook-apple-ios-14-could-cut-audience-network-revenue-in-half.html> accessed 30 August 2020; Kieren McCarthy, 'Facebook Apologizes to Users, Businesses for Apple's Monstrous Efforts to Protect Its Customers' Privacy' (27 August 2020) <https://www.theregister.com/2020/08/27/facebook_ios_ads/> accessed 30 August 2020.

[261] 'How We're Preparing Businesses for the Impact of IOS 14' (*Facebook for Business*, 26 August 2020) <https://www.facebook.com/business/news/preparing-our-partners-for-ios-14-launch> accessed 30 August 2020.

[262] 'Preparing Audience Network for IOS 14' (*Facebook Audience Network*, 26 August 2020) <https://en-gb.facebook.com/audiencenetwork/news-and-insights/preparing-audience-network-for-ios14> accessed 30 August 2020.

readers, facial recognition) - allow for widespread tracking of people's location, which in the end can be used to infer detailed and sensitive personal information.

i. The State of the Art of Location Tracking

As a result of the extremely fast-paced technological developments since the 1990s, today individuals carry their electronic devices everywhere with them, which generate unprecedented amounts of data about their behaviour and movement in space. The data collected through these devices allow closely tracking individuals' precise location.[263]

Location data can be obtained through "Satellite-based positioning systems"[264](such as GPS[265]) "wireless technologies"[266] (Wi-Fi and Bluetooth)[267]; "cell-based mobile communication networks" (GSM); "sensor-based systems" (video analytics-enabled devices, eg facial recognition and automated license plate readers),[268] and "chip-card-based systems" (ATMs, POS terminals, transportation card readers etc).[269]

For instance, personal mobile devices that people carry around everywhere with them collect location data through, inter alia, Wi-Fi access points, base station data or GPS, Bluetooth and IP addresses.[270] Smart cards such as credit cards, travel cards used for public transport, loyalty cards etc. can process information through radio frequency identification (RFID).[271] When the card is swiped through a card reader or used in a contactless setting, this indicates the presence of the card

[263] Ezgi Eren, 'Commercial Tracking in Physical Spaces, from an EU Data Protection Perspective' (LLM Dissertation, University of Edinburgh 2019) 9.
[264] WP11, 'D11.5: The Legal Framework for Location-Based Services in Europe' (Future of Identity in the Information Society 2007) D11.5 23 <https://lirias.kuleuven.be/retrieve/40775> accessed 22 August 2019.
[265] Katina Michael and Roger Clarke, 'Location and Tracking of Mobile Devices: Überveillance Stalks the Streets' (2013) 29 Computer Law & Security Review 216, 217–218.
[266] WP11 (n 264) 15.
[267] Mathias Versichele and others, 'The Use of Bluetooth for Analysing Spatiotemporal Dynamics of Human Movement at Mass Events: A Case Study of the Ghent Festivities' (2012) 32 Applied Geography 208.
[268] WP11 (n 264) 15.
[269] ibid 16.
[270] Shakila Bu-Pasha and others, 'EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency' (2016) 2 European Data Protection Law Review 312, 313; Sjaak Nouwt, 'Reasonable Expectations of Geo-Privacy?' (2008) 5 SCRIPT-ed 375, 7–11; Clarke and Wigan (n 18) 142–145; Article 29 Working Party, 'Opinion 13/2011 on Geolocation Services on Smart Mobile Devices' (2011) WP 185 4–6 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf> accessed 3 May 2019.
[271] Katherine M Shelfer and J Drew Procaccino, 'Smart Card Evolution' (2002) 45 Communications of the ACM 83.

holder at the location of the card reader, at the time the card was detected by the reader. Another type of location tracking can be practiced via automated license plate readers, MAC address tracking on Wi-Fi networks and electronic tolling devices,[272] which takes place when the owner of the electronic device or vehicle passes through the location where the sensors are located. Video-analytics enabled surveillance cameras such could also allow location tracking, as these devices could be used to detect the identity of a person and their presence at a specific location at a given time.[273]

The technologies mentioned here, other than personal mobile devices, may not provide meaningful location information unless the collected data is combined with data from other devices placed at other locations. Nevertheless, the speed at which the technology is developing leaves no doubt that such data combination is more than a mere possibility. Considering the proliferation of IoT devices and smart city projects, information about people's movement in space can be easily inferred through these methods.[274]

The 5G technology will increase location detection capabilities.[275] This is due to the reduced penetration capacity of 5G signals, which cannot go through solids as easily as the signals used in 3G or 4G technologies. Due to this reduced penetration capacity, to reach the required coverage levels, a higher number of cellular towers will be required. In the resulting scenario, each cellular tower serves a smaller area, and this facilitates detecting the specific location of each device, through calculating the location of the closest tower.[276] While this aspect may lead to weaker privacy by enhancing surveillance capabilities of telecom operators, 5G has some more privacy-

[272] Eren (n 263) 23–24.

[273] Andrew A Adams and James Ferryman, 'The Future of Video Analytics for Surveillance and Its Ethical Implications' (Social Science Research Network 2012) SSRN Scholarly Paper ID 2174255 <https://papers.ssrn.com/abstract=2174255> accessed 23 April 2019.

[274] David Murakami Wood and Debra Mackinnon, 'Partial Platforms and Oligoptic Surveillance in the Smart City' (2019) 17 Surveillance & Society 176, 13; See also Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2711290 <https://papers.ssrn.com/abstract=2711290> accessed 23 April 2019; de Montjoye and others (n 19).

[275] L Chen and others, 'Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey' (2017) 5 IEEE Access 8956, 8968.

[276] Matthew Kassel, 'As 5G Technology Expands, So Do Concerns Over Privacy' *Wall Street Journal* (New York City, 27 February 2019) <https://www.wsj.com/articles/as-5g-technology-expands-so-do-concerns-over-privacy-11551236460> accessed 12 August 2019; 'Welcome to 5G: Privacy and Security in a Hyperconnected World (or Not?)' (*Privacy International*, 23 July 2019) <http://privacyinternational.org/long-read/3100/welcome-5g-privacy-and-security-hyperconnected-world-or-not> accessed 12 August 2019.

friendly features compared to 4G as well: 5G employs 256-bit encryption for users' identity and location, a feature that the 4G technology lacks.[277]

Location tracking is also considered and used in certain cases to show individuals targeted advertisements or to improve the quality and efficiency of the existing services.[278] A recent example is the project developed by Clear Channel Outdoor, an outdoor advertising company, in Europe, within the scope of which billboards and bus shelters will be equipped with tracking technology that will detect the presence of mobile phones in the proximity.[279] The Financial Times article reporting on the project does not give any further technical details regarding how the tracking will take place other than that the data will be collected via mobile phones and will be anonymised. The company emphasises that the collected data will be fully anonymous and aggregated. This emphasis, however, is not sufficient to dispel concerns about the project's potential for surveillance and privacy violation, since achieving true anonymisation is extremely difficult.[280] Also, a similar project was previously tested in London in 2013 in the form of "tracking bins" where recycling bins were used to track the MAC addresses of the mobile devices of passers-by, yet, the project was terminated due to negative public reaction.[281] Considering the negative impact of COVID-19 on the economy on a global scale, the advertising sector has suffered immensely, and in this sense it may be reasonable for advertising companies to resort to new and potentially more lucrative alternatives. However, widespread tracking like in the project of Clear

---

[277] Andy Purdy, 'Why 5G Can Be More Secure Than 4G' (*Forbes*, 23 September 2019) <https://www.forbes.com/sites/forbestechcouncil/2019/09/23/why-5g-can-be-more-secure-than-4g/> accessed 25 August 2020.

[278] Robert P Minch, 'Location Privacy in the Era of the Internet of Things and Big Data Analytics', *2015 48th Hawaii International Conference on System Sciences* (IEEE 2015) 2 <http://ieeexplore.ieee.org/document/7069994/> accessed 10 August 2019.

[279] Alex Barker, 'Clear Channel to Roll out Billboards "with Brains" in Europe' (*Financial Times*, 10 August 2020) <https://www.ft.com/content/e5c5a996-8d54-4d5c-a5df-a036b5579148> accessed 25 August 2020; Kim Lyons, 'Clear Channel's Billboards Will Start Tracking Consumers in Europe' (*The Verge*, 10 August 2020) <https://www.theverge.com/2020/8/10/21361734/clear-channel-billboards-privacy-ad-tracking-europe> accessed 25 August 2020.

[280] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 UCLA Law Review 1701; AR Beresford and F Stajano, 'Location Privacy in Pervasive Computing' (2003) 2 IEEE Pervasive Computing 46, 48.

[281] Siraj Datoo, 'This Recycling Bin Is Following You' (*Quartz*, 8 August 2013) <https://qz.com/112873/this-recycling-bin-is-following-you/> accessed 10 August 2019; Siraj Datoo and Zachary M Seward, 'City of London Halts Recycling Bins Tracking Phones of Passers-By' (*Quartz*, 12 August 2013) <https://qz.com/114174/city-of-london-halts-recycling-bins-tracking-phones-of-passers-by/> accessed 25 August 2020.

Channel Outdoor or like in the case of tracking bins in 2013 would have major surveillance and privacy concerns and must be approached with absolute caution.

Location tracking has many benefits. It can be helpful in traffic management[282] and crowd management in busy public places like airports, theme parks, concert venues and festival areas, hospitals etc.[283] The COVID-19 crisis has also reminded the benefits of location tracking. On the other hand, while it is beneficial to a certain degree, location data can provide rather intrusive insights into people's private lives, therefore it is quite sensitive and shall be approached with utmost care. Location data presents significant risks even when it is fully anonymised,[284] and it is difficult to effectively anonymise.[285]

In a recent example, openly available location data which was originally collected for advertising purposes was used by researchers from the US to detect the location of drone test facilities and monitor movement in embassies and senate buildings. The data they used was commercially available GPS location data from mobile devices, collected via apps like weather apps and games for advertising purposes.[286] Another significant example where location data was used to gather insights about individuals was the example of Mobilewalla. As mentioned above, during the Black Lives Matter protests in the US at the end of May 2020, many people had their location information unknowingly spied on and analysed by Mobilewalla, a company that profiles users of mobile devices, based on demographics and behaviours, using application and location data obtained from other companies handling vast amounts of data, such as advertisers, data brokers and ISPs.[287]

---

[282] For a relevant example, see Transport for London, 'Oyster Card' (*Transport for London*, February 2019) <https://www.tfl.gov.uk/corporate/privacy-and-cookies/oyster-card> accessed 24 August 2019.

[283] James O'Malley, 'Exclusive: Here's What 3 Big Museums Learn By Tracking Your Phone' (*Gizmodo UK*, 11 April 2017) <https://www.gizmodo.co.uk/2017/04/exclusive-heres-what-museums-learn-by-tracking-your-phone/> accessed 17 August 2019; Ulf Blanke and others, 'Capturing Crowd Dynamics at Large Scale Events Using Participatory GPS-Localization', *2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)* (IEEE 2014) <http://ieeexplore.ieee.org/document/6827652/> accessed 19 August 2019.

[284] For an example on the risks of anonymised location data, see 'The Strava Heat Map Shows Even Militaries Can't Keep Secrets from Social Data' *Wired* <https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/> accessed 25 August 2020 where heat maps indicating the location of people who used a fitness app inadvertently revealed the location of some US military bases.

[285] de Montjoye and others (n 19).

[286] Byron Tau, 'Academic Project Used Marketing Data to Monitor Russian Military Sites' *Wall Street Journal* (20 July 2020) <https://www.wsj.com/articles/academic-project-used-marketing-data-to-monitor-russian-military-sites-11595073601> accessed 25 August 2020.

[287] Haskins (n 20).

Detecting which individuals participate in a protest in this manner could undermine freedom of assembly, expose the protesters to discrimination and create chilling effects on the society as people who know their location will be closely surveilled may refrain from attending protests.

ii. Location Tracking and COVID-19

As the disease COVID-19 has caused a pandemic,[288] governments all around the world were forced to take various measures to fight against it and prevent it from spreading further.[289] Contact tracing, one of the most effective ways of fighting with the disease, has been a subject of attention by the governments and various approaches were developed to perform contact tracing. Contact tracing generally involves tracing the individuals who have contacted an infected person and may be done manually or digitally.

In the EU, a digital contact tracing project aiming to provide a pan-european scheme, called Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), was developed through a collaboration between universities, civil society, and the private sector. The PEPP-PT project is based on analysis of Bluetooth handshakes that are registered when two mobile phones are in proximity of each other.[290] PEPP-PT was criticised for its lack of transparency and for having adopted a centralised approach, where all the collected proximity information would be stored in one centre and which would therefore bear significant privacy risks. Upon criticisms, the PEPP-PT website now states that the project considers two alternatives for the application to be developed, a decentralised and a centralised approach.[291]

Also, academics from 25 countries warned governments about the risks of contact tracing applications that are based on centralised data storage, by publishing a joint statement in April

[288] 'Coronavirus Confirmed as Pandemic by World Health Organization' *BBC News* (11 March 2020) <https://www.bbc.com/news/world-51839944> accessed 2 July 2020.
[289] For more information on policy responses adopted by governments and their impact around the globe, see Albert Meijer and C William R Webster, 'The COVID-19-Crisis and the Information Polity: An Overview of Responses and Discussions in Twenty-One Countries from Six Continents' 32.
[290] Natasha Lomas, 'Europe's PEPP-PT COVID-19 Contacts Tracing Standard Push Could Be Squaring up for a Fight with Apple and Google' (*TechCrunch*) <https://social.techcrunch.com/2020/04/17/europes-pepp-pt-covid-19-contacts-tracing-standard-push-could-be-squaring-up-for-a-fight-with-apple-and-google/> accessed 25 August 2020.
[291] 'Pan-European Privacy Preserving Proximity Tracing (PEPP-PT)' <https://www.pepp-pt.org> accessed 25 August 2020.

2020.[292] The statement emphasises that some types of contact tracing mechanisms may not always be fully accurate, for instance contact tracing via GPS, as the location information collected via GPS is not always accurate. Moreover, it warns that a centralised approach could lead to surveillance and discrimination by the private sector or governments as a result of mission creep, as well as security risks, and loss of trust by the public. All in all, the statement strongly defends a decentralised approach, to be realised in line with the principles of purpose limitation and transparency, and emphasises that any contact tracing app should be voluntary and data should be deleted as soon as the pandemic is over .[293]

Among various efforts for decentralised contact tracing, some noteworthy projects are the Decentralised Privacy-Preserving Proximity Tracing (DP-3T) initiative[294] and Apple and Google's jointly developed "Privacy-Preserving Contact Tracing", which is also based on Bluetooth proximity data.[295] Apple and Google's joint project implemented a software update to enable public health authorities to develop and run contact tracing apps with a decentralised infrastructure. This update does not allow the said apps to send the devices' unique Bluetooth identities to a centralised server.[296]

On the other hand, a centralised approach is still favoured by certain. For instance, the technology branch of the UK's National Health Service (NHS), NHSX, wanted to implement a centralised system to detect fraud in self reporting. The French digital sector ministry is also looking at the centralised system to prevent misuse and attacks by ill-intentioned individuals.[297]

---

[292] 'Contact Tracing Joint Statement' <https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/> accessed 25 August 2020; (as cited in Samuel Stolton, 'EPP Cite Controversial PEPP-PT as Example for Single European COVID-19 App' [*www.euractiv.com*, 21 April 2020] <https://www.euractiv.com/section/digital/news/epp-cite-controversial-pepp-pt-as-example-for-single-european-covid-19-app/> accessed 25 August 2020).

[293] 'Contact Tracing Joint Statement' (n 292).

[294] *DP-3T/Documents* (DP^3T 2020) <https://github.com/DP-3T/documents> accessed 25 August 2020.

[295] Alex Hern and Kari Paul, 'Apple and Google Team up in Bid to Use Smartphones to Track Coronavirus Spread' (*the Guardian*, 10 April 2020) <http://www.theguardian.com/world/2020/apr/10/apple-google-coronavirus-us-app-privacy> accessed 25 August 2020; 'Privacy-Preserving Contact Tracing - Apple and Google' (*Apple*) <https://www.apple.com/covid19/contacttracing> accessed 25 August 2020.

[296] Veale (n 248). Veale also criticises the decentralised contact tracing structure due to undue "infrastructural power" that such apps would confer to big platforms and developers like Google and Apple, as they would be able to develop edge computing solutions on the basis of the collected data even if the data is stored only on devices and not sent to a central server.

[297] ibid; For the French DPA CNIL's commentary on the French contact tracing app, see Commission Nationale de l'Informatique et des Libertés (CNIL), 'Application « StopCovid » : La CNIL Tire Les Conséquences de Ses

Although there are many privacy and security risks, and doubts about their efficiency, [298] contact tracing apps have a significant potential in the fight against the Covid-19 pandemic. The toolbox developed by the European Commission,[299] as well as the standards for "for modelling and predicting the evolution of the virus through anonymised and aggregated mobile location data"[300] could be counted as helpful interventions.

iii. Location Tracking and e-Privacy

Pursuant to Article 9(1) of the e-Privacy Directive, location data can be processed only if it is anonymised or on the basis of the individuals' consent: "*Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service".* To process the said data, users or subscribers shall be fully informed before they give their consent, of the type of location data, the purposes of processing, its duration and if it will be shared with any third parties (Article 9(1) of the e-Privacy Directive).

On the other hand, Member States may introduce exceptions through legislative measures, in specific circumstances listed under Article 15(1) of the e-Privacy Directive. According to Article 15(1) of the e-Privacy Directive, such exceptional measures are possible when they constitute *"a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system[...]*". A public health crisis does fall within the scope of this article; therefore, Member States could introduce legislation that allows for location data processing

Contrôles' (20 July 2020) <https://www.cnil.fr/fr/application-stopcovid-la-cnil-tire-les-consequences-de-ses-controles> accessed 25 August 2020.

