eLaw
Working Paper Series

No 202ť/00! - ELAW– 202ť

Universiteit Leiden
eLaw

Discover the world at Leiden University

18. The role of consent in an algorithmic society – Its evolution, scope, failings and re-conceptualization

Bart Custers, Eduard Fosch-Villaronga, Simone van der Hof, Bart Schermer, Alan M. Sears and Aurelia Tamò-Larrieux

1. INTRODUCTION

Consent plays an essential role in the processing of personal data. In the General Data Protection Regulation (GDPR), it is one of the grounds for lawfulness of processing personal data, perhaps even the most important and most often used ground and indeed the only ground that does not involve a necessity. In the context of privacy and data protection, consent is usually focused on informational self-determination, a concept dating from the 1960s when, with increased data processing capabilities, the issue of data protection first emerged. The core idea of consent is that each person should be able (and entitled) to determine for himself/herself when, how, and to what extent information about him or her is used and for which purposes. This idea is based on the underlying notion that human beings (data subjects in the context of privacy and data protection) make conscious, rational, and free choices.

Throughout the development of data protection law from the 1960s, the inclusion of the concept of consent in different pieces of legislation was progressive. The Hessen Act was the first data protection law in the world, and it introduced the idea of *Zustimmung,* which means approval. In the beginning, however, the concept of consent was not that preeminent. While the first Austrian Data Protection Act from 1978 and the Norwegian Act relating to Personal Data Registers of 1978 included the notion, others did not, like the Swedish Data Act from 1973. Others struggled to incorporate it over time, like France and Belgium, who had it for medical data only in their laws from the 1990s.[1] From these pieces of national legislation, the Council of Europe Committee of Ministers Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector emerged that used the term consent to authorize the use of personal information.[2] Much later, the Data Protection Directive 95/46/EC incorporated consent on a Union level in Article 7(a) as a lawfulness ground. Even though a growing body of literature already illustrated the failures of consent at that time,[3] consent still

[1] CIPIL, 'European Data Protection - National Laws: Current and Historic' (2020) https://www.cipil.law.cam.ac.uk/resources/european-data-protection-national-laws-current-and-historic accessed 1 July 2021.

[2] Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013).

[3] Alessandro Acquisti and Jens Grossklags, 'Privacy and rationality in individual decision making' (2005) *3*(1*) IEEE Security &* Privacy https://ieeexplore.ieee.org/document/1392696 accessed 1 July 2021; Ekaterina Muravyeva, José Janssen, Marcus Specht, and Bart Custers, 'Exploring solutions to

plays a prominent role in the current legal framework, the GDPR, while scholars continue to stress its flaws in different contexts.[4] For instance, parental consent is supposed to contribute to the protection of children's personal data. However, this assumption may be questioned, and, moreover, parental consent may interfere with children's rights.[5]

Policymakers agreed on how consent must be obtained to enhance the utility of consent: opt-in consent became the default, and consent notices have to be 'clear, concise and not unnecessarily disruptive to the use of the service for which it is provided'.[6] How these criteria transform into practice is difficult to say. The GDPR suggests that information to data subjects could be provided along with standardized icons that are 'easily visible, intelligible, and clearly legible manner, a meaningful overview of the intended processing'. However, no official action has been taken yet to develop such standardized icons, and companies visualize consent notices in a wide variety of ways.[7]

Consent as a legal basis for processing is predicated on the notion that data subjects make a conscious decision about the processing of personal data after a careful process of deliberation and risk assessment. While, in theory, such consideration would lead to rational choices about data processing, there is a growing body of literature that claims this is not what is happening in practice.[8] Informed decision-making by individuals is negatively influenced by

---

the privacy paradox in the context of e-assessment: informed consent revisited' (2020) 22(3) *Ethics and Information Technology* https://link.springer.com/article/10.1007/s10676-020-09531-5 accessed 1 July 2021.

4 Bert-Jaap Koops, 'The trouble with European data protection law' (2014) 4(4) *International Data Privacy Law* https://academic.oup.com/idpl/article-abstract/4/4/250/2569063 accessed 1 July 2021; Menno Mostert, Annelien L. Bredenoord, Monique CIH Biesaart, and Johannes JM Van Delden, 'Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach', (2016) 24(7) *European Journal of Human Genetics* https://www.nature.com/articles/ejhg2015239 accessed 1 July 2021; Shara Monteleone 'Addressing the Failure of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation' (2015) 43:69 *Syracuse J. Int'l L. & Com*. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/sjilc43&section=5&casa_token=CDdfZ080OqgAAAAA:_8CDQAnkOAhW-KGtX9hlS1rx4yXuKc4qHDW0ezkej3mMp05_ab5gQJQk4F_TJZmYXcMxHRLtoA accessed 1 July 2021; Eoin Carolan, 'The continuing problems with online consent under the EU's emerging data protection principles' (2016) 32(3) *Computer Law & Security Review* https://www.sciencedirect.com/science/article/abs/pii/S0267364916300322?via%3Dihub accessed 1 July 2021; Lilian Edwards 'Privacy, security and data protection in smart cities: A critical EU law perspective' (2016) 2:28 *Eur. Data Prot. L. Rev.* https://heinonline.org/HOL/Page?handle=hein.journals/edpl2&div=8&g_sent=1&casa_token=7FBDknvtGRIAAAAA:Fh5vDdwpApai0N-F1D9GfBLjBUWeml60jE0SO6aQcslq8ceG0l9DFWQ_1tRZQ0c0mzSjDQqEFA&collection=journals 1 July 2021.

5 Simone van der Hof, ''I agree, or do I: a rights-based analysis of the law on children's consent in the digital world' (2016) 34 *Wis. Int'l LJ 34* 409; Simone van der Hof, Eva Lievens and Ingrida Milkaite 'The protection of children's personal data in a data-driven world. A closer look at the GDPR from a children's rights perspective' in Ton Liefaard, Stephanie Rap, and Peter Rodrigues *Monitoring Children's Rights in the Netherlands: 30 years of the UN Convention on the Rights of the Child* (Leiden University Press (LUP) Leiden University Press 2019).

6 Recital 32 GDPR.

7 Ekaterina Muravyeva, José Janssen, Marcus Specht, and Bart Custers, 'Exploring solutions to the privacy paradox in the context of e-assessment: informed consent revisited' (2020) 22(3) *Ethics and Information Technology* https://link.springer.com/article/10.1007/s10676-020-09531-5 accessed 1 July 2021.

8 Alessandro Acquisti and Jens Grossklags, 'Privacy and rationality in individual decision making' (2005) *3*(1) *IEEE Security & Privacy* https://ieeexplore.ieee.org/document/1392696 accessed 1 July

factors such as bounded rationality, incomplete information, time limitations, and cognitive biases. Data controllers may exploit these factors through design choices within consent flows. So-called 'dark design patterns' may be leveraged to nudge or even trick data subjects into giving consent, capitalizing on the limitations of the human brain. Examples of this can be seen in cookie consent flows. Data controllers use cognitive biases such as the 'middle option', for instance, to nudge users into choosing cookie settings that enable tracking for marketing purposes. Another example is the exploitation of the 'default effect'. By presenting the most privacy infringing cookie setting as the default option and requiring the data subject to make an effort to change these settings, the chance of getting the form of consent that is most desirable for the data controller is intentionally maximized.

