5. Personal data protection in a world of artificial intelligence and Internet of Things: consent, transparency and accountability

Althaf Marsoof and Indranath Gupta

1. INTRODUCTION

The right to the protection of personal data, whether as a standalone right or as an extension of the right to privacy, has gained much significance with advancements in technology. Consent with regard to the collection and processing of one's personal data is a crucial aspect of data protection. Consent represents an agreement on the part of the data subject authorising the collection and processing of the subject's personal data. A necessary corollary to consent is transparency in how the data subject's personal data will be used and processed. Without transparency, consent cannot be obtained in any real sense. Importantly, laws that protect privacy and personal data must ensure that entities responsible for collecting and processing personal data are held accountable to meet the requisite consent and transparency standards. However, artificial intelligence (AI) and the Internet of Things (IoT) have rapidly shifted us away from a model of one-to-one transactions to a one-to-many model in a completely automated environment. This transformation has made it exceptionally challenging to maintain a clear understanding of consent and transparency within this new environment. In this chapter, we explore this challenge with the hope of suggesting how the design and use of products, services, and applications that communicate with one another, incorporating automated technologies that function with little or no human intervention, could better address our expectations of consent and transparency with regard to the collection and processing of personal data.

2. CONSENT, TRANSPARENCY AND ACCOUNTABILITY

Consent is a fundamental concept in law, which has been characterised as a form of "moral magic".[1] Consent can be applied with respect to the human body,[2] private property,[3] to denote a lawful exchange,[4] and even the legitimacy of political power.[5] In the context of privacy, consent symbolises when and to what extent an individual willingly permits intrusions into their private affairs and particulars. The phrase "a man's home is his castle"[6] reflects one of the earliest conceptualisations of privacy, which upholds the sanctity of private life and property, according to which no one, not even the State, could enter a home without the subject's consent, except in narrowly defined circumstances permitted by law.

---

[1] James Konow, 'Coercion and Consent' (2014) 170 *Journal of Institutional and Theoretical Economics* 49.

[2] Milena Popova, *Sexual Consent* (MIT Press 2019), 13–14 (discussing the importance of consent in relation to sexual relations/offences); Jessica W. Berg, Paul S. Appelbaum, Charles W. Lidz, and Lisa S. Parker, *Informed Consent: Legal Theory and Clinical Practice* (Oxford University Press 2001) (discussing the importance of consent in the field of medicine, including research involving human subjects).

[3] Robert A. Simons, *When Bad Things Happen to Good Property* (Environmental Law Institute 2006), 215 (in the context of immovable property, consent distinguishes between lawful enjoyment and trespass); David Vaver, 'Consent or No Consent: The Burden of Proof in Intellectual Property Infringement Suits' [2011] *Intellectual Property Journal* 147 (in the intellectual property context, consent distinguishes between lawful and infringing use).

[4] Oren Bar-Gill and Lucian Arye Bebchuk, 'Consent and Exchange' (2010) 39 *Journal of Legal Studies* 375.

[5] Daniel M. Layman, 'Two Concepts of Consent in Locke's Political Theory' (2016) 18 *Ethics and Politics* 111.

[6] *Peter Semayne v Richard Gresham* (1604) 5 Coke Rep 91.

Although the right to privacy[7] has evolved over time, with limited exceptions being carved out to reflect new realities and public interests,[8] consent as a concept remains fundamental to the exercise of that right. Indeed, the importance of consent became instantly apparent with the invention of computers, which facilitate the automated processing of data, including personal data, and the advent of the internet, which enables the cross-border flow of such data. Technological developments have prompted us to focus on the specific field of data protection as a means of protecting the right to privacy, especially informational privacy.[9]

In 1980, the Council of the Organisation for Economic Co-operation and Development (OECD) made a recommendation with the intent of harmonising privacy and data protection laws across countries, among other things, to address issues arising from the automatic processing and transborder flows of personal data.[10] As an Annex to this recommendation, the Council published a series of guidelines[11] that countries could follow in their harmonisation efforts. According to these OECD Guidelines, personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject,[12] used for the object for which it was collected,[13] the object

---

[7] The right to privacy is enshrined in key international and regional instruments: see e.g. Universal Declaration of Human Rights (10 December 1948, UNGA Res 217 A(III)), art. 12; European Convention for the Protection of Human Rights and Fundamental Freedoms (3 September 1953, ETS 5), art. 8 (right to respect for private and family life); European Union Charter of Fundamental Rights (18 December 2000, [2000] OJ C364/1), art. 7 (respect for private and family life) and art. 8 (protection of personal data).

[8] Exceptions to the right to privacy are permitted when they are in accordance with the law and are necessary to achieve a stated public interest, such as, for instance, national security, public safety, or the prevention of disorder or crime.

[9] Max-Otto Baumann and Wolf J. Schünemann, 'Introduction: Privacy, Data Protection and Cybersecurity in Europe' in Wolf J. Schünemann and Max-Otto Baumann (Eds) *Privacy, Data Protection and Cybersecurity in Europe* (Springer 2017), 2.

[10] OECD, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980, C(80)58/FINAL).

[11] OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, as set out in an Annex to the OECD Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980, C(80)58/FINAL) (OECD Guidelines).

[12] OECD Guidelines, para 7.

[13] OECD Guidelines, para 8.

being specified to the subject no later than at the point of data collection,[14] and should not be disclosed to third parties except with the consent of the data subject or by authority of law.[15] Importantly, the OECD Guidelines require data processing entities to subscribe to standards of openness and transparency in respect of practices and policies applicable to the processing of personal data[16] and for them to be held accountable under the law in respect of their compliance with the standards required of them.[17] The 1980 OECD Guidelines were revised in 2013, and the Council recommended new guidelines.[18] The Revised OECD Guidelines reiterated the privacy principles but strengthened the aspect of accountability by adding a new part that deals exclusively with the demonstration of accountability. Accordingly, for entities that process personal data to meet the requisite accountability standard, they must give effect to the principles set out in the OECD Guidelines for all personal data under their control and, in addition, must provide appropriate safeguards against privacy breaches, set up oversight mechanisms, be able to demonstrate their privacy management programmes at the request of competent authorities, and notify such authorities in the event of privacy breaches.[19]

The principles set out in the OECD Guidelines have seeped into national[20] privacy and data protection laws worldwide, as well as regional legislative frameworks, such as the EU Privacy and Electronic Communications Directive[21] and the General Data Protection Regulation (GDPR).[22] These laws provide the basis and legal framework for the protection of personal data.

---

[14] OECD Guidelines, para 9.

[15] OECD Guidelines, para 10.