[298] Rory Cellan-Jones and Leo Kelion, 'The Great Coronavirus-Tracing Apps Mystery' *BBC News* (22 July 2020) <https://www.bbc.com/news/technology-53485569> accessed 25 August 2020.

[299] Lomas, 'Europe's PEPP-PT COVID-19 Contacts Tracing Standard Push Could Be Squaring up for a Fight with Apple and Google' (n 290).

[300] Samuel Stolton, 'LEAK: EU in Push for Digital Transformation after COVID-19 Crisis' (*www.euractiv.com*, 6 April 2020) <https://www.euractiv.com/section/digital/news/leak-eu-in-push-for-digital-transformation-after-covid-19-crisis/> accessed 2 July 2020.

beyond the remit of Article 9(1) of the e-Privacy Directive. Still, such exceptional measures shall respect the Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms, and shall be "strictly limited to the duration of the emergency at hand".[301] In the meanwhile, in light of the ongoing COVID-19 pandemic, the European Commission has requested telecom operators to provide *"anonymised mobile metadata to help analysing the patterns of diffusion of the coronavirus*".[302] As this request concerns anonymised data, it does not clash with the requirements of Article 9(1) of the e-Privacy Directive; however, the difficulty in true anonymisation remains a concern.

iv. Location tracking in the Draft e-Privacy Regulation

The e-Privacy Regulation aims to regulate location tracking through provisions on metadata. As explained above, the data sent for establishing and maintaining connection in networks, containing unique identifiers like "MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI, the Wi-Fi signal etc."[303] are used to identify electronic devices and therefore their users and to detect their location and movement in space. According to Recital 25 of the draft e-Privacy Regulation, such tracking can be conducted for statistical counting purposes without the end-users' consent, "provided that such counting is limited in time and space to the extent necessary for this purpose".[304] In that case, information about the purposes of the processing, the limits of the tracking and the geographical area should be notified to individuals via adequate information notices.

---

[301] European Data Protection Board, 'Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak.'
<https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf>.

[302] The European Commission, as citedSamuel Stolton, 'LEAK: EU in Push for Digital Transformation after COVID-19 Crisis' (*www.euractiv.com*, 6 April 2020) <https://www.euractiv.com/section/digital/news/leak-eu-in-push-for-digital-transformation-after-covid-19-crisis/ > accessed 2 July 2020. For criticism about telecommunications data sharing, see Privacy International, 'Telecommunications Data and Covid-19' <https://privacyinternational.org/examples/telecommunications-data-and-covid-19> accessed 4 July 2020.

[303] Recital 25 of the draft e-Privacy Regulation (the latest consolidated text of 6 March 2020, see Council 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) (6543/20)' [n 30].

[304] Recital 25 of the draft e-Privacy Regulation (the latest consolidated text of 6 March 2020, see ibid).

If used for more intrusive purposes, such as identifying devices (and therefore the end-users who use the devices) or sending personalized messages to devices, the processing does not fall within the remit of statistical counting. Recital 25 states that commercial messages sent to a person's device when that person enters a store, containing location-based personalized offers or "the tracking of individuals over time, including repeated visits to specified locations" cannot be deemed as statistical counting and has to be conducted on the basis of the individuals' consent or if it is necessary for the provision of the service requested by the individual. In other words, Recital 25 explicitly states that location tracking which goes beyond simple statistical counting cannot be conducted without consent or unless the provision of the service necessitates it.

Another aspect concerning location tracking under the draft e-Privacy Regulation is the introduction of legitimate interests as a legal ground. The latest version of the draft regulation introduced legitimate interest as a legal ground allowing the processing of metadata and location data is a type of metadata. As Recital 17b of the draft e-Privacy Regulation states, one of the purposes of such introduction is to "benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure". On the other hand, introduction of legitimate interests into the text is also criticised because metadata may very well include sensitive personal data. When it comes to sensitive personal data, Article 9 of the GDPR does not allow processing of special categories of personal data on the basis of legitimate interests, whereas the current draft of the e-Privacy Regulation could result in processing, on the basis of legitimate interest, of sensitive personal data contained in metadata.[305] As a result, the current text of the e-Privacy Regulation may result in weaker protection of metadata with sensitive content, compared to the GDPR's standards. However, the Croatian Presidency of the Council seems to have considered this point, as the last paragraph of Recital 17b explicitly states that "A legitimate interest also should not exist if the electronic communications metadata include special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679, unless the conditions of Article 9(2)(g) and (j) of Regulation (EU) 2016/679 are met". Recital 17b also expresses that the interests and fundamental rights and freedoms of the end-user overrides the legitimate interest. Moreover, the Regulation emphasises the necessity for additional conditions and safeguards, such as an impact assessment before

[305] CMS (n 99).

undertaking such processing, and forecloses sharing such metadata with third parties unless anonymised.[306] It has to be noted that all of these aspects will most likely be subject to change, as the regulation is still not finalised. Therefore, PART II of this report will address the issue in greater detail.

C - Next generation profiling tools: Cookie-less tracking

The recent developments in the advertising industry paves the way for tomorrow's cookieless tracking world, which is still a big question mark for many stakeholders in terms of details and technicalities of the cookieless tracking. Cookieless tracking means carrying out tracking activities without using cookies. Although cookies are important in visitors' website experience, the recent changes show that the traditional approach and methods in the online tracking ecosystem are to be changed soon, especially the practice of using third party cookies.[307] Using cookies for tracking purposes means that tracking systems mainly rely on users. This system has considerable flaws in terms of accuracy and precision when delivering ads as well as compelling disadvantages in terms of privacy and security.[308] There are myriad concerns with regards to tracking systems using cookies. The new technologies are expected to address these challenges as much as they can by switching to cookieless systems.[309] Cookieless tracking is regarded as efficient and effective[310] not merely in monitoring users, but also in doing this at a cross-device level as well.[311]

Although the inner workings of the technicalities and details about cookieless tracking systems are still ambiguous in many ways, there are some examples which are being referred to as cookieless tracking. Yet, it is important to note that it would be quite misleading to call examples such as

[306] Recital 17c of the draft e-Privacy Regulation (consolidated text of 6 March 2020, see Council 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) (6543/20)' [n 30]).
[307] 'Cookieless Tracking: Solutions for Accurate Attributions in 2020' (*MobileAds.com*, 30 January 2020) <https://www.mobileads.com/blog/cookieless-tracking> accessed 25 August 2020.
[308] ibid.
[309] ibid.
[310] See for example 'End of Third-Party Cookies Leads to More Effective Data-Driven Marketing' (*RampUp*, 18 May 2020) <https://rampedup.us/end-third-party-cookies-data-driven-marketing/> accessed 25 August 2020.
[311] For details, see 'Cookieless Tracking: Solutions for Accurate Attributions in 2020' (n 307).

Lotame "cookieless tracking" due to the method they are using.[312] However, all stakeholders of the advertising ecosystem are expecting the developments which are yet to come. It is expected that Google[313] can truly develop a method which we could refer to as "cookieless". There are compelling reasons for eliminating cookies and strong and varying implications[314] that are discussed regarding introducing cookieless tracking. Currently, there are some alternatives, for instance, Google's and Criteo's alternative tracking schemes: Google's Turtledove[315] and Criteo's Sparrow.[316] As discussed above, following the developments in the advertising industry, most importantly those introduced by Google, it is expected that concepts such as contextual advertising will become prevalent.

Although details about compliance with the GDPR and ePrivacy laws will be discussed in detail in the PART II of our Report, it is important to note that many believe that not much will change in terms of responsibilities and compliance with the rules set out under the GDPR, even under new schemes that eliminate cookies. It is also argued that such new schemes are designed merely as a way not to obtain consent, considering the problematic nature of consent in today's online advertising ecosystem.[317] In short, it can be concluded that there are still grey areas about the

---

[312] For details, see Adam Solomon, 'Fact Check Series: Cookieless Meets Truthfulness' (*Lotame*, 17 September 2019) <https://www.lotame.com/fact-check-series-cookieless-meets-truthfulness/> accessed 25 August 2020.

[313] For details about the developments and GDPR rules on consent, see Helge Klein, 'Google Analytics: Cookieless Tracking Without GDPR Consent' (8 June 2020) <https://helgeklein.com/blog/2020/06/google-analytics-cookieless-tracking-without-gdpr-consent/> accessed 25 August 2020; for developments and news concerning Google and cookieless tracking see 'Cookieless Web: 3 Areas To Watch In The Second Half Of 2020' (n 163); Frederic Lardinois, 'Google Rolls Back SameSite Cookie Changes to Keep Essential Online Services from Breaking' (*TechCrunch*, 3 April 2020) <https://social.techcrunch.com/2020/04/03/google-rolls-back-samesite-cookie-changes-to-keep-essential-online-services-from-breaking/> accessed 25 August 2020; Justin Schuh, 'Temporarily Rolling Back SameSite Cookie Changes' (*Chromium Blog*) <https://blog.chromium.org/2020/04/temporarily-rolling-back-samesite.html> accessed 25 August 2020; 'Chrome Cookie Tracking Changes 2020' (n 157).

[314] See for example Edelman (n 223).

[315] Johnny Ryan, 'Diagram of Google's Turtledove' (*Twitter*, 30 June 2020) <https://twitter.com/johnnyryan/status/1277896292262428672> accessed 25 August 2020; for further details, see *WICG/Turtledove* (Web Incubator CG 2020) <https://github.com/WICG/turtledove> accessed 25 August 2020.

[316] Johnny Ryan, 'Diagram of Criteo's Sparrow' (*Twitter*, 30 June 2020) <https://twitter.com/johnnyryan/status/1277898759633076226> accessed 25 August 2020; For further details of the project, see *WICG/Sparrow* (Web Incubator CG 2020) <https://github.com/WICG/sparrow> accessed 25 August 2020.

[317] Wolfie Christl, 'On Lotame's Blog Post on Twitter' (*Twitter*, 3 July 2020) <https://twitter.com/WolfieChristl/status/1279023708955344896> accessed 25 August 2020; Wolfie Christl, 'On Lotame's Blog Post on Twitter - 2' (*Twitter*, 3 July 2020) <https://twitter.com/WolfieChristl/status/1279027578578317313> accessed 25 August 2020; For details about the developments and GDPR rules on consent, see Klein (n 313).

application of cookieless tracking, the rationale behind it and its implications. PART I of this Report briefly introduces the concept of cookieless tracking yet leaves the discussions surrounding its practical and legal implications to the PART II.

D - Debates/Challenges

i. Tracking/Cookie Walls and Forced Consent

Some websites have adopted a practice where to access the content of a website the visitors are forced to consent to tracking via cookies or similar technologies such as browser fingerprinting or tracking pixels explained above. Unless they give consent, they are either not allowed to view the contents of the page or their browsing experience is significantly inconvenienced. The practice of forcing users to consent to tracking in this manner is termed a "cookie wall" or "tracking wall" and has been a constant subject of debate. The main questions surrounding the issue were whether the e-Privacy Directive or the GDPR governs such processing through cookies, and whether the applicable legislation permits such consent practices. If the e-Privacy Directive and/or the GDPR is applicable, then consent would need to be interpreted pursuant to the GDPR, through the e-Privacy Directive's reference to the Directive 95/46/EC (Art. 2(f) of the e-Privacy Directive), which is now replaced by a reference to the GDPR (Art. 94(2) of the GDPR). Accordingly, GDPR's Articles 4(11) and 7 apply, which prohibit forced consent and deem consent that is obtained without complying to the rules set out under the GDPR "invalid".

It is open to discussion what constitutes "forced" consent. Advertising networks, publishers, stakeholders who rely mainly on online advertising to support their business model are of the view that cookie walls would not result in "forced" consent and that they are not prohibited under the applicable law. Specifically, one interpretation that is used in support of this argument is that the wording of Recital 25 of the e-Privacy Directive allows for cookie walls,[318] which reads as follows:

> *"Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose."*

[318] Natasha Lomas, 'Cookie Walls Don't Comply with GDPR, Says Dutch DPA' (*TechCrunch*, 8 March 2019) <https://social.techcrunch.com/2019/03/08/cookie-walls-dont-comply-with-gdpr-says-dutch-dpa/> accessed 25 August 2020.

Recital 25 raises questions, especially considering the requirement for consent to be freely given. When faced with a cookie wall, users have no choice but to accept the processing in order to access the content. This condition prevents the consent from being freely given.[319] Correspondingly, Article 29WP has suggested this recital to be reviewed or clarified.[320]

> *"In the 29WP (WP 240) understanding, these take it or leave it approaches rarely meet the requirements for freely given consent. It specifically stated that 'if the consequences of consenting undermine individuals' freedom of choice, consent would not be free."*[321]

In this context, the EDPB's recently updated guidelines on consent provide guidance for the application of consent-related clauses under the e-Privacy Regulation.[322] The EDPB clearly states that consent given in the face of a cookie wall is not freely given,[323] therefore is invalid, unless a viable alternative which would allow visiting the website or using the service is presented. Scrolling through a web page does not constitute consent, either, as it could easily be mixed with other activities and does not satisfy the conditions provided under the GDPR for valid consent.[324]

Following the EDPB's updated guidelines, the Spanish DPA also updated its cookie guidelines in July 2020, with the participation of various stakeholders from the online advertising sector. Previously, the Spanish DPA was one of the few DPAs that had not presented a clear opinion on the issue of cookie walls; however, its updated guidelines follow the EDPB's guidelines, stating that scrolling does not constitute consent and cookie walls cannot be used to obtain consent as such

---

[319] Santos, Bielova and Matte (n 102) 25; Frederik J Zuiderveen Borgesius and others, 'Tracking Walls, Take-It-or-Leave-It Choices, the GDPR, and the EPrivacy Regulation' (2017) 3 European Data Protection Law Review (EDPL) 353; for the opposite view, see Ronald Leenes, 'The Cookiewars: From Regulatory Failure to User Empowerment?' [2015] The Privacy & Identity Lab: 4 years later 31.

[320] Article 29 Data Protection Working Party, 'Opinion 8/2006 on the Review of the Regulatory Framework for Electronic Communications and Services, with Focus on the EPrivacy Directive (WP 126)' (2006) 3 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp126_en.pdf> accessed 25 August 2020.

[321] 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' 75, 25.

[322] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679 - Version 1.1' (2020).

[323] ibid 40.

[324] ibid 86.

consent would not be freely given. The Spanish DPA allowed for a three-months long transition process, until 31 October 2020, for the companies to implement the new guidelines.[325]

In addition to the EDPB and the Spanish DPA, the Dutch, French, German, Danish, Greek, Irish and Belgian DPAs support this view, as well as the European Consumer Organisation (BEUC) and the EU Parliament. On the opposite corner is the Austrian DPA, according to whom consent obtained via tracking/cookie walls constitute valid consent,[326] though it remains to be seen if they will revise this opinion following EDPB's guidelines.

The British DPA, the Information Commissioner's Office (ICO) is yet to present a clear or final opinion on the matter. It seems to have a rather flexible approach, which resulted in "differing opinions as well as practical considerations around the use of partial cookie walls".[327] The ICO's approach is similar and in parallel with the view of the Federation of European Direct and Interactive Marketing (FEDMA) that cookie consent should not focus on GDPR level consent that "is likely to have a strong impact on user's experience (consent fatigue). The general approach of the Article could be rethought more in line with the risk-based approach of the GDPR".[328] Although these concerns exist, after the Planet49 decision, as explained above in Section II(A)(ii) under the subheading "Cookie wars", the CJEU's position is now "fully aligned with the current consent regime under GDPR and the mirroring consent provisions of the latest proposed draft of the e-Privacy Regulation".[329]

Regarding the issues concerning consent, there are compelling arguments with regards to rules relating to consent as well as its implementation. For instance, Bietti argues that consent practices

---

[325] Agencia Española de Protección de Datos, 'Guía sobre el uso de las cookies' (2020); Agencia Española de Protección de Datos, 'La AEPD actualiza su Guía sobre el uso de cookies para adaptarla a las nuevas directrices del Comité Europeo de Protección de Datos' (*AEPD*, 28 July 2020) <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-actualiza-guia-cookies> accessed 25 August 2020.

[326] Santos, Bielova and Matte (n 102) 27–29.

[327] Information Commissioner's Office and Ali Shah, 'Blog: Cookies – What Does "Good" Look Like?' (3 July 2019) <https://ico.org.uk/about-the-ico/news-and-events/blog-cookies-what-does-good-look-like/> accessed 25 August 2020.

[328] Ropes & Gray LLP and Rohan Massey, 'Cookies and Consent - An Update on Developments in the EU's Draft e-Privacy Regulation' (3 October 2019) <https://www.lexology.com/library/detail.aspx?g=5df3464a-65ed-4da7-bebc-b3ceca7a51c5> accessed 26 August 2020.

[329] Ropes & Gray LLP and Rohan Massey, 'Cookies And Consent – An Update On Developments In The EU's Draft e-Privacy Regulation - Privacy - European Union' (14 October 2019) <https://www.mondaq.com/unitedstates/privacy-protection/853504/cookies-and-consent-an-update-on-developments-in-the-eu39s-draft-e-privacy-regulation> accessed 26 August 2020.

in today's platform economy are not only insufficient, but also "positively harmful".[330] She contends that the perspective which focuses on "voluntariness and disclosure such as the ones generally adopted by regulators and courts fail to account for the systemically unjust background conditions within which voluntary individual acts of consent take place".[331]

On the other hand, it is also believed that the main problem with the issues related to consent do not stem from the notion of consent under the legal framework, but from the lack of implementation of the existing legal framework and the problems faced in its application. Put differently, this view argues that the consent rules in the EU describe the ideal practices, which, if fully respected, would allow individuals to enjoy their rights and freedoms in a system where their autonomy is protected. Accordingly, the problem is not the existing laws or rules themselves but rather their implementation and the lack of action by the DPAs.