In this chapter, we address the role of consent in data protection law by explaining first how consent came to existence. Taking a historical perspective, we explain how the concept evolved in different countries, across various pieces of legislation, and for different data subjects, including children. Then, we look at the EU level how consent was established in Directive 95/46/EC and the General Data Protection Regulation and explore its scope and what consent entails by looking at the rulings from the Court of Justice of the European Union, the previously called Article 29 Working Party (WP29) opinions, and the newly issued guidelines by the European Data Protection Board.[9] Building upon the rich body of scholarship that has stressed and focused on the failure of consent, we tie this narrative into the past, present, and future so as to explain why consent has persisted over time to be widely used today and why it is likely to continue to be a central pillar of data protection law. We conclude this chapter by explaining the rationale behind the role of consent in an increasingly algorithmic society. In this respect, we describe the purpose consent serves in a hyper-connected society and explore its *quo vadis* by assessing recent proposals concerning interactive, dynamic consent models, which are already used in research and shared-economy business models.

2. ON THE ORIGINS AND EVOLUTION OF CONSENT

2.1 Origins

To understand the role of consent in data protection law, it is important to understand how this concept came to be. Consent has always been at the basis of personal data protection.

2021; Daniel Kahneman, *Thinking, Fast and Slow,* (Macmillan, 2011); Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness* (Penguin 2009); Pelle Guldborg Hansen, and Andreas Maaløe Jespersen 'Nudge and the manipulation of choice: A framework for the responsible use of the nudge approach to behaviour change in public policy' (2013) 4:1, *European Journal of Risk Regulation* https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/nudge-and-the-manipulation-of-choice/D1ED64479FF868BD79FFE90E76A4AB54 accessed 1 July 2021; On Amir, and Orly Lobel 'Stumble, predict, nudge: How behavioral economics informs law and policy' (2008) 108 *Colum. L. Rev.* https://heinonline.org/HOL/Page?handle=hein.journals/clr108&div=57&g_sent=1&casa_token=sSRScJ-G_cwAAAAA:EjxFFs9GdGEeoccbJePlkEEhfC1WY4KvJZc9RmPaW-N_-WUh72vMQbHj9IIG0gBNxU1zNnC1qA accessed 1 July 2021.

[9] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf last accessed 4 May 2020.

This is because the development of data protection and privacy are closely related to each other. In Europe, privacy, or more precisely the right to privacy, originally placed emphasis on the protection of the private and family life (for instance, see Art 8 European Convention on Human Rights, which was drafted in 1950, well before the concept of personal data protection was developed). Also, the right to privacy is closely related to bodily integrity. Both the protection of private and family life and the protection of the body strongly hinge on the concept of consent. If someone enters your home with your consent, no right to privacy is violated. If someone touches you with your consent, no bodily integrity is violated. However, if these things happen without consent, these basic rights are violated. In other words, the presence or absence of consent determines whether specific actions or behaviour are allowed.

Whereas the conceptualization of the modern right to privacy came into existence at the end of the 19th century,[10] the right to data protection followed much later, in the second half of the 20th century, with the rise of information technology and its increased data processing capabilities. Usually, privacy is considered to have several different aspects, including spatial aspects (private home), relational aspects (private communication), physical aspects (bodily integrity), and also informational aspects (private information). Obviously, these aspects can sometimes overlap. The aspect of informational privacy was first developed in the 1960s, when it was argued that each person should have a right to determine for himself/herself when, how and to what extent information about him or her is communicated to others.[11] This approach, putting personal autonomy and informed consent in a central position, is usually referred to as *informational self-determination*, although this term was only first used in 1983 in a landmark ruling of the German Constitutional Court.[12]

The term 'consent' was 'present from the very beginning' in data protection, although not as a right of the data subject.[13] Although not using the word 'consent' expressly, the fifth principle of the Annex of the Council of Europe Committee of Ministers, Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector of 1973 breathed into existence the idea of consent.[14] In its words, 'without appropriate authorisation, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties'. According to Kosta, the authorized use of information had a broad meaning, ranging from a general permission granted by law to a license given by a controlling authority.[15] However, the idea that consent was an individual right would appear later on, since this *authorization* was external and not from the data subject herself.

The Council of Europe Committee of Ministers, Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector came into effect in

---

[10] Louis Brandeis and Samuel Warren, 'The right to privacy' (1890) 4(5) *Harvard Law Review*.

[11] Alan F. Westin, *Privacy and Freedom* (The Bodley Head 1967).

[12] BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfGE 65, 1.

[13] Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013).

[14] Council of Europe Committee of Ministers, Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector. Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies, available at https://rm.coe.int/1680502830 (accessed 23 June 2020).

[15] Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013).

1974 as a response to the threats to privacy arising from the public sector.[16] There is no reference to consent in this resolution, probably because the government needs a legal ground for processing information about individuals. Still, this shows a dichotomy between the public and private sectors in the understanding of consent's role. In this chapter, we focus on the private sector only.

Since then, a lot of successive legislation has been created in the area of data protection law. In the EU, regulation proceeds from the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the so-called OECD privacy principles (Tene, 2013). These principles, to some extent inspired by the abovementioned Hesse Data Protection Act,[17] put informational self-determination and data subject rights in a central position. The OECD principles were incorporated in the Council of Europe's 1981 Treaty of Strasbourg, the Convention for the protection of individuals with regards to the automatic processing of personal data in 1981 (CoE Convention 108).[18] The aim of the Convention 108 was (and is) to ensure early on harmonization of data protection acts among Member States.[19] Today, this international treaty counts 55 ratifications, including European States and third countries such as Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay.[20] Initially, the term consent was not prominent in the text and only appeared once to prevent designated authorities to offer assistance to a data subject abroad without her consent (Art 15.3 CoE Convention 108).[21] Years later, in 2016, the notion of consent has been further specified in the Convention, and, referring to the lawful basis for processing personal data, it stated 'the data subject's consent must be freely given, specific, informed and unambiguous' and stressed that 'expression of consent does not waive the need to respect the basic principles for the protection of personal data [...] and the proportionality of the processing.'[22]

2.2 The EU Data Protection Directive (Directive 95/46/EC)

Over time, with each legislative reform, the right to data protection has been gradually further disconnected from the right to privacy. Simultaneously, the right to data protection has increas-

---

[16] Council of Europe Committee of Ministers, Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector. Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies, available at https://rm.coe.int/16804d1c51 (accessed 23 June 2020).

[17] The German text in the Hesse Data Protection Act uses the word 'Zustimmung', which can be translated into consent, but also into approval. The Federal German Data Protection Act of 1997 (Bundesdatenschutzgesetz, BDSG) uses the word 'Einwilligung'.

[18] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS. 108) (28.01.1981).

[19] Interestingly, when drafting the 1978 data protection act in France, the French legislator and the French Data Protection Authority (Commission nationale de l'informatique et des libertés, CNIL) assumed that consent would not be useful and that one would not use this as a legal ground: 'cet article ne servait en réalité à rien et n'ont pas souhaité 'utiliser' (Debet et al. 2015). Hence, the French data protection act did not contain a concept of consent in 1978.