[16] OECD Guidelines, para 12.

[17] OECD Guidelines, para 14.

[18] OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, as set out in an Annex to the OECD Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (11 July 2013, C(2013)79) (Revised OECD Guidelines).

[19] Revised OECD Guidelines, para 15.

[20] See e.g. Personal Data Protection Act 2012 of Singapore (PDPA); Privacy Act 1988 of Australia (Privacy Act); Digital Personal Data Protection Act 2023 of India (DPDP Act).

[21] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), [2002] OJ L 201/37 (Privacy and Electronic Communications Directive).

[22] 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

Importantly, consent, transparency, and accountability are standard features of these laws. For instance, the EU Privacy and Electronic Communications Directive seeks to guarantee the confidentiality of electronic communications by prohibiting the interception or surveillance of electronic communications (unless authorised by law) without the consent of the users.[23] In addition, the use of traffic or location data for marketing or value-added services is also subject to the express consent of such users.[24] Notably, the Directive defines consent 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] That is, a data subject's or user's consent with respect to the use of their personal data must be signified by an informed indication to that effect. Arguably, an informed indication of consent is only possible when the data subject is provided with adequate information about how their personal data will be used. In other words, the provisions mentioned above of the Privacy and Electronic Communications Directive suggest that consent cannot be exercised freely and meaningfully unless there is transparency about how the data subject's personal data will be subsequently used or processed.

Similarly, the EU GDPR incorporates several fundamental principles that share similarities with the OECD Guidelines. Among these core tenets is the principle of "lawfulness, fairness, and transparency" in processing personal data. Accordingly, all personal data must be "processed lawfully, fairly and in a transparent manner in relation to the data subject".[26] Article 6(1) of the GDPR sets out specific conditions under which the collection of personal data by a data controller may be regarded as lawful. The lawfulness requirement under art. 6(1)(a) of the GDPR requires that before personal data can be processed, the data subject must have "given consent to the processing of his or her personal data for one or more specific purposes" unless one of the other conditions set out in art. 6(1)(b)–(f) are satisfied.[27] Indeed, the collection of data

---

of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L119/1 (GDPR).

[23] Privacy and Electronic Communications Directive, art. 5(1).

[24] Privacy and Electronic Communications Directive, arts 6(3) and 9(1).

[25] Privacy and Electronic Communications Directive, art. 2(f), which defines consent referentially (with a reference to the definition in Directive 95/46/EC, which is now repealed).

[26] GDPR, art. 5(1)(a).

[27] The other conditions upon which personal data may be lawfully collected include situations where the processing of personal data is necessary to perform a contract to which the data subject is a party, to comply with legal obligations that apply to a data controller, where processing of personal data is required to protect the vital interests of the data subject or another natural person, processing

upon obtaining consent from the data subject is arguably the most obvious and common means of collecting personal data for processing. The GDPR defines consent as "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".[28] Importantly, in dealing with the conditions for consent, the GDPR provides that "[i]f the data subject's consent is to be given following a request by electronic means, the request must be *clear, concise and not unnecessarily disruptive* to the use of the service for which it is provided".[29] The GDPR adds, in dealing with the principle of transparency that "any information addressed to the public or to the data subject *[must] be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation [must] be used*".[30] In addition, as part of the GDPR's accountability requirement, it mandates that entities that process personal data must be "responsible for, and be able to demonstrate compliance with" the principles set out therein, which includes the consent and transparency requirements. In essence, the GDPR's framework establishes a strong connection between consent and transparency, reinforced by a corresponding requirement for accountability.[31]

Likewise, in Singapore, a data subject is deemed not to have given consent for the collection, use or disclosure of personal data unless the data subject has been informed of "the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data".[32] Thus, Singapore's data protection legislation adopts transparency standards that directly relate to the exercise of consent. In addition, entities that process personal data are held accountable by being required to comply with the

---

necessary to carry out a task in the public interest or in the discharge of official authority vested in the data controller, or where processing of personal data is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (see GDPR, art. 6(1)(b)–(f)).

[28] GDPR, art. 4(11).

[29] GDPR, rec. 32, read with art. 7.

[30] GDPR, rec. 58, read with art. 12.

[31] Notably, the European Commission's proposed Regulation on Electronic Communications adopts the GDPR's notice and consent framework. See European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final (Brussels: 10 January 2017).

[32] PDPA, s 20.

principles and standards, including consent and transparency requirements, as set out in Singapore's data protection law.[33] Australia's privacy legislation also adopts a similar approach.[34] Under India's new data protection law (i.e. the Digital Personal Data Protection Act 2023), personal data may be processed only "for a lawful purpose"[35] (i.e. any purpose which is not expressly forbidden by law),[36] provided that the data subject had consented to such processing[37] or it is for certain legitimate uses.[38] The law provides that the consent given by the data subject must be "free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose".[39] Importantly, any request for the processing of personal data must be accompanied by or preceded by a notice providing the data subject the details about, among other things, "the personal data and the purpose for which the same is proposed to be processed".[40] In addition, just as in the case of the EU, Singapore, and Australia, the Indian law ensures accountability in how entities that process personal data comply with the consent and transparency requirements.[41]

The provisions of the regional and national privacy/data protection laws considered above reveal that consent, transparency, and accountability are interconnected concepts. Consent can be freely and meaningfully exercised only when there is transparency. It has been highlighted that "[t]ransparency allows a data subject to determine the extent and consequences of data processing in advance. It gives data subjects greater control over their personal data and helps make consent meaningful and informed".[42] In order to facilitate free and meaningful consent, both national and regional privacy laws have adopted a notice and consent approach, whereby data subjects are provided

---

[33] PDPA, s 11.

[34] Privacy Act, Schedule 1, Part 2. Accountability under the Privacy Act is achieved by making the provisions of the privacy legislation enforceable under Part 6 of the Regulatory Powers (Standard Provisions) Act 2014 (see Privacy Act, s. 80V).

[35] DPDP Act, s. 4(1).

[36] DPDP Act, s. 4(2).

[37] DPDP Act, s. 4(1)(a).

[38] DPDP Act, s. 4(1)(b).

[39] DPDP Act, s. 6(1).

[40] DPDP Act, s. 5(1)(i).

[41] DPDP Act, s. 8.