- **CNIL's (National Data Protection Commission, Commission National d'Informatique et des Libertés) cookie guidelines and the ban on cookie walls**

The French DPA CNIL's cookie guidelines[332] adopted on 19 July 2019, repeals CNIL's previous guidelines from 2013 and clarifies consent requirements under Article 82 of the French Data Protection Act, concerning the implementation of cookie rules under the e-Privacy Directive.[333] Accordingly, in order to set non-essential cookies, end-users shall actively give their consent after being informed of the standards provided under Articles 4(11) and 7 of the GDPR, and simply continuing to browse a website or pre-ticked boxes do not constitute valid consent. The guidelines also prohibit cookie walls in its Article 2, on the grounds that consent cannot be freely given in the existence of a cookie wall. Considering that the CNIL's guidelines were adopted before EDPB's

[330] Elettra Bietti, 'Consent as a Free Pass: Platform Power and the Limits of the Informational Turn' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3489577 <https://papers.ssrn.com/abstract=3489577> accessed 25 August 2020.
[331] ibid.
[332] Commission Nationale de l'Informatique et des Libertés, 'Délibération N° 2019-093 Du 4 Juillet 2019 Portant Adoption de Lignes Directrices Relatives à l'application de l'article 82 de La Loi Du 6 Janvier 1978 Modifiée Aux Opérations de Lecture Ou Écriture Dans Le Terminal d'un Utilisateur (Notamment Aux Cookies et Autres Traceurs) (Rectificatif)' <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337> accessed 25 August 2020.
[333] Latham & Watkins LLP, 'France's CNIL Publishes New Guidance on Cookies' (*Global Privacy & Security Compliance Law Blog*, 7 August 2019) <https://www.globalprivacyblog.com/security/frances-cnil-publishes-new-guidance-on-cookies/> accessed 25 August 2020.

updated guidelines on consent, an explicit prohibition of cookie walls was a significant step that led to much outcry from various actors in the online advertising sector: several professional associations (including, among others, Interactive Advertising Bureau (IAB) France, the Mobile Marketing Association France, the Federation of E-Commerce and Distance Selling federation (FEVAD), the Internet Companies Syndicate (SRI)) sought before the French Council of State the annulment of the said guidelines, arguing the CNIL has exceeded its authority by imposing strict rules and prohibiting cookie walls.

On 19 June 2020, the Council of State declared that, by prohibiting cookie walls on the basis of the freely-given consent requirement under the GDPR, CNIL has exceeded its powers, which are limited to making non-binding regulations or legal instruments.[334] According to the Council of State, the CNIL should have simply reminded that the EDPB finds cookie walls to be unlawful under the GDPR, rather than giving the opinion of the EDPB a binding quality.[335] Nevertheless, the Council of State stated that, considering that the GDPR is supposed to remain a flexible body of law, the CNIL does not have the authority to prohibit cookie walls, especially not by way of issuing guidelines.[336] On the other hand, with regard to other disputed aspects addressed by the guidelines, such as the requirements for the consent to be valid, information obligations as well as the time limits for the cookies set without obtaining the end-users' consent, the Council of State rejected the applicants' requests and stated that the CNIL has not exceeded its powers but only clarified the relevant legislation.[337]

On the same date, on 19 June 2020, the Council of State decided on another significant matter relating to freely given consent in online advertising, confirming the CNIL's decision of 21

[334] *Décision du Conseil d'État, 19 juin 2020, Lignes directrices de la CNIL relatives aux cookies et autres traceurs de connexion*.
[335] ibid 9.
[336] ibid 10.
[337] ibid 11–17.

January 2019[338] to fine Google 50 million Euros.[339] The original complaint against Google before the CNIL, which culminated in this 50 million Euro fine, concerned the lack of a valid legal ground for data processing conducted by Google especially with regard to personalized advertisements in Android devices. The CNIL had taken up the issue upon the complaints of the organisations None Of Your Business ("NOYB") and La Quadrature du Net ("LQDN"). Following its examination, the CNIL had issued the fine on the grounds that Google failed to provide adequate transparency, did not inform its users to the standards expected by the GDPR (particularly concerning the data retention periods and the purposes of data processing), and, failed to obtain the freely-given and informed consent of its users for personalised advertising practices on Android devices.

Google objected to the CNIL's decision, among others, on the grounds that it did not have jurisdiction to address this matter, since Google's European headquarters was in Ireland, making the Irish DPA competent. The CNIL found itself competent after exchanging views with the Irish DPA, due to the fact that Google's Irish headquarters did not have the decision-making authority over other European branches of Google: *"the Irish establishment did not have a decision-making power on the processing operations carried out in the context of the operating system Android and the services provided by GOOGLE LLC, in relation to the creation of an account during the configuration of a mobile phone"*.[340] The CNIL's point was that the one-stop shop mechanism does not apply because the decision making by Google takes place in California, not in Europe, resulting in every European DPA being competent. In this context, it does not make a difference whether Google has moved its main establishment to Ireland.

---

[338] *Décision du Conseil d'État, 19 juin 2020, Sanction infligée à Google par la CNIL*; Commission Nationale de l'Informatique et des Libertés, 'Délibération SAN-2019-001 Du 21 Janvier 2019' <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1> accessed 25 August 2020; 'Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 Pronouncing a Financial Sanction against GOOGLE LLC.' 29; Commission Nationale de l'Informatique et des Libertés, 'The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC' (21 January 2019) <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc> accessed 25 August 2020.

[339] Gaspard Sebag, 'Google Loses $56 Million Fight in French Test of EU Privacy Law' (19 June 2020) 56 <https://www.bloombergquint.com/amp/onweb/google-loses-56-million-fight-in-french-test-of-eu-privacy-law> accessed 25 August 2020.

[340] Commission Nationale de l'Informatique et des Libertés, 'The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC' (n 338).

The Council of State agreed with the CNIL, stating that, on the contrary of Google's arguments, the CNIL had the jurisdiction to address the issue and was correct in its observations. Moreover, the Council of State confirmed that the fine of 50 million Euros was appropriate considering the gravity of Google's practices and their duration, as well as Google's financial status and power. This decision's importance lies in the fact that it confirms the CNIL's observations regarding Google's consent practices, and that Google indeed did not obtain freely given and informed consent of its users for personalised advertising on Android devices.

- **The draft e-Privacy Regulation and cookie walls**

When it comes to the draft e-Privacy Regulation, it has to be noted that the first draft of the European Parliament, dated 26 October 2017, introduced a ban on tracking walls in Articles 8(1)(1)(b) and Recital 22. However, that first draft has undergone many changes since 2017 and most recently, the draft text proposed by the Finnish Presidency in 2019 introduced the idea of tracking walls being lawful, especially for advertising purposes.[341]

Although in an indirect manner, Recital 21 of the Finnish draft of the ePrivacy Proposal of 2019 presents the idea of legitimizing tracking walls for advertising. This referral shows that it is a controversial topic in the context of politics among the stakeholders. This draft marks that consent can be considered valid when the data processing related to a service the user requested is conducted for the purpose of advertising. [342]

Moreover, according to Recital 21(b) of the draft e-Privacy Regulation, legitimate interest can be used as "a legal basis to use processing and storage capabilities of terminal equipment or to collect information from an end-user's terminal equipment", by service providers which have a role in the protection of freedom of expression and information, such as online newspapers, and which finance their services through advertising. The Recital states that end-users should be informed about the details and purposes of such processing and accept it. If this version of the regulation becomes final, it would be possible to have tracking walls on websites.[343] More details about the

[341] Santos, Bielova and Matte (n 102) 63–64.
[342] ibid.
[343] ibid.

legitimate interest as a legal ground under the e-Privacy Regulation can be found below in subsection D(iii).

Borgesius, LIBE Report from 2017, talks about blacklisting/grey listing certain uses of tracking walls and underscores four points by making suggestions about "location tracking"; "browsers and default settings"; "tracking walls"; and "the confidentiality of communications".[344] Borgesius contends that regarding these four points, the ePrivacy proposal fails to provide adequate protection of the right to privacy and confidentiality of communications and that "some provisions in the ePrivacy proposal offer less protection than the GDPR".[345]

Article 29 WP has a similar opinion as it states that forced consent shall be prohibited in five circumstances, more specifically in the following circumstances:

> "*(1) Tracking on websites, apps and or locations that reveal information about special categories of data (health, political, sexual, trade union etc.). Even if visits to services providing information about such special categories of data do not disclose in themselves special categories of data about these users, there is a high impact on the private life of those users if they are labelled as being interested in such information; (2) Tracking by unidentified third parties for unspecified purposes. This is for example the case when a website or app auctions its advertising space, and unknown third parties may actually start to track the users through the website or app; (3) All government funded services; (4) All circumstances identified in the GDPR that lead to invalid consent, such as for example an unequal balance of power, if there is no equivalent alternative, or forced consent is part of a contract; (5) Bundled consent for processing for multiple purposes. Consent should be granular*".[346]

ii. **Do-Not-Track signals**

The first draft of the e-Privacy Regulation included an article that required the browsers to present their users the first moment they were using the browser with an option to opt-out from tracking.

---

[344] Zuiderveen Borgesius and others (n 37) 8–9.
[345] ibid 8.
[346] Article 29 Data Protection Working Party, 'Opinion 03/2016 on the Evaluation and Review of the EPrivacy Directive (2002/58/EC) (WP 240)' (n 118) 17.

Even that version of the Article was criticised, suggesting that every browser should by default not track its user, unless the user explicitly opts-in to it,[347] but it would still improve user privacy. Unfortunately, later on Article 10 was completely deleted from the draft Regulation.[348]

Signalling consent through browser settings may not be appropriate, as it would hardly comply with the legal requirements of valid consent. On this point, Santos et al. opine that browser settings fail to meet the requirements of valid consent because the purposes of processing are not specified, the settings cannot ensure that the user is informed and they do not provide a sufficient method to express an unambiguous consent.[349] Furthermore, they do not agree with the Article 29 WP's statement that browser settings could be regarded as a mechanism for expressing consent, especially if the settings are presented in an unambiguous way. Santos et al. ground their disagreement on the fact that "many browser vendors expose cookie settings in browser preferences that are hard to find".[350] In addition, it is important to note that "the location and user interface of such cookie settings changes significantly from one version of the browser to another" and also because cookie settings might not work on all tracking technologies. For instance, because there is no exact way to identify browser fingerprinting and furthermore, "the purpose of such fingerprinting is not known, browser preferences are not a meaningful control mechanism for this tracking technology".[351] Although the technology signalling that a user does not want cookies placed on their device, namely Do-Not-Track signals, have existed for a long time now, it was never mandatory for software developers to provide the Do-Not-Track option and when they did, many websites did not respect users' choice not to receive cookies.

The e-Privacy Regulation had originally included an Article 10 which introduced a mandatory Do-Not-Track signal option for software.[352] According to the Article, this option would be presented to users upon installation, in line with the privacy by design and default principles adopted by the GDPR, and would be an important step towards resolving the ever-present problem of consent

[347] Zuiderveen Borgesius and others (n 37) 9.
[348] Johnny Ryan, 'Brave Writes to All European Governments to Press for Strong EPrivacy Protections' (*Brave Browser*, 10 October 2019) <https://brave.com/eprivacy-october2019/> accessed 26 August 2020.
[349] Santos, Bielova and Matte (n 102) 8.
[350] ibid.
[351] ibid.
[352] Ryan, 'Brave Writes to All European Governments to Press for Strong EPrivacy Protections' (n 348).

fatigue. Still, the suggested article was not perfect, it was criticised even in its original form and suggestions were made for the Article to require for the browsers not to track users by default and provide them with an option to opt-in to tracking.[353] In LIBE Report, Borgesius states that *"Browsers, default settings, and Do Not Track Article 10 does not offer sufficient privacy protection"* and that Article 10 provides that *"browsers and similar software should offer people the option to allow or reject third party tracking (internet-wide tracking)".*[354] It is important to note that the provision previously prescribed browsers to have privacy-friendly settings by default. As Borgesius points out, it is far from easy to reconcile Article 10 with the GDPR as the GDPR sets out rules that require data protection by design and by default. Accordingly, EU legislators are recommended to employ privacy by design approach and that browsers as well as similar software should adopt privacy friendly settings by default which puts limits to online tracking.[355] Furthermore, it is suggested that there be a requirement for Do Not Track or any other similar standard in order to comply with the rules since such a requirement would allow individuals *"to signal with their browser that they do not want to be tracked"*.[356] Another important point made in the LIBE Report concerns the non-discriminatory application of Do-Not-Track, in other words, it is believed that Do-Not-Track application should be technology neutral and also encapsulate cookies and device fingerprinting.[357] Lastly, as the Report underscores it goes without saying that *"the standard should be user-friendly, and be backed by law and proper enforcement".*[358]

These suggestions could have been helpful to improve the proposed Article 10. Unfortunately, Article 10 was later on completely deleted from the draft during the Council discussions due to the Austrian Presidency's suggestion for deleting this article on the basis that it would create further consent fatigue - an argument which is quite difficult to agree with.[359] The deletion of Article 10 is clearly a missed opportunity to solve the consent fatigue problem and undermines the aim to provide more efficient choice and protection to individuals.

[353] Zuiderveen Borgesius and others (n 37) 9.
[354] ibid.
[355] ibid.
[356] ibid.
[357] ibid.
[358] ibid.
[359] See also Zuiderveen Borgesius and others (n 319).

iii. Introduction of legitimate interests as a ground for processing of electronic communications data, including both content and metadata

As addressed above in section B(iii) on location tracking and e-Privacy, as well as in section D(i) on the draft e-Privacy Regulation and cookie walls, the Croatian Presidency of the Council of the European Union introduced legitimate interests as a legal ground for processing.

According to Recital 17b of the latest consolidated text of the draft e-Privacy Regulation, one of the purposes of such introduction is to "benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure". While it may be beneficial in this sense, the introduction of legitimate interests into the text is also criticised because metadata may very well include sensitive personal data, and when it comes to sensitive personal data, Article 9 of the GDPR does not allow processing of special categories of personal data on the basis of legitimate interests. In light of this, the current draft of the e-Privacy Regulation could result in the processing, on the basis of legitimate interest, of sensitive personal data contained in metadata.[360] As a result, the introduction of legitimate interests as a legal ground for processing metadata into the e-Privacy Regulation would result in weaker protection of metadata with sensitive content, compared to the GDPR. As pointed out by the former Bulgarian Presidency, considering the sensitive nature of the communications data, a wider and non-specific provision like the legitimate interest ground in the current draft that allows processing of communications data would violate the case-law of the CJEU.[361] The EDPB had also made an explicit statement in this regard, in its statement of 25 May 2018:

> *"[T]here should be no possibility under the ePrivacy Regulation to process electronic communications content and metadata based on open-ended grounds, such as 'legitimate interests', that go beyond what is necessary for the provision of an electronic communications service."* [362]

[360] CMS (n 99).

[361] 'EU Council Considers Undermining EPrivacy' (*EDRi*, 25 July 2018) <https://edri.org/eu-council-considers-undermining-eprivacy/> accessed 26 August 2020.

[362] 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/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf> accessed 26 August 2020.

The introduction of legitimate interests into the draft e-Privacy Regulation is criticised also on the grounds that it "has turned the ePrivacy reform into a surveillance tool," creating a "blatant disregard for fundamental rights".[363]

The Croatian Presidency seems to have introduced safeguards to combat such concerns and criticisms. For instance the final paragraph of Recital 17(b) states that *"A legitimate interest [...] should not exist if the electronic communications metadata include special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679, unless the conditions of Article 9(2)(g) and (j) of Regulation (EU) 2016/679 are met"*. Moreover, the same paragraph states that *"[S]uch metadata should not be used to determine the nature or characteristics of an end-user or to build an individual profile of an end-user. In such usage cases, the end-user's interests and fundamental rights and freedoms override the interest of the service provider, as such processing operations can seriously interfere with one's private life, for instance when used for segmentation purposes, to monitor the behaviour of a specific end-user or to draw conclusions concerning her or his private life"*. In addition, the Regulation emphasises the necessity of extra conditions and safeguards, such as an impact assessment before undertaking such processing, and forecloses sharing such metadata with third parties unless anonymised.[364]

According to Recital 21b of the e-Privacy Regulation, legitimate interest can be used as "a legal basis to use processing and storage capabilities of terminal equipment or to collect information from an end-user's terminal equipment", by service providers which have a role in the protection of freedom of expression and information, such as online newspapers, and which finance their services through advertising. The recital states that end-users should be informed about the details and purposes of such processing and accept it. The wording of this part of Recital 21b about end-users accepting the processing may be problematic, as it seems to confuse legitimate interest with consent. And another potential problem with this term is that, while consent is subject to GDPR standards, the standards this "acceptance" will need to comply with are far from being clear.

---

[363] Statement by Estelle Masse, as reported in Jennifer Baker, 'Critics on Croatia's EPrivacy Proposal: Legitimate Interest Provisions Not Legitimate' (25 February 2020) <https://iapp.org/news/a/critics-on-croatias-eprivacy-proposal-legitimate-interest-provisions-not-legitimate/> accessed 26 August 2020.

[364] Recital 17c of the draft e-Privacy Regulation (consolidated text of 6 March 2020, see Council 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) (6543/20)' [n 30]).

Moreover, like the last paragraph of Recital 17(b), the last paragraph of Recital 21(b) states that legitimate interests should not be used as a legal ground for processing activities where the end-users are profiled and if the information includes special categories of personal data. Most online behavioural advertising would fall under this category; therefore, it would not be possible to use legitimate interest as the legal ground for this type of advertising. This point seems to be aimed at providing relief in the face of concerns from various stakeholders.