[20] *See* the full list of members here: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=Jdfyn0PF accessed 1 July 2021.

[21] Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013).

[22] *See* https://rm.coe.int/convention-for-the-protection-of-individuals-with-regard-to-automatic-/16806b6ec2 para 40 accessed 1 July 2021.

ingly been regulated on a higher level, eventually even being adopted in the list of fundamental rights in the Charter on Fundamental Rights of the EU (CFR). Fundamental rights typically are inherent, inalienable, universal, indivisible and interdependent, putting human dignity and autonomy at the center. This also applies to the fundamental right to data protection in Article 8 of the CFR. This development of the right to data protection and the underlying notions of consent are strongly rooted in a long tradition of humanism, in which the value and agency of human beings is emphasized, and in a firm (though not always correct) belief in rational choice theory, which assumes that people base all their choices and behaviour on rational thinking.

Convention 108 provided further guidance for national governments when drafting national data protection laws. In 1995, influenced by both Convention 108 and the OECD principles, the EU adopted EU Directive 95/46/EC, the so-called Data Protection Directive (DPD), causing all EU Member States to harmonize national data protection laws.[23] In the initial Commission Proposal for the Directive, consent was presented as a right of the data subject under Article 12, which was ultimately removed and the definition of consent was placed under Article 2 of the Directive.[24] There, consent was defined as 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.[25] The DPD only stated that the data subject had to 'signify' consent without clarifying that consent required a clear affirmative action from the data subject or without explaining other concepts such as *freely given*, *specific*, *informed* further.[26] However, the interpretation of Article 2 of the DPD was highly dependent on the Member States' understanding of consent and the interpretation by data protection authorities and courts. While the WP29 never acknowledged the possibility of implied consent,[27] other data protection authorities were more lenient in this regard.[28] Further, consent was given a primary position in comparison to other legal bases for the processing of personal data under Article 7 by some countries.[29]

Although the DPD represented a reasonable harmonization effort, it was not very precise. For instance, it did not specify what methods the controller could use to obtain valid consent or fulfil their obligation to keep evidence of the data subject's consent. Other important aspects for the data subject, such as the possibility to withdraw consent or that silence is not consent, were only achieved and made expressly clear in the GDPR.

---

[23] Bart Custers, Alan M. Sears, Francien Dechesne, Ilina Georgieva, Tommaso Tani, and Simone van der Hof, *EU Personal Data Protection in policy and Practice* (TMC Asser Press 2019).

[24] Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013).

[25] Art 2(h) DPD.

[26] Detlev Gabel and Tim Hickman, 'Chapter 8: Consent – Unlocking the EU General Data Protection Regulation' (2019). White & Case https://www.whitecase.com/publications/article/chapter-8-consent-unlocking-eu-general-data-protection-regulation#:~:text=%22Consent%22%20means%20any%20freely%20given,subject%20must%20%22signify%22%20consent accessed 30 June 2020.

[27] Article 19 Working Party, Opinion 15/2011 on the definition of consent, Adopted on 13 July 2011, 01197/11/EN WP187.

[28] For instance, implied consent was considered valid in some circumstances under the UK Data Protection Act. See Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013).

[29] This was the case for the Czech Republic, France, Greece, and Portugal, and, to a lesser extent, Austria, Germany, and Spain. See Douwe Korff 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments' (2010) Working Paper No.2 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1638949 accessed 1 July 2021.

The DPD was silent on potential vulnerabilities with respect to the processing of personal data of children, but some national data protection laws at the time provided for extra protection for children, such as the Spanish[30] and Dutch data protection acts,[31] by providing a minimum age for valid consent and requiring parental consent for children below that age.[32] Moreover, pursuant to the UN Convention of the Rights of the Child 1989, it was (and still is) generally recognized in Europe (and beyond) that the fundamental rights of children (including their data protection rights in the EU[33]) require special attention and explanation and should generally be applied more rigorously. Thus, even in the absence of specific provisions in data protection legislation, the special interests of children already had to be taken into account at the time of the DPD and it had to be assumed that children under a certain age were not perceived as (sufficiently) capable to make their own decisions (e.g., in the form of consent to the processing of their personal data).[34] [35]

---

[30] Art 13 Spanish Data Protection Law (*Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal)*.

[31] Art 5 of the Wet bescherming persoonsgegevens, 2000.

[32] Terri Dowty and Douwe Korff Protecting the Virtual Child: The Law and Children's Consent to Sharing Personal Data (ARCH 2009).

[33] However, the Children's Rights Committee extends the right to data protection in the case of children to the rest of the world by expressly including it in Article 16, UN Convention on the Rights of the Child 1989, see General Comment No 25 on children's rights in relation to the digital environment (final version is accepted but not yet published; https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx accessed 19 January 2022.

[34] Children (i.e., individuals below 18) are people in development and their fundamental rights deserve special protection. On the basis of the UN Convention on the Rights of the Child 1989 (CRC), parents are primarily responsible for their children (Art 18 CRC) and depending on their evolving capacities (Art 5 CRC), as they grow older, children are increasingly deemed to be able to make their own decisions. This is also reflected in data protection rules that stipulate that children are allowed to decide on the processing of their personal data before the age of 18 (although the ages may vary from 13 to 16 per Member State). In addition, the best interest of the child principle (Art 3 CRC) will have to be taken into account more generally in the application of data protection rules, in which the best interest of the child must be a primary consideration in relation to all actions, both public and private, concerning a child. The best interests principle is a threefold concept: (1) a substantive right: the best interests of children must be given due weight in a balancing of interests (which may not be easy given the powerful interests of some online platforms), (2) a fundamental legal principle of interpretation: the most child-friendly interpretation must be given to a provision if it is open to multiple interpretations, and (3) rule of procedure: decisions aimed at children must be accompanied by an impact assessment and procedural safeguards that do justice to their interests; see Committee on the Rights of the Children (2013, 3).

[35] See Terri Dowty and Douwe Korff Protecting the Virtual Child: The Law and Children's Consent to Sharing Personal Data (ARCH 2009); A case in point that Dowty and Korff mention is France where the CNIL stated that the guarantees offered by the law to all must be even more rigorous when minors are involved and took a clear stance on the necessity of parental consent in the processing of children's sensitive personal data and pictures, and the transfer of data to third parties in the case of games (of chance). Another mentioned case in Dowty and Korff is the Belgian data protection authority that issued guidelines at the time for the protection of children's privacy on the Internet which requires parental consent in cases where the child has not reached the age of discernment or in particular instances (processing of sensitive personal data, transfer of data to third parties, marketing, publicly available information).

3. THE SCOPE OF CONSENT WITHIN THE GDPR

Directive 95/46/EC was replaced by the General Data Protection Regulation (GDPR) in May 2018. The GDPR is a further harmonization of EU data protection law, since it is directly binding for all citizens in all EU Member States. With each of these developments, the conditions for consent have been strengthened.[36] The Article 4(11) GDPR defines consent as follows:

> 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Elaborating on this definition, different institutions, judgments, and literature shaped the notion of consent further. Consent must be obtained before the data processing activity, not subsequently.[37] Moreover, the data subject has to have the possibility to withdraw consent at any time, and the controller must be able to demonstrate that the data subject has consented.[38] In certain instances, consent must also be explicit.[39] Besides, there is a discussion in Europe on whether the data subject must personally give his or her consent (German tradition) or whether a third party could consent on an individual's behalf as long as it has the authority to do so.[40]

Further protection of people is one of the main drivers for data protection law. For instance, data subject rights are a central element in data protection.[41] However, the strong focus on consent in data protection law also reveals another driver, namely the empowerment of people.