[42] Indranath Gupta and Paarth Naithani, 'Transparent communication under Article 12 of the GDPR: Advocating a standardised approach for universal understandability' (2022) 5 *Journal of Data Protection & Privacy* 150, 152.

with information in a transparent manner to enable such free and meaningful consent to be exercised in respect to the collection, use, and disclosure of their personal data. Accordingly, there is an inherent link between consent and transparency, and in dealing with consent, it is necessary to consider this aspect of transparency. As such, entities entrusted with collecting and processing personal data must meet specific standards, particularly with regard to the notice requirement. Since proper notice is critical in ensuring free and meaningful consent, when entities that collect and process personal data fail to comply with transparency standards, particularly with notice requirements, they must be held accountable for their failures. Otherwise, there will be challenges with regard to the exercise of free and meaningful consent.

In the next part, we explore the normative requirements for consent to be regarded as freely and meaningfully given. Understanding the true meaning of consent from such a normative point of view is essential to determine whether consent as a principle is still relevant and practicable in the context of how technology is evolving in the age of AI and IoT.

3. THE NORMATIVE REQUIREMENTS FOR CONSENT

In this part, we examine the normative requirements for consent to be considered free and meaningful. As noted above, consent is a concept that permeates all areas of law. However, what do we mean by consent? What are our expectations in relation to granting or receiving consent? And importantly, how do we demonstrate consent? To respond to these questions, it is best to begin with some abstraction. The *Oxford English Dictionary* defines "consent" as "[v]oluntary agreement to or acquiescence in what another proposes or desires; compliance, concurrence, permission".[43] It has been suggested that "[w]here called for, consent can sometimes function like a proprietary gate that one opens to allow another's access, access that would be impermissible absent the act of voluntarily opening the gate".[44] Consent consists of three essential components: a consenting party, a recipient of the consent, and the specific act or course of conduct to which the consent applies. Acts of consent establish

[43] "Consent, n.", *Oxford English Dictionary Online* (Oxford University Press 2000).

[44] John Kleinig, 'The Nature of Consent' in Franklin Miller and Alan Wertheimer (eds) *The Ethics of Consent: Theory and Practice* (Oxford University Press 2010), 4.

entitlements, create obligations, and shift risks and responsibilities from one person to another.[45]

As noted by some of the greatest philosophers, "voluntariness" is a crucial component of consent. Unless there is voluntary consent, there is truly no consent at all. For instance, in the context of contracts, Hobbes posited that a contract represents a mutual agreement, and the voluntary act of the will of the parties is the glue that holds a contract together.[46] In discussing consent within the fabric of political theory, Locke asserted that "consent must be fully voluntary".[47] Consent must come out of an individual's free will and should not depend on anyone else's will.[48] Therefore, consent is a rational and voluntary choice that is freely given.[49]

But for consent to be an exercise of one's free will, it must be consent that is informed. One cannot give consent without acquiring an appreciation of the terms with respect to which such consent is given.[50] This is why, in many contexts, there is an insistence on "informed consent", particularly in connection with research involving human subjects,[51] activities involving medical procedures on the human body,[52] or the use of genetic resources and traditional

---

[45] David Johnston, 'A History of Consent in Western Thought' in Franklin Miller and Alan Wertheimer (eds) *The Ethics of Consent: Theory and Practice* (Oxford University Press 2010), 25.

[46] Joseph H. Katy, 'Contract Law and the Social Contract: What Legal History Can Teach Us About the Political Theory of Hobbes and Locke' (1999) 31 *Ottawa Law Review* 73, 81.

[47] Layman (n 5) 112.

[48] Layman (n 5) 117.

[49] Vera Bergelson, 'Consent to Harm' in Franklin Miller and Alan Wertheimer (eds) *The Ethics of Consent: Theory and Practice* (Oxford University Press 2010), 175.

[50] Brian H. Bix, 'Contracts' in Franklin Miller and Alan Wertheimer (eds) The Ethics of Consent: Theory and Practice (Oxford University Press 2010), 253–254.

[51] Sharona Hoffman, 'Regulating Clinical Research: Informed Consent, Privacy, and IRBs' (2003) 31 *Capital University Law Review* 71; David M. Parker, Steven G. Pine and Zachary W. Ernst, 'Privacy and Informed Consent for Research in the Age of Big Data' (2019) 123 *Penn State Law Review* 703.

[52] P.D.G. Skegg, 'Informed Consent to Medical Procedures' (1975) 15 *Medical Science & Law* 124; Gene R. Beaty and Thomas Knapp, 'Informed Consent to Medical Treatment' (1977) 19 *Air Force Law Review* 63; D.S. Ferguson, 'Informed Consent to Medical Treatment' (1984) 5 *Advocates' Quarterly* 165.

knowledge.[53] Informed consent allows an individual or a community (as the case may be) to make a "responsible choice".[54]

An important feature of consent is that it must not be obtained by fraud or misrepresentation. When there is fraud or misrepresentation, the party consenting may, as a matter of fact, signify consent expressly or tacitly in response to certain propositions put forward to that party. But the course of action that is to follow on the part of the party to whom such consent was given is not in alignment with the terms on which the consent was obtained. In essence, this misalignment vitiates consent. In the context of contractual consent, it has been observed:

> Misrepresentation involves situations where the promisee obtained the other party's consent by making a fraudulent misrepresentation about a material fact, with knowledge of its falsity and with the intent to induce the other party to enter into the contract, and where the other party justifiably relied on the misrepresentation. This defense reflects contract law's recognition that there is no free will in such a context. The misrepresentation deprived the promisor of the information necessary for consent.[55]

The point here is that when there is fraud and/or misrepresentation, consent cannot be informed and, therefore, does not represent a responsible choice of the consenting party. It runs counter to the very idea of free will.

Another important feature of consent is that it must not be obtained through coercion. Consent that is coerced is not representative of the exercise of free will. Two points are worth noting here. First, when consent is coerced, even though the external manifestation of consent (such as saying "yes" or ticking a box on a website to signify agreement) might exist, there is really no mental assent to the transaction or proposition put forward by the party who obtains such consent. When there is coercion, "one might do what would ordinarily be taken to signify consent without actually consenting".[56] Second, and from a contractual standpoint, a party coerced into consenting to enter into a contract is considered to be under duress. Although originally confined to physical threats and then extended to economic threats, the doctrine today applies to circumstances where a "wrongful act by the other party combined with a

---

[53] Anne Perrault, 'Facilitating Prior Informed Consent Context of Genetic Resources and Traditional Knowledge' (2004) 4 *Sustainable Development Law & Policy* 21.

[54] Benjamin Freedman, 'A moral theory of informed consent' (1975) 5 *Hastings Center Report* 32, 35.

[55] Chunlin Leonhard, 'The Unbearable Lightness of Consent in Contract Law' (2012) 63 *Case Western Reserve Law Review* 57, 74.