The Croatian Presidency may have aimed to protect online newspapers by introducing this recital, since online newspapers mostly rely on advertising to survive. However, considering that the advertising methods they most frequently use involve profiling of individual users and inferring sensitive information about their private lives, this recital could easily fail to achieve its intended purpose.[365]

Within the main body of the text, Article 6b(e) introduces legitimate interests of the provider of the electronic communications service or network as a legal ground to process electronic communications metadata. However, as mentioned in Recital 17(b), the fundamental rights and freedoms of the end-user is a limiting factor: Article 6b(e) clearly stipulates that processing of metadata is only allowed as long as the end-user's interests or fundamental rights and freedoms do not override the interests of the service or network provider.[366] Moreover, second paragraph of the same subclause clarifies that if the end-user will be profiled through processing the metadata, or if their behaviour and characteristics will be deducted from the metadata, the legitimate interests of the service or network provider will be automatically overridden and it will not be possible to process the metadata on the basis of this legal ground.

Legitimate interest is also included in Article 8(1)(g) as a legal ground for the processing of the information stored in the end-user's terminal equipment. In line with Article 6b(e), such processing is allowed if "*it is necessary for the purpose of the legitimate interests pursued by a service*

[365] For further criticisms and views on the introduction of legitimate interests as a legal ground in the draft e-Privacy Regulation by various stakeholders, see Baker (n 363).

[366] See Recital 17b of the draft e-Privacy Directive (consolidated text of 6 March 2020) also for specific examples indicating where processing may be grounded legitimate interest. Council 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) (6543/20)' <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6543_2020_INIT&from=EN> accessed 30 June 2020.

provider to use processing and storage capabilities of terminal equipment or to collect information from an end-user's terminal equipment, except when such interest is overridden by the interests or fundamental rights and freedoms of the end-user". The article states, in the following paragraph, that if the end-user is a child or if the processing aims to *"determine the nature and characteristics of the end-user or to build an individual profile of the end-user or the processing, storage or collection of the information by the service provider contains special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679"*, then the interests of the end-user will override the interests of the service provider.[367]

It has to be noted that all of the above-mentioned aspects will most likely be subject to change, as the regulation is still far from being finalised. The current text of the draft regulation has become significantly more complex and has drawn major criticisms, considering the reduced level of protection compared to the European Parliament's position.[368] In light of potential changes to be made by the German Presidency, PART II of this report will address the issue with more clarity and detail.

iv. Online child abuse and e-privacy

Children spending time online unsupervised is a necessity for them to learn how to navigate the online environment, to participate in different communities, find creative outlets and communicate with their peers. However, it also leaves them open to risky situations, one of which is online sexual abuse.[369] The Covid-19 crisis has aggravated this risk, as children are spending more time online than ever and doing so in physical isolation. In response to the aggravated situation, the European Commission introduced an initiative titled "EU strategy for a more effective fight against child abuse". Within this framework, the Commission announced that they will "propose

[367] Article 8(1)(g) of the draft e-Privacy Regulation (consolidated text of 6 March 2020).
[368] Baker (n 363).
[369] European Commission, 'Communication From The Commission To The European Parliament, The Council, The European Economic and Social Committee and the Committee of The Regions EU Strategy for a More Effective Fight against Child Sexual Abuse (COM(2020) 607 Final)' 1 <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf> accessed 26 August 2020.

legislation to require online platforms to detect and report sharing of" online child abuse material.[370]

In its strategy, the European Commission states that in a first stage, the Commission aims to *"propose the necessary legislation to ensure that providers of electronic communications services can continue their current voluntary practices to detect in their systems child sexual abuse after December 2020".*[371] Furthermore, in a second stage, the Commission states that it aims to *"propose the necessary legislation to tackle child sexual abuse online effectively including by requiring relevant online services providers to detect known child sexual abuse material and require them to report that material to public authorities".*[372]

An important issue to consider when it comes to online child abuse and e-privacy is end-to-end encryption[373] and how it may prevent online platforms from detecting and reporting the majority of the child abuse cases.[374] In addition, under the EU Internet Forum, the Commission launched an expert process with industry to map and assess and address challenges stemming from the complexities of the online ecosystem and find potential *"technical solutions to detect and report*

[370] European Commission, 'Delivering on a Security Union: Initiatives to Fight Child Sexual Abuse, Drugs and Illegal Firearms' (*European Commission - European Commission*, 24 July 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1380> accessed 26 August 2020.

[371] European Commission, 'Communication From The Commission To The European Parliament, The Council, The European Economic and Social Committee and the Committee of The Regions EU Strategy for a More Effective Fight against Child Sexual Abuse (COM(2020) 607 Final)' (n 369) 6.

[372] ibid.

[373] For concerns, see for example Priti Patel, William Barr, Kevin McAleenan, Peter Dutton, 'Open Letter from the Home Secretary - alongside US Attorney General Barr, Secretary of Homeland Security (Acting) McAleenan, and Australian Minister for Home Affairs Dutton - to Mark Zuckerberg' (*GOV.UK*, 23 December 2019) <https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg/open-letter-from-the-home-secretary-alongside-us-attorney-general-barr-secretary-of-homeland-security-acting-mcaleenan-and-australian-minister-f> accessed 26 August 2020.

[374] Hany Farid, 'Briefing: End-to-End Encryption and Child Sexual Abuse Material' <https://5rightsfoundation.com/uploads/5rights-briefing-on-e2e-encryption--csam.pdf>; Jennifer Valentino-DeVries and Gabriel JX Dance, 'Facebook Encryption Eyed in Fight Against Online Child Sex Abuse - The New York Times' (*The New York Times*, 2 October 2019) <https://www.nytimes.com/2019/10/02/technology/encryption-online-child-sex-abuse.html> accessed 26 August 2020; NCMEC, 'End-to-End Encryption: Ignoring Abuse Won't Stop It' (3 October 2019) <https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption> accessed 26 August 2020; NCMEC, 'End-to-End Encryption' <https://www.missingkids.org/theissues/end-to-end-encryption> accessed 26 August 2020; 'Facebook Urged to Halt Encryption Plans over Child Abuse Risks' <https://www.ft.com/content/feda422a-483a-11ea-aeb3-955839e06441> accessed 26 August 2020.

child sexual abuse in end-to-end encrypted electronic communications, and to address regulatory and operational challenges and opportunities in the fight against these crimes."[375]

The topics of prevention of child sexual abuse is also debated under the draft e-Privacy Regulation. The current draft includes in its Article 6(d) the prevention of child sexual abuse as a legal ground for processing of electronic communications data, which seems to be a positive development for the protection of children. Still, it is criticised on the basis that processing of more electronic communications data will widen the attack surface and weaken the security of electronic communications.[376]

Although there is no doubt that steps should be taken for contributing to the global fight against online child abuse and that there is a need for more precise and effective legal framework and accordingly there was consensus that this issue should be addressed, numerous stakeholders had different views with regards to how it should be done. More specifically, there were differing opinions about addressing challenges in a separate legislation or rather introducing "a permanent legal ground allowing the processing of electronic communications data for the purpose of preventing child abuse".[377] During the discussions under the Finnish Presidency, a permanent legal ground was introduced in Article 6(d) of the draft e-Privacy Regulation.[378]

Moreover, it is important to note that numerous stakeholders argued against Article 6(d) regarding the processing of electronic communications data to prevent child sexual abuse contending that it could create vulnerabilities, especially when it comes to securing electronic communications.[379] EDRi's commentary supports this view, stating that this possibility could lead to more surveillance and therefore work against the main purpose of the e-Privacy Regulation to protect privacy and

---

[375] European Commission, 'Communication From The Commission To The European Parliament, The Council, The European Economic and Social Committee and the Committee of The Regions EU Strategy for a More Effective Fight against Child Sexual Abuse (COM(2020) 607 Final)' (n 369) 17.

[376] Stefano Leucci and Sofia Dilinois in 'EDPS Workshop Highlights Importance of Encryption and Weaknesses in Proposed E-Privacy Rules, FLECEP20200063 (Unpublished)' 2–3.

[377] Council 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) - Progress Report (14447/19)' 4, para 6 <https://data.consilium.europa.eu/doc/document/ST-14447-2019-INIT/en/pdf> accessed 26 August 2020.

[378] ibid.

[379] See statement by Leucci, from Nexa Centre for Internet and Society, in 'EDPS Workshop Highlights Importance of Encryption and Weaknesses in Proposed E-Privacy Rules, FLECEP20200063 (Unpublished)' (n 376).

confidentiality.[380] The differing critical perspectives with regards to e-Privacy Regulation and online child protection in the context of new technologies will be addressed in PART II of this Report.

v. Backdoors and weakened security

Recent debates and discussions underscore the importance of encryption.[381] As it can be seen from the open letter written by the UK Home Department, US Attorney General, US Homeland Security and Australian Home Affairs,[382] States are reluctant to support end-to-end encryption and want a "backdoor for law enforcement to circumvent legitimate encryption methods in order to access private communications".[383]

The e-Privacy Regulation allows access and processing of electronic communications data in case *"it is necessary for compliance with a legal obligation to which the provider is subject laid down by Union or Member State law in accordance with Article 11, which respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security"* (Article 6(d)). This paragraph is criticised as it may enable MSs to enact legislation, which would allow backdoors on end-users' terminal devices. Backdoors decrease the security of communications, in addition to increasing the risks and the costs associated with the electronic communications.[384] In other words, they are quite open to abuse. Moreover, they do not comply with the GDPR's principles such as fairness, transparency, and security.[385]

---

[380] Jakubowska (n 61).

[381] ISOC, 'The Internet Community Stands up for Encryption' (*Internet Society*) <https://www.internetsociety.org/encryption/internet-community-stands-up-for-encryption/> accessed 26 August 2020; Ella Jakubowska, 'Why Weak Encryption Is Everybody's Problem' (*EDRi*, 9 October 2019) <https://edri.org/why-weak-encryption-is-everybodys-problem/> accessed 26 August 2020; Article 29 Data Protection Working Party, 'Opinion 03/2016 on the Evaluation and Review of the EPrivacy Directive (2002/58/EC) (WP 240)' (n 118).

[382] Priti Patel, William Barr, Kevin McAleenan, Peter Dutton (n 373); Jakubowska (n 381).

[383] Jakubowska (n 381).

[384] Iraklis Symenoidis in 'EDPS Workshop Highlights Importance of Encryption and Weaknesses in Proposed E-Privacy Rules, FLECEP20200063 (Unpublished)' (n 376) 3.

[385] Marit Hansen in ibid.

On top of the criticisms regarding backdoors, the draft proposal is also criticised due to the high number of legal grounds allowing processing of electronic communications data, in the latest version of the proposed text, since this would "weaken cybersecurity by increasing the complexity of communication systems and enlarging the "surface of attack".[386]

vi. Data retention

Paragraph 4 of Article 7 of the draft e-Privacy Regulation enables the MSs to require commercial actors to retain the data for longer periods than previously allowed, "to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security". This is criticised as the MSs may take advantage of this provision to bypass the CJEU's recent jurisdiction limiting MSs data retention capabilities, via resorting to the use of the electronic communications data collected by commercial actors, which would then result in increased surveillance of all types of electronic communications.[387]

vii. Competition and ePrivacy: the CMA report and Google's acquisition of Fitbit

The fact that a few big platforms like Google and Facebook dominate online product and services markets as well as online advertising markets is quite concerning from a competition viewpoint, considering how these platforms have gained and currently hold the power to significantly influence the online products and services due to their dominance, and as a result also create concerns regarding ePrivacy. For instance, Google holds more than 90% of the £7.3 billion online search advertising market in the UK. Facebook holds more than 50% of the £5.5 billion online display advertising market.[388] Another example of their dominance can be seen in the shares of user attention these platforms hold: Google and Facebook held 38 percent of the users' attention in February 2020 in the UK and this number went up to 39 percent in April 2020, during the Covid-

[386] Stefano Leucci in ibid 2.

[387] Digitalcourage, 'EPrivacy: Private Data Retention through the Back Door' (*EDRi*, 22 May 2019) <https://edri.org/eprivacy-private-data-retention-through-the-back-door/> accessed 26 August 2020; 'EU States Vote on EPrivacy Reform: We Were Promised More Privacy. Instead, We Are Getting a Surveillance Toolkit.' (n 61).

[388] Competition and Markets Authority, 'Online Platforms and Digital Advertising - Market Study Final Report' (2020) 5 <https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf> accessed 25 August 2020.

19 pandemic.[389] Due to their dominance, their products and services benefit from strong "network effects, economies of scale and unmatchable access to user data",[390] which is making it more and more difficult for their competitors to compete with them. This creates a negative effect with regard to the competition in the relevant markets, especially the digital advertising market, increasing the prices of goods and services, and "leads to reduced innovation and choice and to consumers giving up more data than they would like".[391] Moreover, the dominance of these platforms have a negative effect on the online publishers, such as newspapers and other content creators, as explained above in Section II, subheading A(v) on "Alternatives and contextual advertising".

In light of these problems, competition authorities have started paying more attention to online platforms and their data practices. Most recently, the UK Competition and Markets Authority (CMA) has initiated an investigation into online platforms and digital advertising in July 2019. The main goals behind the investigation were to understand market power of online platforms, their effect on consumers, the amount of information and control the consumers have over their data and the effect of the market power the online platforms have on competition.[392] The final report was released on 1 July 2020.[393]

From an e-privacy viewpoint, some important suggestions raised by the report, regarding potential interventions are as follows: First of all, in line with the interim report of December 2019, CMA suggests creating a shared data ecosystem to increase competition, where platforms open their databases for new market entrants and smaller companies and share data relating to users via common user IDs.[394] Secondly, CMA suggests that consumers should be allowed to sell access to

[389] ibid 48.
[390] ibid 5.
[391] ibid.
[392] 'Online Platforms and Digital Advertising Market Study - GOV.UK' <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study> accessed 25 August 2020.
[393] Competition and Markets Authority, 'New Regime Needed to Take on Tech Giants' (*GOV.UK*, 7 January 2020) <https://www.gov.uk/government/news/new-regime-needed-to-take-on-tech-giants> accessed 25 August 2020; Competition and Markets Authority (n 388); See also Ian Brown's briefing paper 'Interoperability as a tool for competition regulation', 30 July 2020, which summarizes important points raised in Vestager, Furman and Stigler reviews and the CMA reports on and other intervention suggestions so far Ian Brown, 'Interoperability as a Tool for Competition Regulation' (LawArXiv 2020) preprint <https://osf.io/fbvxd> accessed 26 August 2020.
[394] Competition and Markets Authority (n 388) para 8.241-8.242.

their personal data, and it mentions the introduction of data self management through "Personal Information Management Services (PIMs)" and "Personal Data Stores (PDS)".[395]

CMA also suggests that certain platforms shall be banned from using certain types of personal data they collect through one service on another one, as well as supporting the idea of purpose limitation and the other relevant requirements under the GDPR.[396]

CMA's suggestions above were criticised on the grounds that, first of all, creating a shared data ecosystem presents a significant risk when it comes to data protection and may lead to a race to the bottom. Secondly, the idea of data self-management is questioned, considering the ease such a scheme may provide in abusing the user data through forced consent, in an environment where power imbalances and information asymmetries persist. On the other hand, suggestions regarding enforcing the GDPR's purpose limitation principle and the idea that some types of personal data should not be used across different services of the same platform are welcomed.[397]

Google's acquisition of FitBit and its significance in the online tracking ecosystem[398]

Google's intentions to acquire Fitbit raised significant questions in the EU concerning both competition and privacy, in light of the risk that Google's acquisition of Fitbit's data, which includes sensitive health and biometric data of its users, may strengthen its dominance even further and open the door for data abuses.[399]

---

[395] ibid 8.246.

[396] Wolfie Christl, 'Wolfie Christl on Twitter - CMA Interventions' (*Twitter*, 7 January 2020) <https://twitter.com/WolfieChristl/status/1278308711786840065> accessed 25 August 2020.

[397] Wolfie Christl, 'Wolfie Christl On CMA's New Report' (*Twitter*) <https://twitter.com/WolfieChristl/status/1278293847471271939> accessed 26 August 2020.

[398] For the importance and the risks raised by collection of health data, see Melanie Lefkowitz, 'Study: Online Trackers Follow Health Site Visitors' (*Cornell Chronicle*, 24 June 2020) <https://news.cornell.edu/stories/2020/06/study-online-trackers-follow-health-site-visitors> accessed 26 August 2020; Privacy International, 'Your Mental Health for Sale' (2019) <https://privacyinternational.org/sites/default/files/2019-09/Your%20mental%20health%20for%20sale%20-%20Privacy%20International.pdf> accessed 26 August 2020; Privacy International, 'Privacy International Study Shows Your Mental Health Is for Sale' (*Privacy International*, 3 September 2019) <http://privacyinternational.org/long-read/3194/privacy-international-investigation-your-mental-health-sale> accessed 26 August 2020.

[399] Andrés Arrieta and Mitch Stoltz, 'Google-Fitbit Merger Would Cement Google's Data Empire' (*Electronic Frontier Foundation*, 7 April 2020) <https://www.eff.org/deeplinks/2020/04/google-fitbit-merger-would-cement-googles-data-empire> accessed 26 August 2020; Privacy International, 'Press Release: Privacy International Calls for

Within the scope of the European Commission's investigation, Google promised not to use Fitbit's data for advertising purposes and keep the collected data separate for 5 years. Accordingly, Google will establish a scheme called Fitbit Account Data which will include auditable controls on technical and process-related aspects. Google will not transfer the data to its servers or use the data for Google's advertising services, in a manner that Fitbit will remain the only data controller. The European Commission is testing the proposed scheme to determine if in those circumstances the acquisition would disturb competition and whether the proposed data scheme would be compliant with the data protection and privacy laws.