---

[36] Bart W. Schermer, Bart Custers, and Simone van der Hof, 'The crisis of consent: How stronger legal protection may lead to weaker consent in data protection' (2014) 16(2) *Ethics and Information Technology* https://link.springer.com/content/pdf/10.1007/s10676-014-9343-8.pdf accessed 1 July 2021.

[37] Fashion ID, Case C-40/17, [2019] (ECLI:EU:C:2019:629), at para 102:

> With regard to the consent referred to in Article 2(h) and Article 7(a) of Directive 95/46, it appears that such consent must be given prior to the collection and disclosure by transmission of the data subject's data. In such circumstances, it is for the operator of the website, rather than for the provider of the social plugin, to obtain that consent, since it is the fact that the visitor consults that website that triggers the processing of the personal data.

Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP 259 rev.01, 10 April 2018); Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal, 'Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence' (2020) Proceedings of the 2020 CHI conference on human factors in computing systems, https://dl.acm.org/doi/abs/10.1145/3313831.3376321?casa_token=hUw6tYBhxBwAAAAA:QS1ngSx-vEHnm90FZ24KxUUA-iXeqHr062mKjV7CKa7m5jEeor-eXQ7dvnZ7szIZRhwLOMPZbQ accessed 1 July 2021.

[38] Art 7(1) and (3) GDPR; European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf last accessed 4 May 2020.

[39] For example, where special categories of data are processed under Art 9 GDPR, or when automated decision-making is used under Art 22 GDPR.

[40] Sebastian Dienst 'Lawful processing of personal data in companies under the General Data Protection Regulation' in Daniel Rücker and Tobias Kugler, *New European General Data Protection Regulation: A Practitioner's Guide* (Nomos Verlagsgesellschaft 2017); ICO (2020b) Consent, https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent-1-0.pdf accessed 30 June 2020.

[41] Helena Ursic *Uncontrollable: Data subject rights and the data-driven economy* (Leiden University, The Netherlands, PhD thesis2019).

For the data economy, this might make sense, as it could empower informed consumers.[42] The focus on consent, however, has also been used as a starting point in contexts where it may not work well. For instance, the separate regime for personal data in criminal law, regulated by EU Directive 2016/680 (the Law Enforcement Directive) is based on transparency, consent and control, even though this is not always realistic in criminal investigations.[43]

Although consent is not the only valid legal basis for processing personal data, it is the only one that is not based on necessity – the other legal bases in Article 6 of the GDPR are (necessity for) performance of a contract, legal obligation, vital interest of the data subject, public interest, and legitimate interest of the data controller. Even a contract as a legal basis assumes a necessity, i.e., processing personal data is only allowed to the extent needed to perform the contractual obligations. Furthermore, a contract also obviously includes some form of consent, since people are at liberty to decide for themselves whether they want to enter into a contract or not.[44] However, consent is only valid if the data subject can genuinely exercise a real choice, not bundled with the acceptance of additional terms or conditions, or if its performance is indissociable of a request for the processing of personal data unnecessary for the actual performance of that contract.[45] It will not be considered *freely given* if the data subject cannot refuse, withdraw consent without impediment, or when a clear power imbalance between the data subject and the controller exists (i.e., when the controller is a public authority, insurance business, or an employer).[46] Not every imbalance makes free choice impossible, and only a case-by-case analysis will determine it, but that the imbalance needs to be of some significance to prevent users from having a genuine choice.

The information provided to the data subject as part of the request for consent should allow the data subject to understand to what he or she agrees.[47] Therefore, the information required

---

[42] Bart Custers, and Daniel Bachlechner, 'Advancing the EU data economy: Conditions for realizing the full potential of data reuse' (2017) 22:4 *Information Polity*.

[43] Mark Leiser and Bart Custers, 'The Law Enforcement Directive: Conceptual challenges of EU Directive 2016/680' (2019) 5 *Eur. Data Prot. L. Rev.*

[44] Note however that in the case of minors, there is only legal capacity to enter a contract from a certain age; the GDPR is silent on this, however these ages are determined by the national contract laws of the Member States. See also Art 8(3) on the application of national contract law, rules on the validity, formation or effect of an agreement relating to a child with regard to consent in Art 8(1).

[45] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP 259 rev.01, 10 April 2018); E.G. González and P. De Hert, 2019 Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles. In *Era Forum*, Springer Berlin Heidelberg, *19*(4), pp. 597–621; Elena Gil González and Paul De Hert, 'Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles' (2019) 19(4) *ERA Forum* https://link.springer.com/article/10.1007/s12027-018-0546-z accessed 1 July 2021; Eleni Kosta, 'Article 7. Conditions for consent' In Christopher Kuner, Lee Bygrave, and Christopher Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[46] Lee Bygrave and Luca Tosoni 'Commentary on Article 4(1): Personal Data' Christopher Kuner, Lee Bygrave, and Christopher Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020); Eleni Kosta, 'Article 7. Conditions for consent' In Christopher Kuner, Lee Bygrave, and Christopher Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[47] CNIL, 'Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against Google LLC' 21 January 2019 https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf (accessed 30 June 2020).

and set out in the GDPR, which can be written, oral, or visual, needs to be clear and plain so that lay people can understand it.[48] The European Data Protection Board (EDPB) supervising GDPR compliance, stresses that data controllers will have to think about their target audience in advance,[49] and if it involves children,[50] it must ensure that the information is understandable to them (see also Art 12(1) GDPR).

Consent also needs to be an unambiguous indication of the data subject's preferences in an active motion or declaration.[51] A statement or an explicit affirmative action signifies agreement to the processing of personal data relating to him or her. However, silence, pre-ticked boxes, opt-out constructions that require an intervention from the data subject to prevent agreement, and also inactivity cannot constitute consent.[52] Instead, the data subject must take a deliberate action that indicates the acceptance of the proposed processing, by ticking an opt-in box, signing, selecting technical settings or preference dashboard settings, or responding to email consent requests.

From a moral perspective, consent requests fulfil a practical purpose, as they allow individuals to express their preferences, observing their autonomy and well-being. In a sense, a consent transaction also functions as a warning that there may be consequences of a particular choice, consequences that may be beneficial for the individual, but also consequences that may be non-beneficial or potentially harmful. With the many, many consent requests people are confronted with nowadays, consent to personal data-processing practices has become quite a mundane activity in the digital world.[53] When downloading apps to our smartphones, we – almost automatically – consent to the privacy policies associated with the particular services they provide. Also, when subscribing to social networking services, consenting to their privacy policies is inescapable. Another particularly visible practice is to ask internet users to accept cookies (i.e., small pieces of data stored on people's computers to 'remember' their actions and preferences). As a result of all these practices, everyone is quite familiar with consent requests nowadays.

---

[48] Recital 42 GDPR.

