Editorial

A couple of weeks back, I had an informal meeting with members of a European Data Protection Authority (DPA) on the regulation of cookies. My involvement with cookie regulation going more than a decade back,[1] I've always been a bit disappointed that DPAs have largely shied away from adopting the role of sherif in the online cookie Wild West. The current status quo is conceived by many to be suboptimal, to put it mildly.

To me, the provision in the e-Privacy Directive,[2] as amended by the Citizens' Rights Directive,[3] should be interpreted as protecting device integrity. Just like you can in principle not enter the home of a person – it is a personal, private space – you can in principle not enter a device of a person – that is a personal, private space as well. The provision was put in place more than two decades ago and has gained every more relevance. Today, many people would feel access to their smart phone to be even more intrusive than access to their home, given the sensitive data stored on or that can be accessed through that device. Although there is an obvious link to the right to data protection in the legal instrument, it is the e-Privacy Directive and not the e-Data Protection Directive, meaning that the essential question on this point is not whether personal data are processed, but rather whether the sanctity of private spaces, as protected inter alia by Article 8 of the European Convention on Human Rights, is undermined.

The relevant provision in the e-Privacy Directive holds:

> Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.[4]

DOI: 10.21552/edpl/2024/1/3

1 <https://www.acm.nl/sites/default/files/old_publication/publicaties/10167_Onderzoek%20cookies%20OPTA-TNO.pdf>.

2 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

3 Directive 2009/136/EC of the European Parliament and of the Council of 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.

4 Art 5(3) e-Privacy Directive.

Importantly, cookies are treated similarly as other forms of spy- and malware that put information on or take data from a personal device, as is underlined by the relevant recital in the Citizens' Rights Directive:

> Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses). It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of providing information and offering the right to refuse should be as user-friendly as possible.[5]

Consent is a relevant exception to the principle of device integrity, just like it is with one's home right. Of course, some people may enter a person's house whenever, such as children or other people living in the home; to others, such as neighbors, one may give the key, while expecting them to make use of the possibility to access prudently; still others, such as friends or colleagues, can enter upon explicit invitation and only do so occasionally. The limited number of people having access to the physical private domain, of course, sharply contrasts to the number of parties having access to the digital private domain. It is not uncommon that hundreds and sometimes thousands of parties have access to computers and smart devices through persistent cookies and other means; mostly, these are professional parties, with whom the user has no personal relationship.

Although there might be citizens who truly don't care about their device integrity or their personal data being shared with a multitude of parties, it is clear that most people, when asked, do not actually want the cookies they accept. Functional cookies that are helpful to enjoy the service requested, such as cookies that store volume or language preferences or webstores that safe what you put in the chart, are generally welcomed, but this does not hold true for other cookies and especially for third-party cookies.

The e-Privacy Directive makes clear that for consent, the relevant principles from the General Data Protection Regulation (GDPR)[6] should be taken into account.[7] The GDPR specifies that for consent to be valid, it needs to be freely given, specific, informed and unambiguous. The data subject should indicate their wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data.[8] It is the controller who should be able to demonstrate that the data subject has consented to processing of their personal data, the request for consent has to be presented in a manner clearly distinguishable from other matters, in an intelligible and easily accessible form,

5 Recital 66 Citizens' Rights Directive.

6 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).

7 Art 2 sub (f) e-Privacy Directive.

8 Art 4 sub 11 GDPR.

using clear and plain language. The data subject has the right to withdraw their consent at any time and when assessing whether consent is freely given, utmost account should be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[9] When information society services are offered to a minor, parental consent has to be obtained[10] and when sensitive personal data are processed (eg revealing racial or ethnic origin, political opinions, religious beliefs, sexual orientation or health conditions), explicit consent should be obtained.[11]

Many parties do not conform to these rules. Websites often do not inform citizens in detail about what will be done with their data and with whom they will be shared; parties sometimes work with pre-ticked boxes or even opt-out approaches; the description of what can and will be done with personal data is often general and vague, while the terms and language used can at times be cryptic and legalistic; using dark patterns, users are nudged towards consenting; people are refused access to services when they do not consent to (non-functional) cookies; sometimes, cookie-consent is tied to consent for other parts of the agreement with a party; websites generally do not distinguish between age groups or ask for parental consent; and parties generally do not distinguish between consent for ordinary personal data and sensitive personal data.