[56] Kleinig (n 44) 12.

lack of reasonable alternatives"[57] can be established. Whether or not a party had a reasonable alternative could depend on numerous factors. For instance, whether a comparable agreement with a suitable alternative party with different terms was available, whether the party consenting had a reasonable opportunity to negotiate alternative terms, whether the party proposing the terms was a monopoly in the market, or whether the offered terms were standard contract terms utilised by players in a given industry.[58] Indeed, it has been suggested that "consent is stronger with a negotiated exchange than a standardized one (e.g. a negotiated contract versus a standard-form contract)".[59]

It is also important to note that consent to a particular transaction or proposition originates in the human mind. But it is impossible to read minds. Thus, we are compelled to look for external manifestations of consent. The most obvious is when the party consenting makes it explicitly clear through affirmative action. This is usually known as express consent. In the internet's context, this could come in the form of a simple act of ticking a box indicating consent. For instance, under the EU GDPR, for consent to be established, there must be a "clear affirmative act […] such as by a written statement, including by electronic means, or an oral statement".[60] For the online context, such affirmative acts could include "ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data".[61]

Consent could also be tacit or implied. Tacit consent is inferred from the circumstances surrounding the act in question.[62] That is, a data subject does not explicitly express their consent, but the requisite consent is inferred from conduct. Interestingly, the GDPR does not recognise tacit consent. Thus, unless a data subject expressly consents to the collection and processing of personal data, a data controller cannot lawfully process such data unless one of the other conditions in art. 6(1)(b)–(f) of the GDPR becomes relevant. But other data protection laws are not this absolute. For instance, in Singapore, there are three notions of consent, namely: consent that is expressed, implied, and deemed by the operation of law. While the circumstances in which consent is deemed by the operation of law closely resemble those set out in art. 6(1)

---

57 Bix (n 50) 257.

58 Bix (n 50) 254.

59 James Konow, 'Coercion and Consent' (2014) 170 *Journal of Institutional and Theoretical Economics* 49, 55.

60 GDPR, rec. 32.

61 GDPR, rec. 32.

62 Layman (n 5) 119–120.

(b)–(f) of the GDPR[63] and express consent refers to consent given expressly by the data subject; implied consent has been interpreted by the Singapore Data Protection Commission in the following manner:

> a form of actual consent where the individual does, in fact, consent to the collection, use and disclosure of his personal data (as the case may be) although he has not expressly stated his consent in written or verbal form. It is a concept that is more expansive and malleable than deemed consent as its ambit is defined by the circumstances and conduct of the individual; but is necessarily more restricted in scope than express consent which is an expression of agreement of the range of purposes contemplated by the organisation to which the individual agrees or accepts.[64]

A similar notion of tacit or implied consent can also be found in India's new data protection law. Thus, for instance, where the data subject voluntarily provides personal data to a data fiduciary (the Indian equivalent of a data controller or processor), and there is nothing to indicate that the data subject objects to the use of the voluntarily disclosed personal data by the data fiduciary, the requisite consent may be implied.[65]

In the discussion above, we have made a modest attempt to extract the key features of consent, which, in our view, represent the normative standard and character of consent. Indeed, drafters of data protection laws, such as the GDPR, have done their best to capture the normative essence of consent. Thus, for instance, when the GDPR explicitly states that an affirmative act establishing consent must be "a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her",[66] it captures the idea that consent must be voluntary (free from coercion/duress), informed (free from misrepresentations and complete in terms of the disclosure), and represents a responsible choice of the data subject.

However, in practice, the normative standard representing free and meaningful consent (i.e. consent that is voluntary, informed, and representative of a responsible choice) remains elusive, as it is often mapped against existing technologies, their processes, and overall functions. When a standard is mapped in this way, its clock stops the moment the underlying technologies begin to evolve over time. The elasticity embedded in such a standard will decide its fate and acceptance – that is, whether it accommodates the technological

---

[63] See (n 27) and accompanying text.

[64] *In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012 and German European School Singapore* [2019] SGPDPC 8, [12].

[65] DPDP Act, s. 7.

[66] GDPR, rec. 32.

advances and continues to work at an optimal level or falls apart due to inbuilt rigidity in the standard. As such, the fundamental question we must address is whether the normative standard for free and meaningful consent is sufficiently elastic to be applied with respect to emerging or future technologies.

However, the rapid evolution of technology must not detract from the essential role of consent in protecting our rights concerning personal data and privacy. As a fundamental element of privacy and data protection, consent must evolve in tandem with technological advancements. Achieving a consent framework that is both current and future-proof requires embedding adaptability at its core. This adaptation calls for a paradigm shift toward the development of technologies that inherently honour and implement our expectations relating to consent, guided by the principles of privacy by design and default. By integrating consent mechanisms directly into the fabric of technology from the design stage, we set a foundation for a consent standard that is not only neutral to the type of technology but is also equipped to handle the unpredictable nature of technological progress. In the next part of this chapter, we explore the challenges of aligning our expectations and standards for consent with the practical realities and complexities introduced by emerging and future technologies, paving the way for a discussion on the pivotal role of privacy by design and default in achieving these goals.

4. CHALLENGES OF ANCHORING CONSENT IN THE CONTEXT OF MODERN TECHNOLOGICAL DEVELOPMENTS

Early human interactions were simple. Most of them did not require the sharing of personal information. Even when personal information was required to conclude transactions, it was shared *inter presentes*, with manual or mechanical means being used to collect and subsequently process such information. The person or entity collecting the personal information was visibly clear and certain. The purpose and object for which such information was being collected were equally clear and certain. In those circumstances, consent regarding the collection and use of personal information did not take such a prominent role as it does today. It was taken for granted and often implied by conduct.

But, as discussed earlier in this chapter, with the growth of telecommunications and the internet, transactions became more complex with the emergence of numerous intermediaries and data capable of being transmitted across jurisdictions. Personal information is no longer stored in physical formats – such as in forms enclosed in physical files maintained in filing cabinets. Instead, personal information, or more accurately, "data", is converted to or supplied in digital formats for storage in computer servers. This is why computers and the internet have elevated the significance of consent, clothing it with a far more

important role in the collection, use, and disclosure of personal information. Thus, it is not surprising that current privacy legal frameworks adopt a notice and consent approach explicitly directed at the collection and processing of personal information.