[49] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf last accessed 4 May 2020.

[50] Note that the GDPR does not define 'children' which is an unfortunate omission, however, it is reasonable to use the definition of Art 1 CRC unless the GDPR provides otherwise; see also Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013); Milda Macenaite and Eleni Kosta, 'Consent for processing children's personal data in the EU: following in US footsteps?' (2017) 26 (2) *Information & Communications Technology Law*; Simone van der Hof, Eva Lievens and Ingrida Milkaite 'The protection of children's personal data in a data-driven world. A closer look at the GDPR from a children's rights perspective' in Ton Liefaard, Stephanie Rap, and Peter Rodrigues. *Monitoring Children's Rights in the Netherlands: 30 years of the UN Convention on the Rights of the Child*) Leiden University Press (LUP) Leiden University Press 2019).

[51] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP 259 rev.01, 10 April 2018).

[52] Recital 32 GDPR. The ECJ has also stated that a pre-ticked checkbox does not constitute valid consent (*Planet49*, Case C-673/17, [2019] (ECLI:EU:C:2019:801), at paras 62–63.

[53] Bart Custers, Francien Dechesne, F., Wolter Pieters, Bart W. Schermer and Simone van der Hof 'Consent and Privacy' in: Peter Schaber, and Andreas Müller (eds.) *The Routledge Handbook of the Ethics of Consent* (Routledge 2018).

In the case of information society services[54] offered directly to a child,[55] children can consent to the processing of their personal data when they have reached the age of digital consent, as stipulated by Article 8 of the GDPR.[56] This age is not determined uniformly across the EU[57] and Member States are free to choose an age below 16 as long as it is not below 13. This has created a veritable patchwork of ages in which every possibility – namely 13, 14, 15 and 16 – occurs.[58] When a child is under the age of digital consent, parents (or a child's legal representative) must consent to the processing of children's personal data.[59] Article 8 of the GDPR holds an implicit requirement of age verification given that it must be clear whether the provision applies in relation to a data subject, although it only needs to be verified when a person says they are over the age of digital consent.[60] In the case of parental consent, the consent must be verified with available technology as coming from the parent or legal representative of the child (Art 8(2) GDPR).[61] In the event that the law allows children to give consent themselves, specific attention will have to be paid to adequately informing children about the processing

[54] An information society service is 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services' (Art 1(b), Directive (EU) 2015/1535); such services include basically any commercial online service.

[55] Not 'offered directly to child' are services directed at over 18 with no evidence to the contrary that children still have access. The use of age verification methods that can easily be circumvented is therefore discouraged in such a case. Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP 259 rev.01, 10 April 2018).

[56] See on the legislative history of this provision: Milda Macenaite and Eleni Kosta, 'Consent for processing children's personal data in the EU: following in US footsteps?' (2017) 26 (2) *Information & Communications Technology Law*.

[57] The reason is that the determination of the age of consent is seen as part of the national private law competence of Member States; Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013).

[58] For an overview, see Ingrida Milkaite, and Eva Lievens 'Children's rights to privacy and data protection around the world: challenges in the digital realm' (2019) 10:1 *European Journal of Law and Technology*. For the reasoning behind choices in some Member States, *see* Simone van der Hof, Eva Lievens and Ingrida Milkaite 'The protection of children's personal data in a data-driven world. A closer look at the GDPR from a children's rights perspective' in Ton Liefaard, Stephanie Rap, and Peter Rodrigues. *Monitoring Children's Rights in the Netherlands: 30 years of the UN Convention on the Rights of the Child* (Leiden University Press 2019). Moreover, there is no uniform rule for determining the applicable law in this respect to the detriment of legal certainty for businesses.

[59] Parental consent is part of the special protection that children under the GDPR have with regard to the processing of their personal data because – as Recital 38 states – they are 'less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data'. This protection applies in particular but not exclusively in the case of 'marketing or the creation of personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child'. Note that according to Recital 38 parental consent is not necessary when preventive or counseling services are offered directly to a child.

[60] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP 259 rev.01, 10 April 2018), 25.

[61] In practice questions exist as to what are adequate verification methods for age and parental consent, *see* Simone van der Hof, Eva Lievens and Ingrida Milkaite 'The protection of children's personal data in a data-driven world. A closer look at the GDPR from a children's rights perspective' in Ton Liefaard, Stephanie Rap, and Peter Rodrigues. *Monitoring Children's Rights in the Netherlands: 30 years of the UN Convention on the Rights of the Child* (Leiden University Press 2019).

of personal data so that they really understand to what they are consenting.[62] Furthermore, consent can be reconfirmed by the child itself as soon as he or she reaches the age of digital consent; although parental consent remains a valid ground for data processing when the child takes no action.[63] Moreover, the data controller must inform the child that it can withdraw consent given by the parent before it reaches the age of consent.[64]

4. FAILURES OF CONSENT

As stated above, the legal grounds 6(b) through 6(f) of the GDPR for processing personal data are not conditional on the consent of the data subject. When the processing of personal data is necessary for the goals and interests described in paragraphs (b) through (f), the processing is deemed legitimate, regardless whether the data subject approves.[65] Conversely, when data processing cannot be legitimized by one of these grounds, consent is the only option that remains. One could argue that consent is thus the legitimate ground of last resort: only when processing cannot be legitimized by one of the necessity grounds, the 'morally transformative' power of consent should be used.[66]

However, especially in the area of (online) marketing, consent seems to be the rule rather than the exception. One of the main reasons for this reliance on consent is that the data protection authorities do not consider using (intrusive) tracking and profiling for marketing or advertising purposes a legitimate interest.[67] This pushes data controllers towards consent as legal basis. Furthermore, consent provides the data controller with legal certainty: the data subject has clearly confirmed that he or she accepts the processing of personal data. With a legal basis like 'the legitimate interest of the data controller' (6(f) GDPR) there is far less certainty, as a data protection authority may disagree with the weighing of interests by the data controller.

---

[62] Recitals 39 and 58 GDPR; Art 12 GDPR; Simone van der Hof, Eva Lievens and Ingrida Milkaite 'The protection of children's personal data in a data-driven world. A closer look at the GDPR from a children's rights perspective' in Ton Liefaard, Stephanie Rap, and Peter Rodrigues. *Monitoring Children's Rights in the Netherlands: 30 years of the UN Convention on the Rights of the Child* (Leiden University Press 2019).

[63] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP 259 rev.01, 10 April 2018), 27.

[64] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP 259 rev.01, 10 April 2018), 27.

[65] The data subject does have the right to object to processing based on 6e or 6f GDPR as a legal ground (see Art 21 GDPR).

[66] Bart W. Schermer, Bart Custers, and Simone van der Hof, 'The crisis of consent: How stronger legal protection may lead to weaker consent in data protection' (2014) 16:2 *Ethics and Information Technology*.

[67] While direct marketing may be a legitimate interest (see Recital 47), data protection authorities argue that given the scope and nature of profiling, Art 6(f) of the GDPR will generally not provide a legal basis for processing, leaving only consent. See: Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679' (WP 259 rev.01, 10 April 2018), 15; European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf last accessed 4 May 2020. For more details on how this works, see Calders, Toon, and Bart Custers. 'What is data mining and how does it work?' in Bart Custers, Toon Calders, Bart W. Schermer and Tal Zarsky (2013) *Discrimination and Privacy in the Information Society* (Springer 2013).