Politico reported that the industry responded negatively to Google's proposal and consumer groups requested the deal to be further investigated. Experts from academia and civil society also warned the Commission to reconsider the deal, since similar deals in the past, such as Google-DoubleClick and Facebook-WhatsApp, have proven quite problematic from both privacy and competition law aspects.[400] For instance, Facebook had argued during the European Commission's investigation into its acquisition of WhatsApp in 2014 that "it would be unable to establish reliable automated matching between Facebook users' accounts and WhatsApp users' accounts".[401] Only two years had passed after this statement when WhatsApp introduced the possibility to link its users' phone numbers with their Facebook profiles. Even though Facebook stated that such matching was not technically possible in 2014, the European Commission found that it was indeed possible, and Facebook had knowingly stated otherwise during the investigation in 2014. As a result, Facebook was fined €110 million since it had provided incorrect or misleading information. The Commission stated that this new information does not affect its assessment of the merger as the Commission had already explored the potential effects of such technical possibility during its investigation.[402] However, even if one accepts that such a merger does not disturb competition in the relevant markets, it is difficult to argue that merging databases in this manner would not create significant risks from a data protection and privacy viewpoint. It is difficult to assess the effect of mergers

---

the Google/Fitbit Merger to Be Blocked' (*Privacy International*, 17 June 2020) <http://privacyinternational.org/press-release/3750/press-release-privacy-international-calls-googlefitbit-merger-be-blocked> accessed 26 August 2020.

[400] Francesca Bria and others, 'Europe Must Not Rush Google-Fitbit Deal' (*Politico*, 22 July 2020) <https://www.politico.eu/article/europe-must-not-rush-google-fitbit-deal-data-privacy/> accessed 25 August 2020.

[401] European Commission, 'Mergers: Commission Fines Facebook €110 Million for Providing Misleading Information about WhatsApp Takeover' (*European Commission - European Commission*, 18 May 2017) <https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369> accessed 26 August 2020.

[402] ibid.

and acquisitions involving big datasets, as, among other problems, information asymmetries between big data companies and regulatory/supervisory authorities contribute to a lack of understanding from the authority's side. Technical capabilities to be acquired by the company as a result of the acquisition may seem harmless to the authorities at first. Nevertheless, the biggest selling point in such mergers is the data, and it has to be kept in mind that the distinctive characteristic of big data is that in time it is possible to develop/discover new and potentially highly lucrative uses of it and thus, a seemingly harmless acquisition may create significant disturbances to the competition such as monopolization and critical risks to users' privacy in the not-so-distant future.

The Commission was expected to make its decision regarding Google's acquisition of FitBit by 8 August 2020[403] and it was regarded as highly possible that the deal would be approved under the current circumstances.[404] However, on August 4, 2020, as a reflection of the above-mentioned concerns, the Commission decided to initiate an in-depth investigation to assess the deal under the EU Merger Regulation. In its press release, the Commission expresses its concerns that the deal would further strengthen Google's position in the online advertising markets "by increasing the already vast amount of data that Google could use for personalisation of the ads it serves and displays.".[405] The Commission states its doubts regarding Google's proposal of data silos, which includes keeping the data acquired from FitBit separate from Google's own databases, in data silos that Google would create, and not using it for Google's advertising business. According to the Commission, creation of such data silos cannot dismiss their doubts regarding the effects of the transaction:

> *"However, the Commission considers that the data silo commitment proposed by Google is insufficient to clearly dismiss the serious doubts identified at this stage as to the effects of the transaction. Among others, this is because the data silo remedy did not cover all the*

[403] 'EU Wants to Ascertain Google Will Not Use Fitbit Data for Advertising' (*CDE News | Corporate Dispatch*, 16 July 2020) <https://corporatedispatch.com/eu-wants-to-ascertain-google-will-not-use-fitbit-data-for-advertising/> accessed 25 August 2020.
[404] Bria and others (n 400).
[405] European Commission, 'Mergers: Commission Opens in-Depth Investigation into the Proposed Acquisition of Fitbit by Google' (*European Commission - European Commission*, 8 April 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1446> accessed 25 August 2020.

data that Google would access as a result of the transaction and would be valuable for advertising purposes."[406]

At this stage, the Commission needs to make a decision by 9 December 2020,[407] which is highly anticipated and may have great significance for similar acquisitions in the future.

Concluding Remarks

Before moving on to PART II of this Report, we aimed to explain the chronological advent of and important issues concerning ePrivacy laws both in Europe and Turkey. In PART I of this Report, we set the scene before furthering the discussions on the most debated issues concerning e-Privacy laws. To do so, in Section I, we first provided a general overview of the chronology of the e-Privacy laws and a summary of the applicable legal framework both in Europe and in Turkey. Secondly, we underscored the important points concerning the current debates on the draft e-Privacy Regulation. In Section II, we explained location tracking and online identifiers under the draft e-Privacy Regulation. We delved into online tracking technologies, location tracking, and next generation profiling tools and cookieless tracking before furthering the discussion on tracking/cookie walls and forced consent, Do-Not-Track signals, introduction of legitimate interest as a ground for processing of electronic communications data, the critical issue of online child abuse prevention, backdoors and weakened security challenges, data retention and finally concluded by a brief summary of the competition and its relation with ePrivacy with a specific focus on the CMA Report and Google's acquisition of Fitbit.

Moving forward, in PART II of our Report, we will build on the discussions we carried out above and aim to delve into the business impact of turning all cookies (except necessary cookies) off on websites, the implications of cookieless tracking technologies for different stakeholders while addressing the question of how do we balance user privacy and the data economy in the context of online advertising. We will also discuss the legal and economic implications of the current technologies as well as cookieless technologies. We further aim to look at the legislation aspect and answer the questions of whether there is a need for strict regulations to protect users or whether

[406] ibid.
[407] ibid.

the optimal approach would be self-regulation/co-regulation or not. We will also address how digital literacy could be seen as a compelling option in enhancing individuals' rights to data protection and privacy.

In an effort to find the optimum approach to find the right balance between protecting users' right to privacy and supporting transparency, fairness, and innovation in the golden age of the online advertising industry, the issues and challenges we mentioned in PART I of this Report are crucial to understand before drawing a roadmap for Turkey. In this context, the PART I of this Report concludes that before carrying out an in-depth analysis of the relevant laws and rules that exist in the current data protection and privacy regimes both in the EU and in Turkey, and before drawing a roadmap for Turkish legislators, developing a true understanding of the important points that are emphasised in the above discussions are of utmost importance.

Overall, in light of the above discussions, it can be concluded that the current situation with regards to the enactment of the long-waited e-Privacy Regulation, the reasons behind its postponement and the challenges that rotate around the debates concerning e-Privacy legislation require careful consideration. We believe that the current debates generally lack to take account of novel technologies, especially in the area of online advertising. No matter where in the world, enactment of e-Privacy laws will have strong implications and pivotal importance not only for the future of businesses and the economy of a country, but will also have tangible impact for individuals' rights, freedoms and liberties. Due to the dynamic nature of ever-developing technologies and ever-changing online tracking methods, it is absolutely necessary to appreciate that the decisions made for shaping the legislation calls for additional scrutiny as it needs to keep up with the developments in the advertising sector and its surrounding fields.

Although PART II of our Report will mainly focus on the business and legal impact of the novel technologies and their interlink with the long-debated issues such as consent, the essences lying at the heart of the privacy and data protection regimes and their implications in practice will also be underscored from consumer protection, competition, and human rights perspectives. PART II of our Report will aim to address all the challenges we explained in PART I and provide a multi-layered and holistic approach with a specific focus on the practical implications of e-Privacy rules.

Lastly and arguably most importantly, we believe that the ever-changing nature of online advertising technologies should be taken into account and be well-understood before making policy decisions and laws which will govern the ePrivacy ecosystem. In this way only, the optimal approach where different stakeholders' rights and interests are protected can be achieved and the risk of making laws that are doomed to be outdated and inefficient can be avoided.

Bibliography

Adams AA and Ferryman J, 'The Future of Video Analytics for Surveillance and Its Ethical Implications' (Social Science Research Network 2012) SSRN Scholarly Paper ID 2174255 <https://papers.ssrn.com/abstract=2174255> accessed 23 April 2019

Adform, 'What Is Ad Fraud and How Can It Be Prevented' (2019) <https://iabeurope.eu/wp-content/uploads/2019/11/what-is-ad-fraud-and-how-can-it-be-prevented.pdf> accessed 24 August 2020

Agencia Española de Protección de Datos, 'Guía sobre el uso de las cookies' (2020)

——, 'La AEPD actualiza su Guía sobre el uso de cookies para adaptarla a las nuevas directrices del Comité Europeo de Protección de Datos' (*AEPD*, 28 July 2020) <https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-actualiza-guia-cookies> accessed 25 August 2020

Aljazeera News, 'Qatar Makes COVID-19 App Mandatory, Experts Question Efficiency' (*Aljazeera*, 26 May 2020) <https://www.aljazeera.com/news/2020/05/qatar-covid-19-app-mandatory-experts-question-efficiency-200524201502130.html> accessed 24 August 2020

'AmIUnique' <https://amiunique.org/> accessed 24 August 2020

Arrieta A and Stoltz M, 'Google-Fitbit Merger Would Cement Google's Data Empire' (*Electronic Frontier Foundation*, 7 April 2020) <https://www.eff.org/deeplinks/2020/04/google-fitbit-merger-would-cement-googles-data-empire> accessed 26 August 2020

Article 29 Data Protection Working Party, 'Opinion 8/2006 on the Review of the Regulatory Framework for Electronic Communications and Services, with Focus on the EPrivacy Directive (WP 126)' (2006) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp126_en.pdf> accessed 25 August 2020

——, 'Opinion 1/2008 on Data Protection Issues Related to Search Engines (WP148)' (2008) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf> accessed 24 August 2020

——, 'Opinion 2/2010 on Online Behavioural Advertising (WP 171)' (2010) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf> accessed 24 August 2020

——, ‘Opinion 04/2012 on Cookie Consent Exemption (WP 194)’ (2012) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf> accessed 24 August 2020

——, ‘Opinion 03/2016 on the Evaluation and Review of the EPrivacy Directive (2002/58/EC) (WP 240)’ (2016) <https://www.pdpjournals.com/docs/88612.pdf>

Article 29 Working Party, ‘Opinion 13/2011 on Geolocation Services on Smart Mobile Devices’ (2011) WP 185 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf> accessed 3 May 2019

Atabey A, *Is Google at Odds with the GDPR? Evaluation of Google’s Personal Data Collection on Mobile Operating Systems in Light of the Principles of Purpose Limitation, Data Minimisation, and Accountability* (1st edn, Oniki Levha Yayıncılık 2020)

Atabey A and Berber LK, ‘Addressable TV and Consent Sequencing’ (2020) 1 Global Privacy Law Review <https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/1.1/GPLR2020004> accessed 21 September 2020

Baker J, ‘Critics on Croatia’s EPrivacy Proposal: Legitimate Interest Provisions Not Legitimate’ (25 February 2020) <https://iapp.org/news/a/critics-on-croatias-eprivacy-proposal-legitimate-interest-provisions-not-legitimate/> accessed 26 August 2020

Barker A, ‘Clear Channel to Roll out Billboards “with Brains” in Europe’ (*Financial Times*, 10 August 2020) <https://www.ft.com/content/e5c5a996-8d54-4d5c-a5df-a036b5579148> accessed 25 August 2020

Beresford AR and Stajano F, ‘Location Privacy in Pervasive Computing’ (2003) 2 IEEE Pervasive Computing 46

Berthélémy C, ‘Captured States - e-Privacy Regulation Victim of a “Lobby Onslaught”’ (*EDRi*, 23 May 2019) <https://edri.org/coe-eprivacy-regulation-victim-of-lobby-onslaught/> accessed 24 August 2020

‘Beschluss Der Konferenz Der Unabhängigen Datenschutzaufsichtsbehörden Des Bundes Und Der Länder - 12.05.2020 - Hinweise Zum Einsatz von Google Analytics Im Nicht-Öffentlichen Bereich’ <https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf> accessed 25 August 2020

Bietti E, ‘Consent as a Free Pass: Platform Power and the Limits of the Informational Turn’ (Social Science Research Network 2020) SSRN Scholarly Paper ID 3489577 <https://papers.ssrn.com/abstract=3489577> accessed 25 August 2020

Bisarya S and Bulmer WE, ‘Rule of Law, Democracy and Human Rights: The Paramountcy of Moderation’ in Anne Meuwese, Ernst Hirsch Ballin and Maurice Adams (eds), *Constitutionalism and the Rule of Law: Bridging Idealism and Realism* (Cambridge University Press 2017) <https://www.cambridge.org/core/books/constitutionalism-and-the-rule-of-law/rule-of-law-

democracy-and-human-rights-the-paramountcy-of-moderation/A0519089C517185986BC2165F622CF0F> accessed 24 August 2020

Blanke U and others, 'Capturing Crowd Dynamics at Large Scale Events Using Participatory GPS-Localization', *2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)* (IEEE 2014) <http://ieeexplore.ieee.org/document/6827652/> accessed 19 August 2019

Bradshaw T, 'Facebook Attacks Apple for Curbing Personalised Ads' (26 August 2020) <https://www.ft.com/content/1a72d3d7-f2ec-4bb1-9f61-d65afba41821> accessed 30 August 2020

Branded, 'So *that's* How Breitbart Is Still Making Money' (22 July 2020) <https://branded.substack.com/p/so-thats-how-breitbart-is-still-making> accessed 25 August 2020

Bria F and others, 'Europe Must Not Rush Google-Fitbit Deal' (*Politico*, 22 July 2020) <https://www.politico.eu/article/europe-must-not-rush-google-fitbit-deal-data-privacy/> accessed 25 August 2020

Brignull H, 'What Are Dark Patterns?' (2018) <https://darkpatterns.org> accessed 20 August 2020

Brown I, 'Interoperability as a Tool for Competition Regulation' (LawArXiv 2020) preprint <https://osf.io/fbvxd> accessed 26 August 2020

BTS & Partners, 'ICTA Launches A Public Consultation On The Draft EPrivacy Regulation' (18 May 2020) <https://www.bts-legal.com/publication-detail/ICTA%20Launches%20A%20Public%20Consultation%20On%20The%20Draft%20ePrivacy%20Regulation> accessed 24 August 2020

'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 24 August 2020

Bu-Pasha S and others, 'EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for Transparency' (2016) 2 European Data Protection Law Review 312

Burgess M, 'We Need to Fix GDPR's Biggest Failure: Broken Cookie Notices' [2020] *Wired UK* <https://www.wired.co.uk/article/gdpr-cookie-consent-eprivacy> accessed 1 July 2020

Buttarelli G, 'The Urgent Case for a New EPrivacy Law' (*European Data Protection Supervisor - European Data Protection Supervisor*, 19 October 2018) <https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en> accessed 23 August 2020

Cadwalladr C and Graham-Harrison E, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' *The Guardian* (17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 17 September 2020

Cann V and Balanyá B, 'Captured States: When EU Governments Are a Channel for Corporate

Interests' (Corporate Europe Observatory (CEO) 2019) <https://corporateeurope.org/sites/default/files/ceo-captured-states-final_0.pdf> accessed 24 August 2020

Cellan-Jones R and Kelion L, 'The Great Coronavirus-Tracing Apps Mystery' *BBC News* (22 July 2020) <https://www.bbc.com/news/technology-53485569> accessed 25 August 2020

Centre for Intellectual Property and Information Law, 'European Data Protection and Electronic Privacy: Transnational Resources' <https://www.cipil.law.cam.ac.uk/resources/pan-european-data-protection-and-e-privacy>

——, 'Personal Data and Privacy in Telecommunications Directive 97/66/EC' <https://www.cipil.law.cam.ac.uk/resourceseuropean-travaux/personal-data-and-privacy-telecommunications-directive-9766ec> accessed 24 August 2020

Chang A, 'How the Internet Keeps Poor People in Poor Neighborhoods' (*Vox*, 12 December 2016) <https://www.vox.com/2016/12/12/13867692/poor-neighborhoods-targeted-ads-internet-cartoon> accessed 24 August 2020

Chen L and others, 'Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey' (2017) 5 IEEE Access 8956

Christl W, 'Corporate Surveillance in Everyday Life' (Cracked Labs 2017) <https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf> accessed 24 August 2020

——, 'Wolfie Christl on Twitter - CMA Interventions' (*Twitter*, 7 January 2020) <https://twitter.com/WolfieChristl/status/1278308711786840065> accessed 25 August 2020

——, 'On Lotame's Blog Post on Twitter' (*Twitter*, 3 July 2020) <https://twitter.com/WolfieChristl/status/1279023708955344896> accessed 25 August 2020

——, 'On Lotame's Blog Post on Twitter - 2' (*Twitter*, 3 July 2020) <https://twitter.com/WolfieChristl/status/1279027578578317313> accessed 25 August 2020

——, 'Wolfie Christl on Twitter on MobiBurn' (*Twitter*, 28 August 2020) <https://twitter.com/WolfieChristl/status/1299287573370724353> accessed 30 August 2020

——, 'Wolfie Christl on Criteo' (*Twitter*, 31 August 2020) <https://twitter.com/WolfieChristl/status/1300528762153586688> accessed 17 September 2020

——, 'Wolfie Christl On CMA's New Report' (*Twitter*) <https://twitter.com/WolfieChristl/status/1278293847471271939> accessed 26 August 2020

'Chrome Cookie Tracking Changes 2020' (*YIELDKIT*, 31 January 2020) <https://www.yieldkit.com/news/chrome-cookie-tracking-changes-2020/> accessed 24 August 2020