But does notice and consent give rise to a flavour of consent, as we have identified above, that may be regarded as truly free and meaningful? We argue that it does not, at least in some instances. For consent to be free and meaningful, the party consenting must be fully aware of the circumstances in which, and the objectives for which, the subject's personal data is being collected. However, this aspect of consent is difficult to achieve for several reasons. First, more often than not, notices comprise language that is incomprehensible to the average person. They contain legal jargon, complex technical descriptions, and confusing terms that are only understood by persons with legal and/or technical knowledge. While the transparency requirement seeks to address this problem by imposing the need for notices to use intelligible, clear, and plain language, it does not "guarantee that data subjects understand what data controllers convey, and it will always depend on the data subjects' expertise".[67] Second, it is often the case that notice preceding consent is given in circumstances where data subjects do not have the opportunity to appreciate the contents of the notice fully. For instance, when notices are presented to data subjects in the course of entering into a transaction or during the process of completing a particular operation, the data subject's mind is not capable of fully appreciating the contents of a notice.[68]

For consent to be given freely, it must not be obtained through coercion. Data subjects must have the option to either accept or deny a request involving the use of their personal information. For instance, art. 7 of the GDPR provides that "[w]hen assessing whether consent is freely given, utmost account shall 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*". Thus, if a service provider requires users to consent to personal information being shared with third parties for marketing or value-added purposes but makes the provision of the service itself conditional upon granting such consent, the service provider is coercing consent from its users. Such conduct by service providers will violate art. 7 of the GDPR. Indeed, at the time of writing this chapter, there was an interesting update to WhatsApp's privacy policy that gave its non-EU users an ultimatum – to either accept its new privacy policy, which would allow it

[67] Gupta and Naithani (n 42) 154.

[68] Moira Paterson and Maeve McDonagh, 'Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data' (2018) 44 *Monash University Law Review* 1, 14.

to share users' personal information with Facebook (now known as Meta), WhatsApp's parent company at the time, or to leave the messaging platform for good.[69] Clearly, the provision of WhatsApp's messaging service did not depend on or require users to share their personal information with Facebook or any third party. For that reason, we are not surprised that WhatsApp's privacy policy could not be extended to the EU, where it would have been unlawful,[70] but extended to the rest of the world.[71] Unfortunately, privacy laws outside the EU, except in jurisdictions where GDPR-styled laws have been enacted,[72] do not contain a provision equivalent to art. 7 of the GDPR, which has allowed WhatsApp to coerce consent from its non-EU users. Our point is that consent obtained without a genuine choice is forced and cannot be considered freely given. When a few entities dominate technology-related services, there are times when consent may appear lawful through adherence to notice and consent practices, yet it may lack genuine voluntariness.

Additionally, technological advancements have made it even more difficult to achieve free and meaningful consent. We are increasingly moving towards a world dominated by AI. In the past, when a data subject consented to the collection and use of personal data, there was clarity about how and by what entities the collected personal data was to be used. However, in the future, we are likely to see – indeed, we are already witnessing – instances where the collection and use of our personal information take place within an evolving context, where decisions are made on our behalf by AI-powered machines to more efficiently perform contractual obligations that arise in the course of a particular

---

[69] Karandeep Singh, 'WhatsApp in damage-control mode after its Facebook-or-die ultimatum', *Android Police* (12 January 2021), accessed 24 January 2025 at https://www.androidpolice.com/2021/01/12/whatsapps-new-terms-of-service-are-a-facebook-or-die-ultimatum/.

[70] Binding Decision 1/2021 on the dispute arising from the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR (adopted on 28 July 2021); Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (art. 65 GDPR) (adopted on 5 December 2022).

[71] Nandana James, 'WhatsApp's new privacy policy: Yet another reason why India needs data protection law', *Business Line* (10 January 2021), accessed 24 January 2025 at https://www.thehindubusinessline.com/info-tech/whatsapps-new-privacy-policy-yet-another-reason-why-india-needs-data-protection-law/article33542521.ece.

[72] For instance, Singapore's data protection law provides that "[a]n organisation shall not […] as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual" (PDPA, s. 14(2)). This is comparable to GDPR's art. 7.

process or during the supply of a particular service. We will likely encounter situations where our original consent is no longer valid and fresh consent is needed as and when automated decisions alter how our personal data is used. A process that embeds AI behaves in this fashion and "exacerbates and exponentially multiplies the existing trends to over-collect data and use data for unintended purposes not disclosed to users at the time of collection".[73] In our view, this is a significant threat to free and meaningful consent.

Indeed, some existing privacy and data protection frameworks address automated processing of personal data, but in our view, they do not go so far as to ensure free and meaningful consent in all circumstances. For instance, art. 22(1) of the GDPR provides that "[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her". Thus, when personal data is used by automated processes and such processes lead to a decision that has a legal effect or has a similarly significant effect on the data subject, the data subject has the right to object. Activities that produce a legal effect include activities that have an impact on an individual's legal rights, a person's legal status, or rights under a contract.[74] In contrast, activities that entail a similarly significant effect envisage activities that must have an equivalent effect to that of a legal effect – setting the threshold fairly high to include, for instance, the automatic refusal of an online credit application or automated decisions about credit limits based on analysis of spending habits and profiling that leads to different individuals being offered different pricing.[75]

It is important to note that there are certain limits to the right to object. The most obvious limitation[76] is that a data subject does not have the right to object to the employment of automated processes by organisations that entail

[73] Karl Manheim and Lyric Kaplan, 'Artificial Intelligence: Risks to Privacy and Democracy' (2019) 21 *Yale Journal of Law and Technology* 106, 122.

[74] Fedelma Good, Samantha Sayers and Olivia Wint, 'GDPR series: how to legitimise your profiling activities' (2018) 18 *Privacy & Data Protection* 7, 8.

[75] Good et al. (n 74) 8.

[76] Article 22(2) of the GDPR sets out three limitations to the right of a data subject not to be subject to a decision solely based on automated processing giving rise to a legal or similarly significant effect. The first limitation concerns situations where such automated decision-making is necessary for entering into or performing a contract between the data subject and a data controller. The second limitation arises in circumstances where such automated decision-making is authorised by EU law or the law of an EU Member State which applies to a data controller. The third limitation is somewhat obvious. It applies to situations where the data subject has explicitly consented to a decision being made based on automated processing.

the use of personal data in arriving at a decision regarding the data subject that does not give rise to any legal or similarly significant effect. However, with the use of AI in various contexts and by numerous entities, including social media platforms, our personal information is already being processed automatically by intelligent algorithms, although such processes do not necessarily give rise to an immediate legal consequence. An example of this is where social media platforms utilise AI to profile their users based on their day-to-day activities for the purpose of promoting or advertising products and services. Unfortunately, there is no possibility of objecting to the use of automated techniques that employ AI when the decision does not produce any legal or similarly significant effect. The natural consequence of this formulation is that our consent (or dissent) is disregarded when our personal information is used for automated decision-making, including profiling, if the outcome does not produce a legal or similarly significant effect. In our view, this does not achieve true and meaningful consent with regard to the collection and use of our personal data by automated algorithms that embed AI.