Furthermore, if online services are also offered to children, the best interests of the child will have to be seriously considered when weighing up all the interests.[68] All this exposes the data controller to enforcement risks.

While consent is a commonly used legal basis for processing personal data, it does have a significant shortcoming: it places the burden of the risk assessment for data processing with the data subject. When asked for consent, the data subject must understand how data is being processed, what the potential risks involved are, and how they should weigh these risks against the benefits associated with the processing (e.g., free goods or services). It is highly questionable whether data subjects are willing and able to make such assessments. Insights from behavioural economics have cast serious doubt on the ability of data subjects to make rational decisions regarding personal data processing.[69] Data subjects have 'bounded rationality', meaning that due to constraints in understanding and available time, data subjects turn to simplified mental models and heuristics to make consent decisions.[70]

In particular the available time to assess a consent request plays a role. In many cases, people are unwilling to devote their time to reading lengthy privacy statements and consent notices. A study into the reading behaviour of privacy statements revealed for instance that on average the subjects spent a maximum of 90 seconds reading a privacy statement which would take a person between ten and 15 minutes to read in full.[71]

Users may also be nudged into giving consent by data controllers. Utz et al. have shown that the way in which consent request is structured and presented has a significant impact on the willingness of data subjects to consent.[72] Data controllers may tweak consent requests and opt-in flows in such a way that data subjects unwittingly consent to the processing of their personal data. So, while a user still theoretically has a free choice in this scenario, that choice is influenced significantly by the data controller.

It also needs to be noted that consent presupposes the freedom of the data subject and a more or less equal relation between the one asking and the one giving consent.[73] In many cases however, there is a significant disparity between data controllers and data subjects in terms of power. This is particularly the case in online environments where subjects are dependent

---

[68] See Simone van der Hof, Eva Lievens and Ingrida Milkaite 'The protection of children's personal data in a data-driven world. A closer look at the GDPR from a children's rights perspective' in Ton Liefaard, Stephanie Rap, and Peter Rodrigues. *Monitoring Children's Rights in the Netherlands: 30 years of the UN Convention on the Rights of the Child* (Leiden University Press 2019).

[69] See for instance: Alessandro Acquisti and Jens Grossklags, 'Privacy and rationality in individual decision making' (2005) *3*(1) *IEEE Security & Privacy* https://ieeexplore.ieee.org/document/1392696 accessed 1 July 2021; Alessandro Acquisti, Curtis Taylor, and Liad Wagman, 'The economics of privacy' (2016) 54(2) *Journal of Economic Literature*.

[70] Alessandro Acquisti and Jens Grossklags, 'Privacy and rationality in individual decision making' (2005) *3*(1) *IEEE Security & Privacy* https://ieeexplore.ieee.org/document/1392696 accessed 1 July 2021.

[71] Jonathan A. Obar and Anne Oeldorf-Hirsch, 'The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services' (2020) 23(1) *Information, Communication & Society*.

[72] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. '(un) informed consent: Studying GDPR consent notices in the field.' In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security* (2019).

[73] Free choice is a prerequisite for valid consent (see Art 4(11) GDPR).

on a small number of dominant market players.[74] Generally, the law seeks to remedy power imbalances by providing the weaker actor with stronger rights or restricting the behaviour of the stronger actor, thus restoring the balance of power. Consumer protection law is a good example of this: certain practices are considered unfair and therefore not allowed, regardless of the consent of the consumer. Consent in data protection largely ignores power imbalances and legitimizes any exploitation of power imbalances as long as the argument can be made that the consent was 'freely given'. Other than the limitations set by Article 7(4) of the GDPR (conditionality of consent), the GDPR is unclear when consent is no longer considered freely given. While data protection authorities have further clarified the notion of 'freely given', they have yet to go so far as to outright outlaw business practices, such as nudging, that clearly benefit from power imbalances.[75]

The above factors are exacerbated by the overreliance on consent as a legal basis. Overreliance on consent may lead to 'consent fatigue'. Ideally, a consent request functions as a warning, triggering the data subject to carefully assess the data processing and weigh the pros and cons of giving consent. However, the amount of consent requests presented to data subjects on a daily basis numbs users and takes away this effect.[76] This 'safeguard inflation' is a threat to the privacy of data subjects, as well as a threat to the validity of the mechanism of consent itself.[77]

To summarize, consent does not necessarily lead to empowerment. Bounded rationality and the abuse of power imbalances may limit the ability of data subjects to make choices that benefit them in the longer term. While consent can be revoked, negative effects are not always directly apparent to the data subject or they cannot be correlated to the consent previously given, leading to a false sense of empowerment.

On top of the problems already mentioned, from the perspective of children, consent can be problematic in a number of other ways as well. Firstly, a high level of protection of children – in the context of consent, but also more generally under the GDPR – leads in practice to children being excluded from online services. Currently, age verification is generally not so sophisticated that children would no longer have access to services (by entering an incorrect date of birth, you can still create an account). However, age verification is expected to become more adequate, if only because companies would otherwise fail to meet the requirements of the GDPR which could lead to hefty fines. Secondly, teenagers may find it annoying when their parents are required to keep watch over them. Parental consent is then seen by them as an invasion of their privacy.[78] A teenager exploring their sexual identity may not want their

---

[74] Elettra Bietti, 'Consent as a free pass: platform power and the limits of the informational turn' (2019) 40 *Pace Law Rev.*, 310; Alessandro Acquisti, Curtis Taylor, and Liad Wagman, 'The economics of privacy' (2016) 54(2) *Journal of Economic Literature*.

[75] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf last accessed 4 May 2020.

[76] Kip Viscusi 'Individual rationality, hazard warnings, and the foundations of tort law.' (1995) 48 *Rutgers L. Rev.*

[77] Bart W. Schermer, Bart Custers, and Simone van der Hof, 'The crisis of consent: How stronger legal protection may lead to weaker consent in data protection' (2014) 16(2) *Ethics and Information Technology* https://link.springer.com/content/pdf/10.1007/s10676-014-9343-8.pdf accessed 1 July 2021.

[78] Ibid. Note that privacy of the child vis a vis their parents may well be the reason that parental consent is not necessary in the case of preventive or counseling services are offered directly to a child (Recital 38 GDPR).

parents looking over their shoulder. Incidentally, there are also children who find it pleasant when their parents are involved, so that they can get advice. It is questionable, however, whether parents understand enough of – increasingly complex – data processing to be a good adviser for their children in that respect. In light of the failures of consent mentioned above, the question is whether consent is an adequate data protection mechanism at all. So, if you want to offer children special protection, parental consent may not be the most appropriate way to do so. Other instruments that aim to protect data subjects, including children, such as privacy by design and data protection impact assessment, are likely to be a more sensible way of meeting the objectives of the GDPR.[79]

The final failure of consent is that addressing consent from an individualistic lens clashes against the backdrop of personal data use in an increasingly algorithmic society that has ulterior economic, political, and societal implications on certain social segments or even society as a whole. In certain instances, such as those that address the common good or public interest, consent may arguably not be fit for purpose. This is expressed in the GDPR by providing other legitimate bases for data processing other than consent, such as legal obligations, the public interest, or the legitimate interests of others. The number of decisions to which consent applies is therefore limited and may even decrease in favor of these other grounds.[80] It has been argued that group privacy may also be a useful concept in addressing the shortcomings of consent caused by its individualistic nature.[81] Group privacy could serve as a value or even a right protecting groups rather than individuals, and group consent could be an instrument replacing individual consent.[82]

5. STRENGTHENING CONSENT

Given the shortcomings of consent, perhaps we have arrived at the time where we should revisit its typical construction and formulation. A number of methods or models have been proposed that may strengthen consent in order to make it more robust. Some of the following proposals address shortcomings in how consent mechanisms are currently realized in order to improve them – several of which may be used in tandem – while others more extensively change the existing framework for consent by focusing on other aspects of data protection.