Chugh A, 'Apple Is Killing A Billion-Dollar Ad Industry With One Popup' (*Medium*, 10 July 2020) <https://medium.com/macoclock/apple-is-killing-a-billion-dollar-ad-industry-with-one-

popup-2f83d182837f> accessed 25 August 2020

Clarke R and Wigan M, 'You Are Where You've Been: The Privacy Implications of Location and Tracking Technologies' (2011) 5 Journal of Location Based Services 138

CMS, 'Tracking under the EPrivacy Regulation' <https://cms.law/en/deu/insight/e-privacy/tracking-under-the-e-privacy-regulation> accessed 24 August 2020

Cointepas R, 'CNAME Cloaking, the Dangerous Disguise of Third-Party Trackers' (*Medium - NextDNS*, 22 November 2019) <https://medium.com/nextdns/cname-cloaking-the-dangerous-disguise-of-third-party-trackers-195205dc522a> accessed 24 August 2020

Columbus L, 'Analytics Are Defining The Future Of Digital Advertising' (*Forbes*, 18 January 2018) <https://www.forbes.com/sites/louiscolumbus/2018/01/18/analytics-are-defining-the-future-of-digital-advertising/> accessed 25 August 2020

Commission Nationale de l'Informatique et des Libertés, 'Délibération N° 2019-093 Du 4 Juillet 2019 Portant Adoption de Lignes Directrices Relatives à l'application de l'article 82 de La Loi Du 6 Janvier 1978 Modifiée Aux Opérations de Lecture Ou Écriture Dans Le Terminal d'un Utilisateur (Notamment Aux Cookies et Autres Traceurs) (Rectificatif)' <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337> accessed 25 August 2020

——, 'Délibération SAN-2019-001 Du 21 Janvier 2019' <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1> accessed 25 August 2020

——, 'The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC' (21 January 2019) <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc> accessed 25 August 2020

Commission Nationale de l'Informatique et des Libertés (CNIL), 'Application « StopCovid » : La CNIL Tire Les Conséquences de Ses Contrôles' (20 July 2020) <https://www.cnil.fr/fr/application-stopcovid-la-cnil-tire-les-consequences-de-ses-controles> accessed 25 August 2020

Competition and Markets Authority, 'New Regime Needed to Take on Tech Giants' (*GOV.UK*, 7 January 2020) <https://www.gov.uk/government/news/new-regime-needed-to-take-on-tech-giants> accessed 25 August 2020

——, 'Online Platforms and Digital Advertising - Market Study Final Report' (2020) <https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf> accessed 25 August 2020

'Contact Tracing Joint Statement' <https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/> accessed 25 August 2020

'Cookieless Tracking: Solutions for Accurate Attributions in 2020' (*MobileAds.com*, 30 January 2020) <https://www.mobileads.com/blog/cookieless-tracking> accessed 25 August 2020

‘Cookieless Web: 3 Areas To Watch In The Second Half Of 2020’ (*AdExchanger*, 26 May 2020) <https://www.adexchanger.com/data-driven-thinking/cookieless-web-3-areas-to-watch-in-the-second-half-of-2020/> accessed 24 August 2020

‘Coronavirus Confirmed as Pandemic by World Health Organization’ *BBC News* (11 March 2020) <https://www.bbc.com/news/world-51839944> accessed 2 July 2020

Corporate Europe Observatory, ‘Shutting down EPrivacy: Lobby Bandwagon Targets Council’ (4 June 2018) <https://corporateeurope.org/en/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targets-council> accessed 24 August 2020

Costello RÁ, ‘The Impacts of AdTech on Privacy Rights and the Rule of Law’ [2020] Technology and Regulation 11

Council 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) (7099/19)’ <https://data.consilium.europa.eu/doc/document/ST-7099-2019-INIT/en/pdf> accessed 24 August 2020

——, ‘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 (9351/19)’ <https://data.consilium.europa.eu/doc/document/ST-9351-2019-INIT/en/pdf> accessed 24 August 2020

——, ‘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 (14447/19)’ <https://data.consilium.europa.eu/doc/document/ST-14447-2019-INIT/en/pdf> accessed 26 August 2020

——, ‘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) (6543/20)’ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6543_2020_INIT&from=EN> accessed 30 June 2020

——, ‘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 (8204/20)’ <https://data.consilium.europa.eu/doc/document/ST-9351-2019-INIT/en/pdf> accessed 24 August 2020

——, ‘Draft Agendas for Council Meetings, during the Second Semester of 2020 (the German Presidency) (9250/20)’ <https://data.consilium.europa.eu/doc/document/ST-9250-2020-INIT/en/pdf> accessed 24 August 2020

——, ‘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 Discussion Paper (9243/20)' <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9243_2020_INIT&from=EN> accessed 24 August 2020

'Cross-Site Request Forgery', , *Wikipedia* (2020) <https://en.wikipedia.org/w/index.php?title=Cross-site_request_forgery&oldid=972395753> accessed 24 August 2020

Dao H, 'Characterizing CNAME Cloaking-Based Tracking' (*APNIC Blog*, 4 August 2020) <https://blog.apnic.net/2020/08/04/characterizing-cname-cloaking-based-tracking/> accessed 24 August 2020

Dao H, Mazel J and Fukuda K, 'Characterizing CNAME Cloaking-Based Tracking on the Web' [2020] IFIP 9

Data Protection Commission, 'Guidance Note: Cookies and Other Tracking Technologies' (2020) <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf> accessed 24 August 2020

——, 'Report by the Data Protection Commission on the Use of Cookies and Other Tracking Technologies - Following a Sweep Conducted between August 2019 and December 2019 (Revised on 15 April 2020)' (2020) <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Data%20Protection%20Commission%20cookies%20sweep%20REVISED%2015%20April%202020%20v.01.pdf> accessed 22 September 2020

Datenschutzkonferenz, 'Konferenz Der Unabhängigen Datenschutzaufsichtsbehörden Des Bundes Und Der Länder - Orientierungshilfe Der Aufsichtsbehörden Für Anbieter von Telemedien' <https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf> accessed 25 August 2020

Datoo S, 'This Recycling Bin Is Following You' (*Quartz*, 8 August 2013) <https://qz.com/112873/this-recycling-bin-is-following-you/> accessed 10 August 2019

Datoo S and Seward ZM, 'City of London Halts Recycling Bins Tracking Phones of Passers-By' (*Quartz*, 12 August 2013) <https://qz.com/114174/city-of-london-halts-recycling-bins-tracking-phones-of-passers-by/> accessed 25 August 2020

Davidson H, 'China's Coronavirus Health Code Apps Raise Concerns over Privacy' (*the Guardian*, 1 April 2020) <http://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy> accessed 24 August 2020

Davies J, 'After GDPR, The New York Times Cut off Ad Exchanges in Europe - and Kept Growing Ad Revenue' (*Digiday*, 16 January 2019) <https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/> accessed 25 August 2020

de Montjoye Y-A and others, 'Unique in the Crowd: The Privacy Bounds of Human Mobility'

(2013) 3 Scientific Reports 1

Deckelmann S, 'Latest Firefox Rolls out Enhanced Tracking Protection 2.0; Blocking Redirect Trackers by Default' (*The Mozilla Blog*, 4 August 2020) <https://blog.mozilla.org/blog/2020/08/04/latest-firefox-rolls-out-enhanced-tracking-protection-2-0-blocking-redirect-trackers-by-default> accessed 24 August 2020

'Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 Pronouncing a Financial Sanction against GOOGLE LLC.' 29

Digitalcourage, 'EPrivacy: Private Data Retention through the Back Door' (*EDRi*, 22 May 2019) <https://edri.org/eprivacy-private-data-retention-through-the-back-door/> accessed 26 August 2020

DP-3T/Documents (DP^3T 2020) <https://github.com/DP-3T/documents> accessed 25 August 2020

Dumbrava C and European Parliamentary Research Service, 'Tracking Mobile Devices to Fight Coronavirus'

Edelman G, 'Why Don't We Just Ban Targeted Advertising?' [2020] *Wired* <https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising/> accessed 25 August 2020

——, 'Can Killing Cookies Save Journalism?' [2020] *Wired* <https://www.wired.com/story/can-killing-cookies-save-journalism/> accessed 25 August 2020

'EDPS Workshop Highlights Importance of Encryption and Weaknesses in Proposed E-Privacy Rules, FLECEP20200063 (Unpublished)'

EDRi, 'EPrivacy: EU Member States Push Crucial Reform on Privacy Norms Close to a Dead End' (*EDRi*, 22 November 2019) <https://edri.org/eprivacy-eu-member-states-push-crucial-reform-on-privacy-norms-close-to-a-dead-end/> accessed 24 August 2020

Edwards L, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2711290 <https://papers.ssrn.com/abstract=2711290> accessed 23 April 2019

——, 'Data Protection and E-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling', *Law, Policy and the Internet* (1st edn, Hart Publishing 2019)

Edwards Z, 'Breitbart.Com Is Partnering with RT.Com & Other Sites via Mislabeled Advertising Inventory' (*Medium*, 23 July 2020) <https://medium.com/@thezedwards/breitbart-com-is-partnering-with-rt-com-other-sites-via-mislabeled-advertising-inventory-6e7e3b5c3318> accessed 25 August 2020

'End of Third-Party Cookies Leads to More Effective Data-Driven Marketing' (*RampUp*, 18 May 2020) <https://rampedup.us/end-third-party-cookies-data-driven-marketing/> accessed 25 August 2020

Englehardt S, 'Firefox 79 Includes Protections against Redirect Tracking' (*Mozilla Security Blog*, 4 August 2020) <https://blog.mozilla.org/security/2020/08/04/firefox-79-includes-protections-against-redirect-tracking> accessed 26 August 2020

Eren E, 'Commercial Tracking in Physical Spaces, from an EU Data Protection Perspective' (LLM Dissertation, University of Edinburgh 2019)

'EU Council Considers Undermining EPrivacy' (*EDRi*, 25 July 2018) <https://edri.org/eu-council-considers-undermining-eprivacy/> accessed 26 August 2020

'EU States Vote on EPrivacy Reform: We Were Promised More Privacy. Instead, We Are Getting a Surveillance Toolkit.' (*Access Now*, 22 November 2019) <https://www.accessnow.org/eu-states-vote-on-eprivacy-reform-we-were-promised-more-privacy-instead-we-are-getting-a-surveillance-toolkit/> accessed 24 August 2020

'EU Wants to Ascertain Google Will Not Use Fitbit Data for Advertising' (*CDE News | Corporate Dispatch*, 16 July 2020) <https://corporatedispatch.com/eu-wants-to-ascertain-google-will-not-use-fitbit-data-for-advertising/> accessed 25 August 2020

European Commission, 'European Commission Recommendation of 29 July 1981 Relating to the Council of Europe Convention for the Protection of Individuals with Regard to Automated Processing of Personal Data [1981] OJ L 246/31' <https://resources.law.cam.ac.uk/cipil/travaux/data_protection/1981%20-%20Commission%20Recommendation%20on%20CoE%20Convention%20OJ%20L246-31.pdf>

——, 'Proposal for an EPrivacy Regulation' (*Shaping Europe's digital future - European Commission*, 10 January 2017) <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation> accessed 23 August 2020

——, 'Mergers: Commission Fines Facebook €110 Million for Providing Misleading Information about WhatsApp Takeover' (*European Commission - European Commission*, 18 May 2017) <https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369> accessed 26 August 2020

——, 'Communication from the Commission to the European Parliament and the Council - Data Protection Rules as a Trust-Enabler in the EU and beyond – Taking Stock' <https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/communication_2019374_final.pdf> accessed 24 August 2020

——, 'Mergers: Commission Opens in-Depth Investigation into the Proposed Acquisition of Fitbit by Google' (*European Commission - European Commission*, 8 April 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1446> accessed 25 August 2020

——, 'Communication From The Commission To The European Parliament, The Council, The European Economic and Social Committee and the Committee of The Regions EU Strategy for a More Effective Fight against Child Sexual Abuse (COM(2020) 607 Final)' <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf> accessed 26 August

2020

——, ‘Delivering on a Security Union: Initiatives to Fight Child Sexual Abuse, Drugs and Illegal Firearms’ (*European Commission - European Commission*, 24 July 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1380> accessed 26 August 2020

——, ‘Data Protection’ <https://ec.europa.eu/info/law/law-topic/data-protection_en> accessed 24 August 2020

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’ (2019) <https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf> accessed 24 August 2020

——, ‘Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak.’ <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf>

——, ‘Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak’ (2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf> accessed 14 August 2020

——, ‘Guidelines 05/2020 on Consent under Regulation 2016/679 - Version 1.1’ (2020)

——, ‘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/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf> accessed 26 August 2020

European Data Protection Supervisor, ‘The EDPS Strategy 2020-2024 - Shaping a Safer Digital Future’ (2020) <https://edps.europa.eu/sites/edp/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf> accessed 21 August 2020

European Parliament, ‘European Parliament Resolution on the Protection, of the Rights of the Individual in the Face of Technical Developments in Data Processing [1979] OJ C 140/34’ <https://resources.law.cam.ac.uk/cipil/travaux/data_protection/1979%20-%20European%20Parliament%20Resolution%20on%20DP.pdf>

——, ‘European Parliament Resolution on the Protection of the Rights of the Individual in the Face of Technical Developments in Data Processing OJ C 87/39’ <https://resources.law.cam.ac.uk/cipil/travaux/data_protection/1982%20-%20Euro%20Parl%20Resolution%20on%20DP%20OJ_C_1982_087%20-%20Final.pdf>

——, ‘Covid-19 Tracing Apps: Ensuring Privacy and Data Protection’ (5 June 2020) <https://www.europarl.europa.eu/news/en/headlines/society/20200429STO78174/covid-19-tracing-apps-ensuring-privacy-and-data-protection> accessed 24 August 2020

——, ‘European Parliament Resolution of 18 June 2020 on Competition Policy’ (18 June 2020) <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0158_EN.html> accessed 24 August 2020

EXTRA BITS - Follow the Cookie Trail - Computerphile (2013) <https://www.youtube.com/watch?v=_d0G6FZ_kR4> accessed 24 August 2020

‘Facebook Urged to Halt Encryption Plans over Child Abuse Risks’ <https://www.ft.com/content/feda422a-483a-11ea-aeb3-955839e06441> accessed 26 August 2020

Farid H, ‘Briefing: End-to-End Encryption and Child Sexual Abuse Material’ <https://5rightsfoundation.com/uploads/5rights-briefing-on-e2e-encryption--csam.pdf>

Federal Trade Commission, ‘Opinion of the Federal Trade Commission in the Matter of Cambridge Analytica, LLC, a Corporation’ <https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_opinionpublic.pdf> accessed 24 August 2020

——, ‘FTC’s Use of Its Authorities to Protect Consumer Privacy and Security’ (2020) <https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf>

Follow the Cookie Trail - Computerphile (2013) <https://www.youtube.com/watch?v=LHSSY8QNvew> accessed 24 August 2020

Fouad I and others, ‘Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels’ (2020) 2020 Proceedings on Privacy Enhancing Technologies 499

Frankenfield J, ‘How Data Analytics Work’ (*Investopedia*, 1 July 2020) <https://www.investopedia.com/terms/d/data-analytics.asp> accessed 25 August 2020

Gary J and Soltani A, ‘First Things First: Online Advertising Practices and Their Effects on Platform Speech’ (*Knight First Amendment Institute at Columbia University*, 21 August 2019) <https://knightcolumbia.org/content/first-things-first-online-advertising-practices-and-their-effects-on-platform-speech> accessed 25 August 2020

Gibbons A, ‘Time for Change and Transparency in Programmatic Advertising’ (*ISBA*, 6 May 2020) <https://www.isba.org.uk/news/time-for-change-and-transparency-in-programmatic-advertising/> accessed 25 August 2020

Graham M, ‘Google Plans to Kill Support for Third-Party Cookies That Track You All over the Internet’ (*CNBC*, 14 January 2020) <https://www.cnbc.com/2020/01/14/google-chrome-to-end-support-for-third-party-cookies-within-two-years.html> accessed 24 August 2020

Hagey K, ‘Behavioral Ad Targeting Not Paying Off for Publishers, Study Suggests’ *Wall Street Journal* (29 May 2019) <https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-for-publishers-study-suggests-11559167195> accessed 25 August 2020

Haskins C, 'Almost 17,000 Protesters Had No Idea A Tech Company Was Tracing Their Location' (*BuzzFeed News*, 25 June 2020) <https://www.buzzfeednews.com/article/carolinehaskins1/protests-tech-company-spying> accessed 30 June 2020

Hern A, 'Major Sites Including New York Times and BBC Hit by "ransomware" Malvertising' (*the Guardian*, 16 March 2016) <http://www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising> accessed 24 August 2020

Hern A and Paul K, 'Apple and Google Team up in Bid to Use Smartphones to Track Coronavirus Spread' (*the Guardian*, 10 April 2020) <http://www.theguardian.com/world/2020/apr/10/apple-google-coronavirus-us-app-privacy> accessed 25 August 2020

Hogan Lovells, 'Study of Proposal for an E-Privacy Regulation' (2019) <https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2019/2019_11_25_study_eprivacy_regulation.pdf?la=en> accessed 24 August 2020

'How Do Tracking Companies Know What You Did Last Summer?' (*Privacy International*, 21 May 2019) <http://privacyinternational.org/explainer/2976/how-do-tracking-companies-know-what-you-did-last-summer> accessed 24 August 2020

'How to Build Better Contextual Bandits Machine Learning Models' (*Google Cloud Blog*) <https://cloud.google.com/blog/products/ai-machine-learning/how-to-build-better-contextual-bandits-machine-learning-models/> accessed 25 August 2020