In addition, under art. 22(2) of the GDPR, even when automated decisions have a legal effect, the right to object does not extend to situations where automated processing of personal data, among other things, "is based on the data subject's explicit consent". Here, the focus is on consent with regard to being subject to automated decision-making processes. But even assuming that a data subject explicitly consents to this, the entity making use of the personal data must have first obtained consent regarding the collection and use of that personal data, under the lawfulness requirement.[77] The challenge here is that when AI is employed to process personal data, the processes and outcomes could evolve over time. Thus, neither the data subject's explicit consent to being subject to automated decision-making processes nor the consent initially given by the data subject that expressly permits the collection and use of personal data for a particular purpose accounts for the evolving nature of AI, which could give rise to outcomes that are not capable of being predicted at the time consent is obtained.[78] As such, the current consent framework, even under more mature regimes such as the GDPR, fails to address the limitations of notice and consent for AI-based methods of data processing.

We are also moving swiftly towards, if not already living in, a world where machines and devices are connected to one another and are capable of making decisions as agents of their human users. However, embracing IoT in this fashion has given rise to complexities in how humans interact with these

---

[77] See GDPR, art. 6(1).

[78] Sonia K. Katyal, 'Private Accountability in the Age of Artificial Intelligence' (2019) 66 *UCLA Law Review* 54, 94–95.

devices and machines and, in particular, how they consent to the collection and use of personal data. Concerns have already been raised about the utility of notice and consent frameworks in IoT environments. For instance, it has been observed that data subjects do not have simple means to express and communicate their consent to the entities collecting data because devices used to collect data in IoT environments have scarce resources – some do not even have a user interface[79] and others operate passively or discreetly; that is, they collect data without emitting any signal.[80] In essence, although we are seeing advancements in technology, paradoxically, we are also witnessing a deterioration in the quality and efficacy of the notice and consent requirement when applied to those technologies.[81]

Given the trajectory we are taking with regard to technology, does it make sense to hold on to a framework of notice and consent when neither notice nor consent reflects the rubric of free and meaningful consent? Instead, would it make more sense to design technology that, by default, gives effect to our expectations of privacy? These matters are considered next.

5. PRIVACY BY DESIGN AND DEFAULT

As a concept, privacy by design and default is nothing new – it was first proposed in the 1990s.[82] The concept points to the idea of implementing default data protection standards at the design phase of a product, relying on the

[79] Cigdem Sengul, 'Privacy, Consent and Authorization in IoT', *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)* (March 2017), accessed 24 January 2025 at https://ieeexplore.ieee.org/document/7899432.

[80] Mathieu Cunche, Daniel Le Métayer and Victor Morel, 'A Generic Information and Consent Framework for the IoT', *TRUSTCOM 2019 – 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications* (August 2019), accessed 24 January 2025 at https://hal.inria.fr/hal-02166181/document; Richard L. Rutledge, Annie I. Antón and Aaron K. Massey, 'Privacy Impacts of IoT Devices: A SmartTV Case Study', *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)*, accessed 24 January 2025 at https://ieeexplore.ieee.org/document/7815633.

[81] Ricardo Neisse, Gianmarco Baldini, Gary Steri and Vincent Mahieu, 'Informed Consent in Internet of Things: the Case Study of Cooperative Intelligent Transport Systems', *2016 23rd International Conference on Telecommunications (ICT)* (May 2016), accessed 24 January 2025 at https://ieeexplore.ieee.org/document/7500480.

[82] Ibraheem Mubarak Alharbi, Suzanne Zyngier and Christopher Hodkinson, 'Privacy by design and customers' perceived privacy and security concerns in the success of e-commerce' (2013) 26 *Journal of Enterprise Information Management* 702, 703.

workings of a particular technology and ensuring that those standards are maintained throughout the product's entire lifecycle. For instance, in a communication of the European Commission, the concept was set out in the following manner:

> The principle of 'Privacy by Design' means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal.[83]

In the EU's context, the GDPR now makes it a legal requirement on the part of data controllers under its "Data Protection by Design and Default" requirement. Article 25 of the GDPR provides that:

> the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures […] which are designed to implement data-protection principles […] in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Thus, art. 25 of the GDPR obligates data controllers to implement appropriate technological and organisational measures to meet the requirements of the GDPR both at the time of determining the means for processing personal data and at the time of the processing itself. This formulation of privacy by design and default "could apparently be about designing a broad range of things – both tangible and intangible – provided they have effects on privacy".[84]

When dealing with privacy by design and default, it is also necessary to refer to Recital 78 of the GDPR, which provides that:

> In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.

---

[83] European Commission, *A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final (Brussels: 4 November 2010), 12.

[84] Dag Wiese Schartum, 'Making privacy by design operative' (2016) 24 *International Journal of Law and Information Technology* 151, 153.

What is significant about Recital 78 is that it not only deals with data controllers but also refers to producers of products, services and applications, the use of which is based on the processing of personal data. However, with respect to the latter, the recital only encourages them to take into account data protection principles when developing and designing such products, services and applications. Indeed, art. 25 makes no reference to such producers of products, services and applications. In other words, the data protection by design and default requirement of the GDPR applies to data controllers and not to the designers of products, services, or applications (i.e. the underlying technologies) that such data controllers may eventually put to use for their purposes.[85] This seemingly means there is no legal requirement to consider privacy implications when designing and developing complex technologies, although data controllers who utilise such technologies must do so.

This could be problematic, particularly when AI and IoT come into play. Although data controllers might engage in the collection and processing of personal information, they may not necessarily have designed or built the technology used by the system they employ for these purposes. Instead of designing technology, it is likely to be more cost-effective for data controllers to purchase or use technology pursuant to a licence from a third party specialising in design and development. Often, data controllers may only be using or licensing an existing technology product simply as an end-user, which would make it difficult, if not impossible, to implement the standard of privacy by design and default effectively. Data controllers certainly have to make choices about what products, services and applications they wish to employ (the tangible aspect) and the kind of business or operational processes and practices (the intangible aspect) that they wish to adopt with respect to the collection and processing of personal data. However, with respect to choices relating to the tangible aspects, once a choice is made, the data controllers become responsible for any outcome that runs counter to the principles set out in privacy laws such as the GDPR. This might not be seen as a problem at first blush. After all, data processors do make a choice to pick a particular technology over others.