Consent to use someone's personal data is rarely renewed after it is initially given; hence, after one registers with or visits a website, consent is implied to be given in perpetuity.[83] As

---

[79] Simone Van der Hof, S. and Eva Lievens, 'The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR' (2018) 23:1 *Communications Law*; Simone van der Hof, Simone, Eva Lievens, Ingrida Milkaite, Valerie Verdoodt, Thijs Hannema, and Ton Liefaard 'The child's right to protection against economic exploitation in the digital world' (2020) 28:4 *The International Journal of Children's Rights*.

[80] Jef Ausloos, 'Balancing in the GDPR: legitimate interest v. right to object' (2017) KU Leuven https://lirias.kuleuven.be/1711832?limo=0 accessed 1 July 2021.

[81] Linnet Taylor, Luciano Floridi, and Bart Van der Sloot, *Group Privacy: New Challenges of Data Technologies* (Springer 2016).

[82] Note that unanimous group consent would boil down to aggregated individual consent decisions, but obviously group consent can also be designed via majorities or qualified majorities.

[83] Bart Custers, 'Click here to consent forever: Expiry dates for informed consent' (2016) 3(1) *Big Data & Society* https://journals.sagepub.com/doi/pdf/10.1177/2053951715624935 accessed 1 July 2021. While users can address this to some extent with websites they merely visit by regularly clear

consent can become outdated – it may no longer reflect the preferences of the user – one mechanism proposed to address this involves mandating expiry dates for consent and requiring data controllers to renew the user's consent after its expiration.[84]

There have also been suggestions to use privacy icons in order to facilitate informing data subjects about how their personal data may be processed.[85] If standardized,[86] these graphics would enable data subjects to more quickly and easily see the purposes for which their data may be used and the risks associated with consenting to them.[87] Of course, by simplifying certain concepts into icons, precision and nuance may be lost, but more detailed information should always be provided together with the icons.[88] Such a multilayered approach is in fact mentioned in the GDPR; however, as it merely states that standardized icons may be used, there has been little movement towards widespread adoption.

To address consent fatigue, the original proposal for an ePrivacy Regulation included in its Recitals a push for software developers to create the ability to set various browser-level options for consenting to different levels of cookies.[89] The idea is that technical means of providing consent 'through transparent and user-friendly settings' may obviate the need to provide consent on every website that a user visits, and the choices made by that user in the 'general privacy settings of a browser or other application should be binding on, and enforcea-

---

their browser's cookies (which store their consent preferences) as this will prompt the website to request consent once again, the same may not be said for websites and apps that require registration as consent is typically given through the acceptance of the terms of service/terms & conditions.

[84] Bart Custers, 'Click here to consent forever: Expiry dates for informed consent' (2016) 3(1) *Big Data & Society* https://journals.sagepub.com/doi/pdf/10.1177/2053951715624935 accessed 1 July 2021.

[85] Lorrie Faith Cranor, 'Necessary but not sufficient: Standardized mechanisms for privacy notice and choice' (2012) 10 *J. on Telecomm. & High Tech*.; The Mozilla Privacy Icons Project' https://wiki.mozilla.org/Privacy_Icons accessed 1 July 2021; Zohar Efroni, Jakob Metzger, Lena Mischau, and Marie Schirmbeck 'Privacy icons: a risk-based approach to visualisation of data processing' (2019) 5 *Eur. Data Prot. L. Rev*.

[86] The Article 29 Working Party has stressed the importance of standardization of such icons. Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (WP260 rev.01, 10 April 2018), para. 52.

[87] Zohar Efroni, Jakob Metzger, Lena Mischau, and Marie Schirmbeck 'Privacy icons: a risk-based approach to visualisation of data processing' (2019) 5 *Eur. Data Prot. L. Rev*.

[88] Art 12(7) GDPR and Recital 60 GDPR.

[89] For example, Recital 23 states:

> End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies'). Such privacy settings should be presented in a [sic] an easily visible and intelligible manner.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010 accessed 1 July 2021. It should be noted that this idea is not particularly new: the Platform for Privacy Preferences (P3P) grew out of interest in online privacy in the mid-1990s and after a five-year process the 1.0 specification was released in 2002, which 'involved a protocol in which web browsers would negotiate with websites over privacy on behalf of their users'. Lorrie Faith Cranor, ' Necessary but not sufficient: Standardized mechanisms for privacy notice and choice' (2012) 10 *J. on Telecomm. & High Tech*.; The Mozilla Privacy Icons Project' https://wiki.mozilla.org/Privacy_Icons accessed 1 July 2021.

ble against, any third parties'.[90] However, in the latest draft of the proposal, many of the specifics were removed from the Recitals, including the portion addressing enforceability by users.[91]

Dynamic consent models – which entails two-way communication between those processing data and the data subjects themselves – have also been proposed to bolster consent.[92] This 'participant-centred' approach 'allows interactions over time; it enables participants to consent to new projects or to alter their consent choices in real time as their circumstances change and to have confidence that these changed choices will take effect'.[93] While dynamic consent models have been primarily advanced in biomedical and genetics research,[94] they may be adapted for a wide array of uses. Data subjects would be able to relatively easily alter their consent preferences, and data controllers and processors would be able obtain consent to process data for different purposes, which may help avoid 'purpose creep'.[95] However, consistently requesting data subjects to update their consent will likely only contribute to consent fatigue. One option to address this would be to employ a technological framework enabling data subjects to opt-in or -out of certain types of processing in advance,[96] somewhat similar to the browser-level settings proposed in the draft ePrivacy Regulation discussed above.

Recently, researchers have also tried to conceptualize the right to repair for informational privacy, so as to essentially provide for a 'right to reasonable customization'.[97] The intention behind such a right is to address the 'take-it-or-leave-it' approach propagated by consent. Building upon the right to repair and privacy by design approaches, the authors propose a new right that to empower consumers to have more negotiation power vis-à-vis data controllers and provide examples of technical solutions to enable customizable online services.[98]

---

[90] Recital 22 GDPR.

[91] Draft for an ePrivacy Regulation, March 2020, Recital 20a ePrivacy Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6543_2020_INIT&from=EN accessed 1 July 2021. Recitals 22–24 ePrivacy Regulation that concerned browser-level consent were essentially removed and replaced with Recital 20a ePrivacy Regulation.