'How to Delete Flash Cookies, Permacookies, and Zombie Cookies' (*ReputationDefender*, 12 April 2018) <https://www.reputationdefender.com/blog/privacy/how-to-delete-flash-cookies-permacookies-and-zombie-cookies> accessed 24 August 2020

'How We're Preparing Businesses for the Impact of IOS 14' (*Facebook for Business*, 26 August 2020) <https://www.facebook.com/business/news/preparing-our-partners-for-ios-14-launch> accessed 30 August 2020

Hsiao S, 'How Our Display Buying Platforms Share Revenue with Publishers' (*Google Ad Manager*) <https://blog.google/products/admanager/display-buying-share-revenue-publishers> accessed 25 August 2020

Information and Communication Technologies Authority, 'Public Consultation Regarding the Draft Regulation on the Processing of Personal Data and Protection of Privacy in the Electronic Communications Sector' <https://www.btk.gov.tr/uploads/boarddecisions/kamuoyu-gorusu-alinmasi-elektronik-haberlesme-sektorunde-kisisel-verilerin-islenmesi-ve-gizliligin-korunmasina-iliskin-yonetmelik/77-2020-web.pdf> accessed 18 September 2020

Information Commissioner's Office, 'ICO on the Guidance on the Use of Cookies and Similar Technologies' (3 July 2019) <https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf> accessed 25 August 2020

——, 'Guidance on the Use of Cookies and Similar Technologies' (20 July 2020) <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-

technologies/> accessed 24 August 2020

——, 'What Are PECR?' (20 July 2020) <https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/> accessed 24 August 2020

——, Update Report into Adtech and Real Time Bidding (2019) <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf> accessed 22 September 2020

Information Commissioner's Office and Shah A, 'Blog: Cookies – What Does "Good" Look Like?' (3 July 2019) <https://ico.org.uk/about-the-ico/news-and-events/blog-cookies-what-does-good-look-like/> accessed 25 August 2020

'Introducing Authorized Buyers - Authorized Buyers Help' (*support.google.com*) <https://support.google.com/authorizedbuyers/answer/9070822?hl=en> accessed 24 August 2020

ISOC, 'The Internet Community Stands up for Encryption' (*Internet Society*) <https://www.internetsociety.org/encryption/internet-community-stands-up-for-encryption/> accessed 26 August 2020

Jakob W, 'Conference of German Data Protection Authorities Issues Guidance on Tracking and Cookies' (*IPT Germany*, 3 May 2019) <https://blogs.dlapiper.com/iptgermany/2019/05/03/conference-of-german-data-protection-authorities-issues-guidance-on-tracking-and-cookies/> accessed 25 August 2020

Jakubowska E, 'Why Weak Encryption Is Everybody's Problem' (*EDRi*, 9 October 2019) <https://edri.org/why-weak-encryption-is-everybodys-problem/> accessed 26 August 2020

——, 'EPrivacy Hangs in the Balance, but It's Not over yet...' (*EDRi*, 20 November 2019) <https://edri.org/eprivacy-hangs-in-the-balance-but-its-not-over-yet/> accessed 24 August 2020

Juinen J, 'EU May Overhaul EPrivacy Plan After Nations Criticize It' (3 December 2019) <https://news.bloomberglaw.com/privacy-and-data-security/eu-may-overhaul-eprivacy-plan-after-nations-criticize-it> accessed 24 August 2020

Kassel M, 'As 5G Technology Expands, So Do Concerns Over Privacy' *Wall Street Journal* (New York City, 27 February 2019) <https://www.wsj.com/articles/as-5g-technology-expands-so-do-concerns-over-privacy-11551236460> accessed 12 August 2019

Kayali L, 'Laura Kayali on Twitter' (*Twitter*, 16 June 2020) <https://twitter.com/LauKaya/status/1272940587893821440> accessed 24 August 2020

Klein H, 'Google Analytics: Cookieless Tracking Without GDPR Consent' (8 June 2020) <https://helgeklein.com/blog/2020/06/google-analytics-cookieless-tracking-without-gdpr-consent/> accessed 25 August 2020

Koetsier J, 'Malicious Chinese SDK In 1,200 IOS Apps With Billions Of Installs Causing "Major Privacy Concerns To Hundreds Of Millions Of Consumers"' (*Forbes*, 24 August 2020) <https://www.forbes.com/sites/johnkoetsier/2020/08/24/malicious-chinese-sdk-in-1200-ios-apps-with-billions-of-installs-causing-major-privacy-concerns-to-hundreds-of-millions-of-

consumers/> accessed 26 August 2020

——, 'Apple's New Browser Blocked 90 Web Trackers In 5 Minutes' (Forbes, 17 September 2020) <https://www.forbes.com/sites/johnkoetsier/2020/09/17/apples-new-browser-blocked-90-web-trackers-in-5-minutes/> accessed 20 September 2020

Krishnan S and others, 'Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6' (26 August 2020) <https://tools.ietf.org/html/draft-ietf-6man-rfc4941bis-10> accessed 30 August 2020

Küzeci E, *Kişisel Verilerin Korunması* (4th edn, Oniki Levha Yayıncılık 2020)

Lanne E, 'Coronavirus: A Common Approach for Safe and Efficient Mobile Tracing Apps across the EU' (*European Innovation Partnership on Active and Healthy Ageing - European Commission*, 19 May 2020) <https://ec.europa.eu/eip/ageing/news/coronavirus-common-approach-safe-and-efficient-mobile-tracing-apps-across-eu_en> accessed 24 August 2020

Laperdrix P and others, 'Browser Fingerprinting: A Survey' [2019] arXiv:1905.01051 [cs] <http://arxiv.org/abs/1905.01051> accessed 24 August 2020

Lardinois F, 'Google Wants to Phase out Support for Third-Party Cookies in Chrome within Two Years' (*TechCrunch*, 14 January 2020) <https://social.techcrunch.com/2020/01/14/google-wants-to-phase-out-support-for-third-party-cookies-in-chrome-within-two-years/> accessed 24 August 2020

——, 'Google Rolls Back SameSite Cookie Changes to Keep Essential Online Services from Breaking' (*TechCrunch*, 3 April 2020) <https://social.techcrunch.com/2020/04/03/google-rolls-back-samesite-cookie-changes-to-keep-essential-online-services-from-breaking/> accessed 25 August 2020

Latham & Watkins LLP, 'France's CNIL Publishes New Guidance on Cookies' (*Global Privacy & Security Compliance Law Blog*, 7 August 2019) <https://www.globalprivacyblog.com/security/frances-cnil-publishes-new-guidance-on-cookies/> accessed 25 August 2020

Lee P, 'The E-Privacy Directive - When and How Does It Apply Exactly?' (*Fieldfisher*, 11 August 2011) <https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/the-e-privacy-directive-when-and-how-does-it-apply-exactly> accessed 24 August 2020

Lee Y, 'Taiwan Tracking Citizens' Phones to Make Sure They Stay Indoors during Coronavirus Lockdown' (*The Independent*, 20 March 2020) <https://www.independent.co.uk/news/world/asia/coronavirus-taiwan-update-phone-tracking-lockdown-quarantine-a9413091.html> accessed 24 August 2020

Leenes R, 'The Cookiewars: From Regulatory Failure to User Empowerment?' [2015] The Privacy & Identity Lab: 4 years later 31

Lefkowitz M, 'Study: Online Trackers Follow Health Site Visitors' (*Cornell Chronicle*, 24 June

2020) <https://news.cornell.edu/stories/2020/06/study-online-trackers-follow-health-site-visitors> accessed 26 August 2020

'Legislative Train Schedule - Civil Liberties, Justice and Home Affairs - LIBE - Proposal for a Regulation on Privacy and Electronic Communications' (*European Parliament*) <https://www.europarl.europa.eu/legislative-train/theme-civil-liberties-justice-and-home-affairs-libe/file-jd-e-privacy-reform> accessed 24 August 2020

'Legislative Train Schedule - Connected Digital Single Market - Proposal for a Regulation on Privacy and Electronic Communications' (*European Parliament*) <https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform> accessed 24 August 2020

Lomas N, 'How a Small French Privacy Ruling Could Remake Adtech for Good' (*TechCrunch*, 21 November 2018) <https://social.techcrunch.com/2018/11/20/how-a-small-french-privacy-ruling-could-remake-adtech-for-good/> accessed 25 August 2020

——, 'Google and IAB Ad Category Lists Show "Massive Leakage of Highly Intimate Data," GDPR Complaint Claims' (*TechCrunch*, 28 January 2019) <https://social.techcrunch.com/2019/01/27/google-and-iab-ad-category-lists-show-massive-leakage-of-highly-intimate-data-gdpr-complaint-claims/> accessed 25 August 2020

——, 'Cookie Walls Don't Comply with GDPR, Says Dutch DPA' (*TechCrunch*, 8 March 2019) <https://social.techcrunch.com/2019/03/08/cookie-walls-dont-comply-with-gdpr-says-dutch-dpa/> accessed 25 August 2020

——, 'GDPR Adtech Complaints Keep Stacking up in Europe' (*TechCrunch*, 20 May 2019) <https://social.techcrunch.com/2019/05/20/gdpr-adtech-complaints-keep-stacking-up-in-europe/> accessed 25 August 2020

——, 'Mental Health Websites in Europe Found Sharing User Data for Ads' (*TechCrunch*, 4 September 2019) <https://social.techcrunch.com/2019/09/04/mental-health-websites-in-europe-found-sharing-user-data-for-ads/> accessed 24 August 2020

——, 'Oracle and Salesforce Hit with GDPR Class Action Lawsuits over Cookie Tracking Consent' (*TechCrunch*, 14 August 2020) <https://social.techcrunch.com/2020/08/14/oracle-and-salesforce-hit-with-gdpr-class-action-lawsuits-over-cookie-tracking-consent/> accessed 24 August 2020

——, 'Europe's PEPP-PT COVID-19 Contacts Tracing Standard Push Could Be Squaring up for a Fight with Apple and Google' (*TechCrunch*) <https://social.techcrunch.com/2020/04/17/europes-pepp-pt-covid-19-contacts-tracing-standard-push-could-be-squaring-up-for-a-fight-with-apple-and-google/> accessed 25 August 2020

Lyons K, 'Clear Channel's Billboards Will Start Tracking Consumers in Europe' (*The Verge*, 10 August 2020) <https://www.theverge.com/2020/8/10/21361734/clear-channel-billboards-privacy-ad-tracking-europe> accessed 25 August 2020

Marotta V, Abhishek V and Acquisti A, 'Online Tracking and Publishers' Revenues: An Empirical

Analysis' (2019) <https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf>

Marshall J, Interview with Jason Kint, 'GDPR Is "a Significant Risk to Facebook and Google": A Digiday+ Slack Town Hall with DCN's Jason Kint' (19 April 2018) <https://digiday.com/media/gdpr-significant-risk-facebook-google-digiday-slack-town-hall-dcns-jason-kint/> accessed 24 August 2020

Mayhew H, Saleh T and Williams S, 'Making Data Analytics Work for You--Instead of the Other Way around | McKinsey' (7 October 2016) <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/making-data-analytics-work-for-you-instead-of-the-other-way-around> accessed 25 August 2020

McCarthy K, 'Facebook Apologizes to Users, Businesses for Apple's Monstrous Efforts to Protect Its Customers' Privacy' (27 August 2020) <https://www.theregister.com/2020/08/27/facebook_ios_ads/> accessed 30 August 2020

McDonald AM and Cranor LF, 'The Cost of Reading Privacy Policies' (2008) 4 I/S: A Journal of Law and Policy for the Information Society 543

Mcguigan L, 'Selling The American People: Data, Technology, And The Calculated Transformation Of Advertising' <https://repository.upenn.edu/cgi/viewcontent.cgi?article=4945&context=edissertations>

Meijer A and Webster CWR, 'The COVID-19-Crisis and the Information Polity: An Overview of Responses and Discussions in Twenty-One Countries from Six Continents' 32

Merken S, 'Lawmakers Ask FTC to Probe Online Ad Industry, Pointing to "widespread" Violations' *Reuters* (1 August 2020) <https://www.reuters.com/article/adtech-privacy-ftc-idUSL2N2F22OL> accessed 25 August 2020

Michael K and Clarke R, 'Location and Tracking of Mobile Devices: Überveillance Stalks the Streets' (2013) 29 Computer Law & Security Review 216

Miller A, 'SourMint: Malicious Code, Ad Fraud, and Data Leak in IOS | Snyk' (24 August 2020) <https://snyk.io/blog/sourmint-malicious-code-ad-fraud-and-data-leak-in-ios/> accessed 26 August 2020

Minch RP, 'Location Privacy in the Era of the Internet of Things and Big Data Analytics', *2015 48th Hawaii International Conference on System Sciences* (IEEE 2015) <http://ieeexplore.ieee.org/document/7069994/> accessed 10 August 2019

Mozilla, 'Redirect Tracking Protection' (*MDN Web Docs*) <https://developer.mozilla.org/en-US/docs/Mozilla/Firefox/Privacy/Redirect_tracking_protection> accessed 24 August 2020

Murakami Wood D and Mackinnon D, 'Partial Platforms and Oligoptic Surveillance in the Smart City' (2019) 17 Surveillance & Society 176

Nadler A, Crain M and Donovan J, 'Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech' (Data & Society)

Naranjo D, 'Data Protection Reform - Next Stop: E-Privacy Directive' (*EDRi*, 24 February 2016) <https://edri.org/data-protection-reform-next-stop-e-privacy-directive/> accessed 24 August 2020

Narendra M, '#Privacy: Google Announces Plans to Make Third Party Cookies Obsolete' (*PrivSec Report*, 15 January 2020) <https://gdpr.report/news/2020/01/15/privacy-google-announces-plans-to-make-third-party-cookies-obsolete/> accessed 24 August 2020

NCMEC, 'End-to-End Encryption: Ignoring Abuse Won't Stop It' (3 October 2019) <https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption> accessed 26 August 2020

——, 'End-to-End Encryption' <https://www.missingkids.org/theissues/end-to-end-encryption> accessed 26 August 2020

Norwegian Consumer Council, 'Deceived By Design' (2018) <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> accessed 2 April 2019

——, 'Out of Control' (2020) <https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf> accessed 24 August 2020

Nouwt S, 'Reasonable Expectations of Geo-Privacy?' (2008) 5 SCRIPT-ed 375

Ohm P, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 UCLA Law Review 1701

oiiadmin, 'Follow the Money: How the Online Advertising Ecosystem Funds COVID-19 Junk News and Disinformation' (*The Computational Propaganda Project*) <https://comprop.oii.ox.ac.uk/research/covid19-disinfo-seo/> accessed 25 August 2020

Olejnik L, 'Lukasz Olejnik on Twitter - 22 June 2020' (*Twitter*, 22 June 2020) <https://twitter.com/lukOlejnik/status/1275142030629523457> accessed 25 August 2020

——, 'Lukasz Olejnik on Twitter - 22 June 2020' (*Twitter*, 22 June 2020) <https://twitter.com/lukOlejnik/status/1275158957376536579> accessed 25 August 2020

——, 'European Parliament Calls to Ban Micro-Targeted Ads. Now What?' (*Security, Privacy & Tech Inquiries*, 26 June 2020) <http://blog.lukaszolejnik.com/european-parliament-calls-to-ban-micro-targeted-ads-now-what/> accessed 24 August 2020

——, 'Lukasz Olejnik on Twitter - 20 August 2020' (*Twitter*, 20 August 2020) <https://twitter.com/lukOlejnik/status/1296471401147305986> accessed 24 August 2020

——, 'Lukasz Olejnik on Twitter on IPv6' (*Twitter*, 27 August 2020) <https://twitter.com/lukOlejnik/status/1299012058386780161> accessed 30 August 2020

O'Malley J, 'Exclusive: Here's What 3 Big Museums Learn By Tracking Your Phone' (*Gizmodo UK*, 11 April 2017) <https://www.gizmodo.co.uk/2017/04/exclusive-heres-what-museums-learn-by-tracking-your-phone/> accessed 17 August 2019

O'Neill PH, 'India Is Forcing People to Use Its Covid App, Unlike Any Other Democracy' (*MIT*

Technology Review, 7 May 2020) <https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/> accessed 24 August 2020

'Online Platforms and Digital Advertising Market Study - GOV.UK' <https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study> accessed 25 August 2020

'OpenRTB (Real-Time Bidding)' (*IAB*) <https://www.iab.com/guidelines/real-time-bidding-rtb-project/> accessed 26 August 2020

'Oracle Data Cloud Platform Help Center' <https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/IDManagement/sending_ohashes.html> accessed 24 August 2020

O'Reilly L, Interview with Wendy Sletzer, 'A Key Web Standards Group Will Help Decide What Comes after the Third-Party Cookie' (29 January 2020) <https://digiday.com/media/wendy-seltzer-how-w3c-groups-work/>

Osborne Clarke, 'Planet49: CJEU Rules on Consent Requirements for Cookies' (*Osborne Clarke*, 7 October 2019) <https://www.osborneclarke.com/insights/planet49-cjeu-rules-consent-requirements-cookies/> accessed 24 August 2020

Page C, 'Oracle And Salesforce Hit With $10 Billion GDPR Class-Action Lawsuit' (*Forbes*, 14 August 2020) <https://www.forbes.com/sites/carlypage/2020/08/14/oracle-and-salesforce-hit-with-10-billion-gdpr-class-action-lawsuit/> accessed 24 August 2020

'Pan-European Privacy Preserving Proximity Tracing (PEPP-PT)' <https://www.pepp-pt.org> accessed 25 August 2020

Perrin N, 'Facebook-Google Duopoly Digital Ad Spending Forecast Estimates 2019' (*eMarketer*, 4 November 2019) <https://www.emarketer.com/content/facebook-google-duopoly-won-t-crack-this-year> accessed 25 August 2020