However, when a product, service or application embeds AI or operates in an IoT environment, it becomes much more difficult for data controllers to determine its impact on personal data. As was noted earlier in this chapter, AI systems possess the potential to evolve over time. This has implications for how the requirement for notice and consent operates. Adding to the complexities, most AI systems are not explainable. That is, algorithms, including deep

[85] Ira S. Rubinstein and Nathaniel Good, 'The trouble with Article 25 (and how to fix it): the future of data protection by design and default' (2020) 10 *International Data Privacy Law* 37, 43.

learning techniques, involve hidden layers and highly complex architectures that are impossible to analyse and explain.[86] These systems are often referred to as black boxes "because there is little insight into how they are coded, what datasets they are trained on, how they identify correlations and make decisions, and how reliable and accurate they are".[87] For notice and consent to work well, we noted before that the notice element must fully enable data subjects to determine how their personal data will be used. We noted that this is crucial from a transparency point of view. However, notwithstanding the importance of transparency as a normative objective, in the context of AI, "some commentators have noted that it may be difficult to achieve in practice, highlighting that of itself transparency may not be meaningful".[88] The unexplainability of AI systems, coupled with their ability to evolve, creates many challenges for data controllers to comply with GDPR requirements, especially when they are not the designers of such systems. For instance, data controllers are bound by the notice and consent requirement – but if and when AI systems evolve in how they process personal data in ways that cannot be explained, this is likely to be a cause for concern for data controllers when they are called upon to provide explanations to data subjects or the authorities.

As noted earlier, consent in the normative sense requires "clear affirmative action", reflecting a natural person's exercise of free will in an informed manner and having a free and genuine choice in the overall exercise. It is important to reiterate the need for consent to be timely and relevant to those involved in processing personal data. The goal is to ensure that the consent given to a data controller aligns directly with the specific, immediate purpose of the processing. However, as technology continues to advance, it will become increasingly challenging, if not impossible, to maintain these attributes of consent as a reliable legal basis for processing personal information. The standard application of a clickwrap agreement, which is accepted as a valid norm for obtaining consent under the GDPR, may not necessarily work when products or devices are driven by AI and operate in an IoT environment. For instance, how could a data controller inform data subjects about the available options when the communication nodes are multiplied due to multiple devices communicating in real time? It would be tedious to map the entire data flow between the various

---

[86] Eyal Benvenisti, 'Toward algorithmic checks and balances: a rejoinder' (2018) 29 *European Journal of International Law* 1087, 1088.

[87] Spandana Singh, *Everything in Moderation An Analysis of How Internet Platforms Are Using Artificial Intelligence to Moderate User-Generated Content* (New America/Open Technology Institute 2019), 20.

[88] Lorna McGregor, Daragh Murray and Vivian Ng, 'International human rights law as a framework for algorithmic accountability' (2019) 68 *International & Comparative Law Quarterly* 309, 322.

and numerous products and devices working synchronously with one another, let alone appropriately explain the consent structure to a natural person in comprehensible terms in a manner that could permit free and meaningful consent as conceived under the law. The problem is acute when data controllers rely on third-party technology.

For these reasons, the privacy by design and default requirement must extend not only to data controllers but also to producers of the technologies (i.e. the products, services or applications) that data controllers make use of. The idea of looking at privacy implications at the design stage has been advanced due to the imminent failure to implement privacy measures and safeguards at the post-production stage of a technology product involved in the high-risk processing of personal and sensitive personal information. Advancements in technology introduce uncertainty in the collection and processing of personal data belonging to natural persons. In particular, at the post-deployment stage of products that embed dynamic technologies such as AI and operate in an IoT environment, their functions, operations, and interactions will likely make it extremely difficult for privacy parameters and expectations to fit within the legal framework dealing with privacy and data protection. However, one has to avoid such generalisation and attempt to measure the hypothesis by applying privacy principles to a given technology so that its elasticity can be tested effectively. Further, one needs to ensure that privacy principles and the broad framework on which they work are technology-neutral so that the principles framed can withstand the test of time and advancements in technology.

To demarcate the boundaries of acceptable legal limits, the way forward would be to define the default parameters pertaining to "consent" in a transparent manner at the design phase of a product, service or application. Aside from the consent requirement, producers of such products, services and applications must acquaint themselves with the general default privacy settings, which are acceptable under the law. Certification mechanisms, which currently extend to data controllers with respect to the process of determining the means of processing, governance, and the technical and organisational measures to implement data protection principles,[89] should also be extended to the design of the products, services and applications (i.e. the technologies) that data controllers may opt to use. This way, certification mechanisms will apply not only to the choices made by data controllers regarding the use of a particular technology,

[89] GDPR, art. 25(3), read with art. 42. See also European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default: Version 2.0* (adopted on 20 October 2020), 28, accessed 24 January 2025 at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

internal governance measures, and safeguards but also to the technology itself, which will increase trust and accountability.[90]

Thus, extending the privacy by design and default obligation beyond data controllers to capture the producers of the underlying technologies will reduce the difficulties and uncertainties that data controllers are likely to face. It will also ensure that users and producers of technologies that collect and process personal data comply with data protection principles. Notably, expanding the privacy by design and default obligation to producers of technologies will facilitate better accountability on the part of all relevant actors. Such an approach, while requiring close monitoring to assess its efficacy, is likely to foster the development of privacy-trusted technologies and products capable of addressing the legal and ethical challenges associated with data collection and processing. On the whole, an approach that adopts privacy by design and default not only at the operational stage (i.e. when technologies are chosen and used by data controllers) but also at the stage of designing technologies that are employed for the collection and processing of personal data in various contexts will, in our view, increase the level of transparency and trust in products, services and applications driven by complex technologies used for the purposes of collecting and processing personal data.

6. IMPLICATIONS OF THE EUROPEAN UNION'S REGULATION ON ARTIFICIAL INTELLIGENCE

The discussion above posits that the increasing use of AI in IoT environments has significantly impacted our traditional understanding of the notice and consent requirement under data protection laws. However, the dominance of AI/IoT technologies is not only a concern in the context of privacy and data protection. It has also raised concerns among ethicists, legal scholars, and regulators more generally. Thus, it is not surprising that in recent times, groups

[90] John Miller and David Hoffman, 'Sponsoring trust in tomorrow's technology: towards a global digital infrastructure policy' (2011) 1 *International Data Privacy Law* 83.

of scholars,[91] international organisations,[92] professional institutions,[93] government agencies,[94] and private entities[95] have, from time to time, put together guidelines and frameworks articulating a number of ethical guidelines to aid the governance of AI. However, these guidelines remain non-binding soft law

[91] High Level Expert Group on AI, *Ethics guidelines for trustworthy AI* (8 April 2019), accessed 24 January 2025 at https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai; Foundation for Best Practices in Machine Learning, *Technical Best Practices from the Foundation for Best Practices in Machine Learning* (19 May 2021).