These concepts of course largely draw from private law standards for contract and consent, but private law offers additional rules. For example, many countries have embedded in their contract law a principle that if one of the parties did not understand the value of the good they are trading, the contract is null and void. When commercial parties harvest large amounts of valuable personal data, while the data subject is oblivious to the value of what they are giving away, this doctrine could apply. In addition, in many cases, there is an imbalance in power between the cookie-consenter and the party requesting consent, which may run into various principles of contract law, as it can undermine the extent to which consent is indeed freely given. Sometimes, especially with respect to critical and essential services, mandating cookie-consent can violate the prohibition of abuse of power or abuse of circumstances. Many contract law systems also harbor ethical concepts, for example holding that if parties agree to immoral contractual clauses, these will be considered null and void. The question is how that principle would apply to parties that request consent for third party access by more than hundred unrelated third parties, eg when downloading a flashlight app. The EU Unfair Commercial Practices Directive blacklists conduct under which a service is advertised as gratis or free, while in fact consumers have to pay. This, arguably, is the case when services are advertised as free, while in fact, consumers are paying with their data.[12]

9 Art 7 GDPR.

10 Art 8 GDPR.

11 Art 9 GDPR.

12 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'.

But the problem with this private law approach to data protection is that it relies on consent. Even if all the cookie-requests did accord to the prevailing legal standards, they would still lead to consent-fatigue – because people are bombarded with multiple consent-requests on a daily basis, they click ok to about anything. The problem may run even deeper, as the reliance on consent may feed into the popular sentiment that the GDPR is primarily a nuisance and does not actually protect the rights and interests of citizens. The inability of DPAs and other governmental authorities to adequately tackle this problem might thus have consequences for their legitimacy and public support. Admittedly, part of this may be water under the bridge, as Google recently announced a change in its policy in a post called 'Preparing for the end of third-party cookies':

> If your site uses third-party cookies, it's time to take action as we approach their deprecation. To facilitate testing, Chrome has restricted third-party cookies for 1% of users from January 4th, 2024. Chrome plans to ramp up third-party cookie restrictions to 100% of users from Q3 2024, subject to addressing any remaining competition concerns of the UK's Competition and Markets Authority. Our goal with the Privacy Sandbox is to reduce cross-site tracking while still enabling the functionality that keeps online content and services freely accessible by everyone. Deprecating and removing third-party cookies encapsulates the challenge, as they enable critical functionality across sign-in, fraud protection, advertising, and generally the ability to embed rich, third-party content in your sites—but at the same time they're also the key enablers of cross-site tracking. In our previous major milestone, we launched a range of APIs providing a privacy-focused alternative to today's status quo for use cases like identity, advertising, and fraud detection. With alternatives in place, we can now move on to begin phasing out third-party cookies. In this Cookie Countdown series, we will take you through the timeline and immediate actions you can take to ensure your sites are prepared.[13]

At the same time, it may feed into the narrative that even data protection is served best by private parties instead of public institutions set up especially for that purpose.

Still, seeing the persistent problem of cookies, the fact that it has been clear for more than a decade that most cookie-consents do not meet the various legal requirements and that this has an impact on the legitimacy of and support for both the GDPR and DPAs, me and the DPA representatives had an interesting discussion where I tried to push them to do more. To them, all they could do is assess in each and every individual case whether a cookie was put on a device in a legitimate fashion, requiring at least an individual assessment per website, its design, terms and conditions and privacy policy, but preferably also of each individual data subject. Obviously, this is so time consuming that it is impossible to do much about the hundreds or thousands of cookie-requests a data subject is faced with.

13 <https://developers.google.com/privacy-sandbox/blog/cookie-countdown-2023oct>.

While this mainly private law approach certainly has its merits, I suggested to adopt a public law approach and start from data protection as a fundamental human right. Under the human rights framework, such as the European Convention on Human Rights (ECHR) of the Council of Europe,[14] an interference with a right is only permissible if it is 'necessary in a democratic society'.[15] The European Court of Human Rights has made clear that this means that for any interference to be legitimate, it needs to accord to the principles of necessity, proportionality and subsidiarity. The Charter of Fundamental Rights of the European Union,[16] specifies:

> In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.[17]

It also harbors the proportionality principle:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[18]

To a large extent, necessity, proportionality and subsidiarity are also the guiding principles of the GDPR, as embedded in the data protection principles of Article 5. The purpose of the data processing initiative must be precisely defined (purpose specification principle), the data collection must be limited to that specific purpose (data minimisation principle) and the data may, in principle, not be further processed for different purposes (purpose limitation principle). The data must be deleted when the goal for processing has been reached (storage limitation principle) and the data controller must make sure that parties, either within or outside their organization, do not gain unlawful access to the data, because they might and will use those data for different (unlawful) purposes (integrity and confidentiality principle). These are all principles that crystallise in further detail what necessity, proportionality and subsidiarity mean in the data protection context, while the lawfulness principle is essentially a copy of the 'in accordance with the law principle' from Article 8 ECHR.

It seems logically intuitive to hold that necessary or functional cookies could meet the necessity requirement, while other cookies, which are not necessary or functionally related to the requested service, do not. This would mean that that roughly, two types

14 Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950.