[92] Aurelia Tamò-Larrieux, *Designing for Privacy and its Legal Framework* (Springer 2018).

[93] Jane Kaye, Edgar A. Whitley, David Lund, Michael Morrison, Harriet Teare, and Karen Melham 'Dynamic consent: a patient interface for twenty-first century research networks' (2015) 23:2 *European Journal of Human Genetics*.

[94] Yaniv Erlich, James B. Williams, David Glazer, Kenneth Yocum, Nita Farahany, Maynard Olson, Arvind Narayanan, Lincoln D. Stein, Jan A. Witkowski, and Robert C. Kain (2014) 12:11 *PLoS biology* e1001983.

[95] This is also sometimes referred to as 'function creep'. Tijmen Wisman, 'Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things' (2013) 4(2) *European Journal of Law and Technology*. While the purpose specification principle in the GDPR addresses this from the outset of processing, dynamic consent models could serve as an additional measure to ensure compliance.

[96] Yaniv Erlich, James B. Williams, David Glazer, Kenneth Yocum, Nita Farahany, Maynard Olson, Arvind Narayanan, Lincoln D. Stein, Jan A. Witkowski, and Robert C. Kain (2014) 12:11 *PLoS biology* e1001983. In this example, so as 'to reduce the burden on participants, the system could provide personalized opt-out/opt-in preferences that would automatically accept a study request based on the subject of the study and reputation of the researcher.'

[97] Aurelia Tamò-Larrieux, Zaira Zihlmann, Kimberly Garcia, and Simon Mayer, 'The right to customization: conceptualizing the right to repair for informational privacy' (2021) *Annual Privacy Forum*, pp. 3–22, Springer.

[98] Aurelia Tamò-Larrieux, Zaira Zihlmann, Kimberly Garcia, and Simon Mayer, 'The right to customization: conceptualizing the right to repair for informational privacy' (2021) *Annual Privacy Forum*, pp. 3-22, Springer.

Personal data processing utilizing artificial intelligence (AI) poses particular issues for consent models – data controllers may not know exactly how the data will be processed and thus cannot properly inform data subjects at the outset.[99] However, AI systems have also been proposed as a way to automate consent, at least certain aspects of it.[100] They may be able to learn data subjects' consent preferences for different types of processing and to configure settings accordingly in a semi-automatic manner; such systems could provide a method to notify data subjects where norms are deviated from in order to obtain their consent when one's preferences are unclear. However, these AI systems are unable to address the difficulties introduced by AI processing of data, and the 'morally transformative' aspect of consent may in fact be lost through automation.[101]

There have also been proposals to reform the current data protection framework – in ways that directly affect consent – in order to address the algorithmic processing of personal data which is rapidly growing. One such proposal is to move away from consent as a stand-alone legitimate basis for processing personal data – consent would then merely be a factor in a reconceptualized legitimate interest test (the new sole ground for processing personal data), alongside the data minimization principle and the performance of a contract ground, for instance.[102] Another suggestion is to move away from the 'autonomy-based' data protection model that focuses on consent, and instead look more towards the infrastructure level, targeting privacy design decisions with accountability mechanisms that include contextual obligations.[103]

6. CONCLUSIONS

Consent has been enshrined in data protection law since its very beginning. In particular, within the private sector, the legal ground of consent today under the GDPR, and already under the preceding Directive 95/46/EC, plays a central role. With the GDPR, the formalities of how consent must be obtained have been further harmonized throughout the EU. The main goals of consent have remained unchanged over time: empowerment of the users, (informational) self-determination, autonomy. Interestingly, even if the goals of consent seem very user-focused, consent shall only be relied upon if it is an appropriate legal ground. However, if the processing is necessary based on a statutory obligation listed in Article 6 of the GDPR,

---

[99] Alexandra Giannopoulou 'Algorithmic systems: The consent is in the detail?' (2020) 9:1 *Internet Policy Review*.

[100] Meg Leta Jones, Ellen Kaufman, and Elizabeth Edenberg 'AI and the ethics of automating consent' (2018) 16:3 *IEEE Security & Privacy*.

[101] For a nuanced look into the use of 'algorithmic assistants' and how they relate to autonomous choice, see: Gal, M.S., 2018. Algorithmic challenges to autonomous choice. *Mich. Tech. L. Rev.*, *25*, p. 59.

[102] Lokke Moerel and Corien Prins, 'Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things'' (2016) SSRN https://ssrn.com/abstract=2784123 accessed 1 July 2021. In the authors' view, the legitimate interest principle should be 'the main and only test for all the various phases of the life cycle of personal data, including collection, use, further use and destruction' as it will offer more effective and legitimate data protection that better keeps up with 'social trends and technological developments'.

[103] Alexandra Giannopoulou 'Algorithmic systems: The consent is in the detail?' (2020) 9:1 *Internet Policy Review*.

then consent takes a back seat. Nonetheless, in the digital economy consent will often be called upon to legitimize the data processing, in particular in the domain of profiling for marketing activities. For data controllers, this has also the benefit of legal certainty: with a consent statement, they can easily prove their data processing is legitimate.

While it has been claimed that consent combined with the information requirements of the GDPR can be helpful in managing (privacy) expectations of a data subject, it has become clear that consent mechanisms have many failures. These failures occur among others because of phenomena we know from behavioral economics literature, such as bounded rationality, incomplete information, time limitations, and cognitive biases. Data controllers are aware of those limitations and can, by means of dark patterns or less malicious design properties, trick data subjects into consenting to specific data processing. In addition, overreliance on consent has led to consent fatigue of users, which has numbed data subjects to the risks of personal data processing activities.

It is questionable why the legislator, via consent as an often-used legal basis, puts the burden of assessing risks of personal data processing operations in the digital economy on the data subject in the first place. Assessment of all the risks involved would require each data subject to fully understand how data is being processed, assess the size of risks of such operations, and weigh these against the benefits associated with often free services. Such an assessment is incredibly time intensive, especially when considering the many services and products we use on a daily basis. Moreover, relying on consent requires information and power symmetry. Yet, data subjects want access to convenient services which their peers are using and the marketplace of applications is often controlled by some major companies, restricting the ability to choose considerably. Peer pressure might be an even more dominant factor when children or young adults are being targeted by specific service providers.

Perfect solutions to overcome these failures of consent do not exist. Yet, means to reconceptualize consent have been proposed. Examples thereof are the use of standardized icons that illustrate more intuitively the ways data is being processed or the reconceptualization of the right to repair as a right to demand customizations. Also, the use of browser-level options that ensure by default the preferred data processing practices of a user, or dynamic consent models that allow, in particular, participants in studies to renew consent over time to the use of their data. Even the use of AI to learn about user individual preferences and automatically choose various consent options for him or her has been proposed. To address the systemic failures of consent, more fundamental rethinking will be necessary. Such rethinking might include reforming the data protection framework in a way that consent is no longer a stand-alone legitimate basis for processing, but merely a factor in determining legitimate interests. Or, the self-determination approach of data protection law could be altogether abandoned. Instead, regulation would target the design and infrastructure of products and services by providing clear obligations on how data may be processed. Such attempts, however, likewise trigger serious challenges (e.g., lack of innovation, paternalism) that would need to be addressed.