Pidgeon D, 'Where Did the Money Go? Guardian Buys Its Own Ad Inventory' (4 October 2016) <https://mediatel.co.uk/news/2016/10/04/where-did-the-money-go-guardian-buys-its-own-ad-inventory> accessed 25 August 2020

Piltz DrC and Zwerschke J, 'DSK Adopts Minimum Requirements for the Use of Google Analytics' (June 2020) <https://www.reuschlaw.de/en/news/dsk-adopts-minimum-requirements-for-the-use-of-google-analytics/> accessed 25 August 2020

Polonetsky J, 'Jules Polonetsky on Twitter' (*Twitter*, 22 June 2020) <https://twitter.com/JulesPolonetsky/status/1275154348918607872> accessed 25 August 2020

'Preparing Audience Network for IOS 14' (*Facebook Audience Network*, 26 August 2020) <https://en-gb.facebook.com/audiencenetwork/news-and-insights/preparing-audience-network-for-ios14> accessed 30 August 2020

Prince B, 'Sophisticated Malvertising Campaign Targets US Defense Industry' (*Dark Reading*, 17

October 2014) <https://www.darkreading.com/attacks-breaches/sophisticated-malvertising-campaign-targets-us-defense-industry-/d/d-id/1316753> accessed 24 August 2020

Priti Patel, William Barr, Kevin McAleenan, Peter Dutton, 'Open Letter from the Home Secretary - alongside US Attorney General Barr, Secretary of Homeland Security (Acting) McAleenan, and Australian Minister for Home Affairs Dutton - to Mark Zuckerberg' (*GOV.UK*, 23 December 2019) <https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg/open-letter-from-the-home-secretary-alongside-us-attorney-general-barr-secretary-of-homeland-security-acting-mcaleenan-and-australian-minister-f> accessed 26 August 2020

Privacy International, 'Case Study: Invisible Discrimination and Poverty' (*Privacy International*, 30 August 2017) <http://privacyinternational.org/case-study/737/case-study-invisible-discrimination-and-poverty> accessed 24 August 2020

——, 'I Asked an Online Tracking Company for All of My Data and Here's What I Found' (*Privacy International*, 7 November 2018) <http://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found> accessed 16 September 2020

——, 'Your Mental Health for Sale' (2019) <https://privacyinternational.org/sites/default/files/2019-09/Your%20mental%20health%20for%20sale%20-%20Privacy%20International.pdf> accessed 26 August 2020

——, 'Privacy International Study Shows Your Mental Health Is for Sale' (*Privacy International*, 3 September 2019) <http://privacyinternational.org/long-read/3194/privacy-international-investigation-your-mental-health-sale> accessed 26 August 2020

——, 'Press Release: Privacy International Calls for the Google/Fitbit Merger to Be Blocked' (*Privacy International*, 17 June 2020) <http://privacyinternational.org/press-release/3750/press-release-privacy-international-calls-googlefitbit-merger-be-blocked> accessed 26 August 2020

'Privacy-Preserving Contact Tracing - Apple and Google' (*Apple*) <https://www.apple.com/covid19/contacttracing> accessed 25 August 2020

Purdy A, 'Why 5G Can Be More Secure Than 4G' (*Forbes*, 23 September 2019) <https://www.forbes.com/sites/forbestechcouncil/2019/09/23/why-5g-can-be-more-secure-than-4g/> accessed 25 August 2020

Ravichandran D and Korula N, 'Effect of Disabling Third-Party Cookies on Publisher Revenue' (2019) <https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf> accessed 25 August 2020

Rodriguez S, 'Facebook Warns Apple's IOS 14 Could Shave More than 50% from Audience Network Revenue' (*CNBC*, 26 August 2020) <https://www.cnbc.com/2020/08/26/facebook-apple-ios-14-could-cut-audience-network-revenue-in-half.html> accessed 30 August 2020

Ropes & Gray LLP and Massey R, 'Cookies and Consent - An Update on Developments in the EU's Draft e-Privacy Regulation' (3 October 2019)

<https://www.lexology.com/library/detail.aspx?g=5df3464a-65ed-4da7-bebc-b3ceca7a51c5> accessed 26 August 2020

——, 'Cookies and Consent – An Update On Developments In The EU's Draft e-Privacy Regulation - Privacy - European Union' (14 October 2019) <https://www.mondaq.com/unitedstates/privacy-protection/853504/cookies-and-consent-an-update-on-developments-in-the-eu39s-draft-e-privacy-regulation> accessed 26 August 2020

Rosenthal R, 'A 5-Step Path to Cookieless Digital Marketing' (*SmartBrief*, 7 May 2020) <https://www.smartbrief.com/original/2020/05/5-step-path-cookieless-digital-marketing> accessed 24 August 2020

Ryan J, 'Report from Dr Johnny Ryan – Behavioural Advertising and Personal Data' (2018) <https://brave.com/wp-content/uploads/2018/09/Behavioural-advertising-and-personal-data.pdf> accessed 24 August 2020

——, 'New Evidence to Regulators: IAB Documents Reveal That It Knew That Real-Time Bidding Would Be "Incompatible with Consent under GDPR".' (*Brave Browser*, 20 February 2019) <https://brave.com/update-on-gdpr-complaint-rtb-ad-auctions/> accessed 24 August 2020

——, 'Major Publisher Group DCN Tells Regulators "the Sky Won't Fall" If RTB Switches to Safe, Non-Personal Data.' (*Brave Browser*, 19 June 2019) <https://brave.com/dcn-letter-rtb/> accessed 25 August 2020

——, 'Brave Writes to All European Governments to Press for Strong EPrivacy Protections' (*Brave Browser*, 10 October 2019) <https://brave.com/eprivacy-october2019/> accessed 26 August 2020

——, 'Submission to Irish Data Protection Commissioner' <https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2020/09/JohnnyRyanDocumnet.pdf> accessed 22 September 2020

——, 'Diagram of Criteo's Sparrow' (*Twitter*, 30 June 2020) <https://twitter.com/johnnyryan/status/1277898759633076226> accessed 25 August 2020

——, 'Diagram of Google's Turtledove' (*Twitter*, 30 June 2020) <https://twitter.com/johnnyryan/status/1277896292262428672> accessed 25 August 2020

——, 'New Data Shows Publisher Revenue Impact of Cutting 3rd Party Trackers' (*Brave Browser*, 1 July 2020) <https://brave.com/npo/> accessed 25 August 2020

——, 'Update (Six Months of Data): Lessons for Growing Publisher Revenue by Removing 3rd Party Tracking' (*Brave Browser*, 24 July 2020) <https://brave.com/publisher-3rd-party-tracking/> accessed 25 August 2020

Santos C, Bielova N and Matte C, 'Are Cookie Banners Indeed Compliant with the Law? Deciphering EU Legal Requirements on Consent and Technical Means to Verify Compliance of Cookie Banners' <https://hal.inria.fr/hal-02875447/document> accessed 24 August 2020

——, 'Are Cookie Banners Indeed Compliant with the Law? Deciphering EU Legal Requirements

on Consent and Technical Means to Verify Compliance of Cookie Banners' 75

Sartor G and others, *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence: Study* (2020) <http://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf> accessed 24 August 2020

Schiff A, 'Lawmakers Call RTB An Unfair And Deceptive Business Practice In Letter To The FTC' (*AdExchanger*, 4 August 2020) <https://www.adexchanger.com/privacy/lawmakers-call-rtb-an-unfair-and-deceptive-business-practice-in-letter-to-the-ftc/> accessed 25 August 2020

Schmidt DC, 'Google Data Collection' (Vanderbilt University 2018) <https://static.poder360.com.br/2018/08/DCN-Google-Data-Collection-Paper.pdf> accessed 24 August 2020

Schuh J, 'Temporarily Rolling Back SameSite Cookie Changes' (*Chromium Blog*) <https://blog.chromium.org/2020/04/temporarily-rolling-back-samesite.html> accessed 25 August 2020

Schwartz MJ, 'Facing the Privacy Implications of IPv6' (9 September 2011) <https://iapp.org/news/a/2011-09-09-facing-the-privacy-implications-of-ipv6/> accessed 30 August 2020

Scott M and Wanat Z, 'Poland's Coronavirus App Offers Playbook for Other Governments' (*POLITICO*, 2 April 2020) <https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments/> accessed 24 August 2020

Sebag G, 'Google Loses $56 Million Fight in French Test of EU Privacy Law' (19 June 2020) <https://www.bloombergquint.com/amp/onweb/google-loses-56-million-fight-in-french-test-of-eu-privacy-law> accessed 25 August 2020

Shelfer KM and Procaccino JD, 'Smart Card Evolution' (2002) 45 Communications of the ACM 83

Solomon A, 'Fact Check Series: Cookieless Meets Truthfulness' (*Lotame*, 17 September 2019) <https://www.lotame.com/fact-check-series-cookieless-meets-truthfulness/> accessed 25 August 2020

Stolton S, 'LEAK: EU in Push for Digital Transformation after COVID-19 Crisis' (*www.euractiv.com*, 6 April 2020) <https://www.euractiv.com/section/digital/news/leak-eu-in-push-for-digital-transformation-after-covid-19-crisis/> accessed 2 July 2020

——, 'EPP Cite Controversial PEPP-PT as Example for Single European COVID-19 App' (*www.euractiv.com*, 21 April 2020) <https://www.euractiv.com/section/digital/news/epp-cite-controversial-pepp-pt-as-example-for-single-european-covid-19-app/> accessed 25 August 2020

Storm TC, 'Cookieless Tracking System' <https://patents.google.com/patent/US20080172495>

Tau B, 'Academic Project Used Marketing Data to Monitor Russian Military Sites' *Wall Street Journal* (20 July 2020) <https://www.wsj.com/articles/academic-project-used-marketing-data-to-

monitor-russian-military-sites-11595073601> accessed 25 August 2020

Tau B and Haggin P, 'Lawmakers Urge FTC Probe of Mobile Ad Industry's Tracking of Consumers' *Wall Street Journal* (31 July 2020) <https://www.wsj.com/articles/lawmakers-urge-ftc-probe-of-mobile-ad-industrys-tracking-of-consumers-11596214541> accessed 25 August 2020

Taylor E and others, 'Follow the Money: How the Online Advertising Ecosystem Funds COVID-19 Junk News and Disinformation' 8

The Constitutional Court of the Republic of Turkey, 'Translation of the Turkish Constiution' <https://www.anayasa.gov.tr/en/legislation/turkish-constiution/> accessed 18 September 2020

'The Privacy Collective | Because Privacy Matters' <https://theprivacycollective.eu/en/> accessed 24 August 2020

'The Strava Heat Map Shows Even Militaries Can't Keep Secrets from Social Data' *Wired* <https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/> accessed 25 August 2020

Tommasoli M, 'Rule of Law and Democracy: Addressing the Gap Between Policies and Practices' (*United Nations UN Chronicle*) <https://www.un.org/en/chronicle/article/rule-law-and-democracy-addressing-gap-between-policies-and-practices> accessed 24 August 2020

Transport for London, 'Oyster Card' (*Transport for London*, February 2019) <https://www.tfl.gov.uk/corporate/privacy-and-cookies/oyster-card> accessed 24 August 2019

'User Privacy and Data Use - App Store' (*Apple Developer*) <https://developer.apple.com/app-store/user-privacy-and-data-use/> accessed 25 August 2020

Valentino-DeVries J and others, 'Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret' *The New York Times* (10 December 2018) <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html> accessed 20 June 2019

Valentino-DeVries J and Dance GJX, 'Facebook Encryption Eyed in Fight Against Online Child Sex Abuse - The New York Times' (*The New York Times*, 2 October 2019) <https://www.nytimes.com/2019/10/02/technology/encryption-online-child-sex-abuse.html> accessed 26 August 2020

Veale M, 'Privacy Is Not the Problem with the Apple-Google Contact-Tracing Toolkit' (*the Guardian*, 1 July 2020) <http://www.theguardian.com/commentisfree/2020/jul/01/apple-google-contact-tracing-app-tech-giant-digital-rights> accessed 25 August 2020

Versichele M and others, 'The Use of Bluetooth for Analysing Spatiotemporal Dynamics of Human Movement at Mass Events: A Case Study of the Ghent Festivities' (2012) 32 Applied Geography 208

Vlasova V, 'Web Skimming with Google Analytics' (*Kaspersky Securelist*, 22 June 2020) <https://securelist.com/web-skimming-with-google-analytics/97414/> accessed 25 August 2020

‘W3c/Web-Advertising’ <https://github.com/w3c/web-advertising>

Wachter S, ‘Affinity Profiling and Discrimination by Association in Online Behavioural Advertising’ (Social Science Research Network 2019) SSRN Scholarly Paper ID 3388639 <https://papers.ssrn.com/abstract=3388639> accessed 9 October 2019

‘Welcome to 5G: Privacy and Security in a Hyperconnected World (or Not?)’ (*Privacy International*, 23 July 2019) <http://privacyinternational.org/long-read/3100/welcome-5g-privacy-and-security-hyperconnected-world-or-not> accessed 12 August 2019

‘What Are Cookies? What Are the Differences between Them (Session vs. Persistent)?’ (*Cisco*, 17 July 2018) <https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117925-technote-csc-00.html> accessed 24 August 2020

‘What Is Session Cookie? - Definition from Techopedia’ (*Techopedia.com*) <http://www.techopedia.com/definition/4910/session-cookie> accessed 24 August 2020

‘WICG/Raw-Sockets’ (*GitHub*) <https://github.com/WICG/raw-sockets> accessed 24 August 2020

WICG/Sparrow (Web Incubator CG 2020) <https://github.com/WICG/sparrow> accessed 25 August 2020

WICG/Turtledove (Web Incubator CG 2020) <https://github.com/WICG/turtledove> accessed 25 August 2020

Willis LE, ‘Why Not Privacy by Default?’ (2014) 29 Berkeley Technology Law Journal 61

‘Wolfie Christl on Twitter - Anonymized Data’ (*Twitter*, 29 July 2020) <https://twitter.com/WolfieChristl/status/1288229191759081472> accessed 24 August 2020

WP11, ‘D11.5: The Legal Framework for Location-Based Services in Europe’ (Future of Identity in the Information Society 2007) D11.5 <https://lirias.kuleuven.be/retrieve/40775> accessed 22 August 2019

‘Your Morning Commute Is Unique: On the Anonymity of Home/Work Location Pairs’ (*33 Bits of Entropy*, 13 May 2009) <https://33bits.wordpress.com/2009/05/13/your-morning-commute-is-unique-on-the-anonymity-of-homework-location-pairs/> accessed 26 June 2019

Zuboff S, *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power* (Profile Books 2019)

Zuiderveen Borgesius F, *Behavioural Sciences and the Regulation of Privacy on the Internet* (Oxford Hart 2015) <https://dare.uva.nl/search?identifier=b0052c52-9815-4782-b4b0-b1cabb3624d0> accessed 11 January 2019

Zuiderveen Borgesius F and others, ‘An Assessment of the Commission’s Proposal on Privacy and Electronic Communications’ (Social Science Research Network 2017) SSRN Scholarly Paper ID 2982290 <https://papers.ssrn.com/abstract=2982290> accessed 24 August 2020

Zuiderveen Borgesius F and Steenbruggen W, 'The Right to Communications Confidentiality in Europe: Protecting Trust, Privacy, and Freedom of Expression' (Social Science Research Network 2018) SSRN Scholarly Paper ID 3152014 <https://papers.ssrn.com/abstract=3152014> accessed 23 August 2020

Zuiderveen Borgesius FJ and others, 'Tracking Walls, Take-It-or-Leave-It Choices, the GDPR, and the EPrivacy Regulation' (2017) 3 European Data Protection Law Review (EDPL) 353

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ, 'ΔΕΛΤΙΟ ΤΥΠΟΥ - Συστάσεις Για Τη Συμμόρφωση Υπευθύνων Επεξεργασίας Δεδομένων Με Την Ειδική Νομοθεσία Για Τις Ηλεκτρονικές Επικοινωνίες' <http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=84,221,176,170,98,24,72,223>

Case C-673/17 *Planet49* ECLI:EU:C:2019:801 [2019]

Constitutional Court Judgment of 2 October 2014, numbered E 2011/149 and K 2014/151, published in the Official Gazette dated 1 January 2015, numbered 29223

Constitutional Court judgment of 9 April 2014, numbered E 2013/122 and K 2014/74, published in the Official Gazette dated 26 July 2014 and numbered 29072

Décision du Conseil d'État, 19 juin 2020, Lignes directrices de la CNIL relatives aux cookies et autres traceurs de connexion

Décision du Conseil d'État, 19 juin 2020, Sanction infligée à Google par la CNIL

Décision n° MED 2018-042 du 30 octobre 2018 mettant en demeure la société VECTAURY

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others

Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Text with EEA relevance) [2008] OJ L 162/20

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 [1995] OJ L 281/31

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [1997] OJ L 24/1

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) [2002] OJ L 201/37

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) [2002] OJ L 201/37

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105/54

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 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 (Text with EEA relevance) [2009] OJ L 337/11

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (Text with EEA relevance) [2015] OJ L 241/1

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L 321/36 2018

Electronic Communications Code dated 5 November 2008, numbered 5809, published in the Official Gazette dated 10 November 2008, numbered 27050

Law no. 6639 Amending Some Laws and Decree Laws, dated 27 March 2015, published in the Official Gazette dated 15 April 2015, numbered 29327

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) 010 final 2017

Regulation Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communication Sector, published in the Official Gazette dated 24 July 2012, numbered 28363

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

The Regulation on the Processing of Personal Data and the Protection of Privacy in the Telecommunication Sector, published in the Official Gazette dated 6 February 2004, numbered 25365