15 Article 8 ECHR.

16 Charter of Fundamental Rights of the European Union (2000/C 364/01).

17 Art 52 para 3 CFREU.

18 Art 52 para 1 CFREU.

of cookies could be distinguished. Those which are necessary and/or functional, and those that are not. The e-Privacy Regulation,[19] which is currently under discussion and would replace the e-Privacy Directive in time, makes a clear distinction between cookies based on necessity and those based on consent:

> The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or (b) the end-user has given his or her consent; or (c) it is necessary for providing an information society service requested by the end-user; or (d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.[20]

For cookies that are necessary, no consent is required; for example, necessary cookies can be based on contractual agreements or the legitimate interest of the data controller.[21] As unnecessary and non-functional cookies do not meet the necessity bar, they are prohibited per se, I argued.

Admittedly, this is a bit of a stretch, because it would render the reference to consent in the e-Privacy Directive redundant, but it would have the advantage that there is no longer a need to assess per individual cookie whether it has been put on a device legitimately. The response, however, was perhaps even more audacious. The representatives of the DPA interpreted the GDPR as a fully private law instrument, which ultimately depends on the consent of the data subject. The standards in Article 5, for example, rest on the interpretation of the data subject. Suppose a baker, they said, had a security camera monitoring the bakery for security purposes. If the baker asks their customers whether they would agree to storing the data for an indefinite period, and they would, this would not run counter to the storage limitation principle. If the baker asks their customers whether the data can be sold to a travel agency, and they consent, such does not run counter to the purpose limitation principle. If the baker asks the customers to provide them with their marital status and political affiliation, that does not run counter to the data minimisation principle if the data subjects consent to that. Ultimately, the representatives of the DPA argued, the data protection principles are subjective notions to be agreed on between the data controller and the data subject, not objective notions to be interpreted by the DPA.

We are proud and honoured to present two enticing opinions. Larry Frohman unveils the origins of German privacy and data protection law and links that to the rise of new

19 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 - 2017/03 (COD).

20 Art 8 proposed e-Privacy Regulation.

21 Art 6 para 1 sub b and f GDPR.

surveillance powers and practices. Martine van Elk goes back even further, and gives a tour of the meaning and relevance of privacy in early modern British society.

In the articles section, we have two contributions on neuroprivacy. Marta Sosa Navarro discusses in particular the workplace and the accessibility of mental personal data about employees to employers. She questions whether EU law is capable of providing adequate protection to people in vulnerable positions. Robert Field compares American and European legislation in the field of neuroprivacy, uncovers their strengths and shortcomings and carves out paths for overcoming those weaknesses. In addition, Maitrayee Pathak compares the multitude of recent EU data regulations and assesses to what extent they succeed in establishing a single data market that is geared towards innovation and competition. Finally, Gauthier Chassang and Lisa Feriol home in on the concept of data altruism and the interplay between several EU regulations, in particular the Data Governance Act and the General Data Protection Regulation.

In the reports section, led by Mark Cole and Christina Etteldorf, a report on data portability in Australia, written by Natalia Jevglevskaja and Ross Buckley, can be found, as well as a perspective on the CNIL' penalty imposed on Amazon, authored by Sven Braun, and an analysis of the interplay between research and data protection regulations in Malta, penned by Mireille Caruana and Roxanne Meilak Borg. There are two additional reports in the practitioner's corner. Paul Grassl, Nina Gerber and Max von Grafenstein offer a perspective on the effectiveness of consent notices; Dominika Kuźnicka-Błaszkowska assesses the use of Article 15 GDPR and the effects thereof.

In the case note section, led by Maria Tzanou, three cases are discussed. Suzanne Nusselder explains jurisprudential standards on the required technical and organisational security measures. Jan Horstmann maps the CJEU's approach to credit rating agencies and profiling, in the recent landmark case. Finally, Robin Vandendriessche, Seppe Maes and Caroline Buts shed light on the yet another case in the Google antitrust saga.

In the book review section, led by Gloria Gonzalez Fuster, two books are discussed. Niovi Vavoula assesses the book by Quintel on migration and border control, a field that is increasingly datafied. Diana Sancho draws attention to a book that not all readers of EDPL will have spotted, namely the latest output of Rodríguez Pineau and Torralba Mendiola.

Finally, this edition also offers something new, something that we plan to do every year, namely a reflection on the past year and an overview of the most important cases, European and national developments and books that appeared last year. Maria provides the reader with an overview of the CJEU cases from 2023, while I do so for the ECtHR jurisprudence. Christina givens an overview of the most important developments for the EDPS, the EDPB, the DPAs and the national courts. Gloria presents the books that the editorial board members of EDPL have suggested for reading.

For those interested in submitting an article, report, case note or book review, please e-mail our Executive Editor Nelly Stratieva (<stratieva@lexxion.eu>) and keep in mind the following deadlines:

– Issue 3/2024: 15 July 2024;
– Issue 4/2024: 15 October 2024;
– Issue 1/2025: 15 January 2025.

Bart van der Sloot
Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University, Netherlands