[92] Organisation for Economic Co-operation and Development, *Recommendation of the Council on Artificial Intelligence* (22 May 2019), accessed 24 January 2025 at https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449; Organisation for Economic Co-operation and Development, *G20 Ministerial Statement on Trade and Digital Economy* (June 2019), accessed 24 January 2025 at https://www.g20.utoronto.ca/2019/2019-trade-Chairs_Statement.pdf.

[93] Singapore Academy of Law, *Applying Ethical Principles for Artificial Intelligence in Regulatory Reform* (July 2020), accessed 24 January 2025 at https://www.sal.org.sg/Resources-Tools/Law-Reform/AI_Ethical_Principles; Singapore Computer Society, *AI Ethics and Governance Body of Knowledge* (November 2020), accessed 24 January 2025 at https://www.scs.org.sg/ai-ethics-bok.

[94] Infocomm Media Development Authority & Personal Data Protection Commission (Singapore), *Model Artificial Intelligence Governance Framework: Second Edition* (21 January 2020), accessed 24 January 2025 at https://www.pdpc.gov.sg/%20Help-and-Resources/2020/01/Model-AI-Governance-Framework; UK Cabinet Office, Central Digital and Data Office & Office for Artificial Intelligence, *Ethics, Transparency and Accountability Framework for Automated Decision-Making* (13 May 2021), accessed 24 January 2025 at https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making; National Institution for Transforming India, *Approach Document for India Part 1–Principles for Responsible AI* (February 2021), accessed 24 January 2025 at https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf; National Institution for Transforming India, *Approach Document for India Part 2–Operationalizing Principles For Responsible AI* (August 2021), accessed 24 January 2025 at https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf; National Institution for Transforming India, *Responsible AI–Adopting the Framework: A Use Case Approach on Facial Recognition Technology*, Discussion Paper (November 2022), accessed 24 January 2025 at https://www.niti.gov.in/sites/default/files/2022-11/Ai_for_All_2022_02112022.pdf.

[95] KPMG, *Ethical AI: Five Guiding Pillars* (2019), accessed 24 January 2025 at https://assets.kpmg.com/content/dam/kpmg/bh/pdf/2020/02/kpmg-ethical%20-ai-five-guiding-pillars.pdf.

instruments. Thus, in our view, the recently enacted EU Regulation setting out harmonised rules on AI (also known as the AI Act)[96] is a significant step towards regulating AI technologies.

The EU AI Act addresses some of the concerns we have raised above in the context of privacy and data protection. As such, a short comment on the AI Act is warranted. The AI Act applies to any "AI system", which is defined as a "machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".[97] The AI Act adopts a risk-based approach[98] to classify AI systems into several categories. These are as follows. First, AI systems that are prohibited[99] because they contradict EU values, such as respect for human dignity, freedom, equality, democracy, rule of law, and fundamental rights, including the right to non-discrimination, data protection and privacy, and the rights of the child.[100] Second, high-risk AI systems, which are subject to heightened scrutiny and regulation in view of their "harmful impact on the health, safety and fundamental rights of persons in the Union".[101] Third, AI systems that pose a limited risk and are therefore subject to certain transparency obligations.[102] Fourth, AI systems classified as minimal or no risk (i.e. AI systems that do not fall into any of the categories mentioned above). Such AI systems are not regulated by the AI Act. However, it is possible for voluntary codes of conduct to be established to guide their development and use.[103] Lastly, General Purpose AI Systems (GPAIs), such as large language models (LLMs), which are subject to certain special rules.[104]

Importantly, the AI Act not only applies to deployers of AI systems (analogous to data controllers in the GDPR's context) but also to providers of such

---

[96] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), [2024] OJ L 2024/1689 (AI Act).

[97] AI Act, art. 3(1).

[98] AI Act, rec. 26.

[99] AI Act, art. 5.

[100] AI Act, rec. 28.

[101] AI Act, rec. 46, read with art. 6.

[102] AI Act, art. 50.

[103] AI Act, art. 95.

[104] AI Act, arts 53–56.

systems (analogous to producers of the products, services and applications in the GDPR's context).[105] Thus, unlike in the GDPR, where the data protection by design and default requirement applies only to data controllers and not to producers of technologies, the AI Act imposes certain design-related obligations on providers of AI systems in addition to the deployers of such systems. However, these design-related obligations are limited to high-risk AI systems.

Thus, for instance, providers of high-risk AI systems will, among other things, become obligated to ensure that they design and develop such systems with a sufficient degree of transparency and in ways that will facilitate human oversight. The transparency obligation is aimed at ensuring that users are able to interpret the system's output and use it appropriately.[106] This will ensure that AI systems are explainable, which could provide better clarity to users of such systems, particularly in providing explanations about decisions reached consequent to their use. Thus, the introduction of a transparency obligation with respect to the design and development of high-risk AI systems could help data controllers insofar as such high-risk AI systems are used for the purposes of collecting and processing personal data.

Similarly, the human oversight obligation is aimed at ensuring that high-risk AI systems "can be effectively overseen by natural persons" when they are in use and contemplates the incorporation of "appropriate human-machine interface tools" into high-risk AI systems.[107] As we noted earlier, especially in the context of IoT environments, some devices that collect our personal data do not even possess the basic resources to ensure that they comply with the notice and consent requirement. Thus, the obligation of human oversight could encourage the development of devices better suited to meet privacy and data protection standards.

In addition, high-risk AI systems must be designed and developed to "achieve an appropriate level of accuracy, robustness, and cybersecurity, and perform consistently in those respects throughout their lifecycle".[108] This, too, is crucial for the data protection context, as technologies used for the collection and processing of personal data should accurately adhere to the purposes for which they are employed. Failure to do so could result in privacy/data breaches, which could significantly impact our right to privacy and data protection.

The obligations in the AI Act outlined above will positively influence the design and development of AI systems, including those that collect and process personal data as part of their functions. However, this will only be to the

[105] AI Act, art. 2.
[106] AI Act, art. 13(1).
[107] AI Act, art. 14(1).
[108] AI Act, art. 15(1).

extent that such AI systems are classified as high risk, as defined in the AI Act. Notably, technologies that make use of AI systems to collect and process our personal data and devices that are employed in IoT environments may not always be regarded as high risk – or even limited risk. Indeed, the European Commission has recognised that the "vast majority of AI systems fall into the category of minimal risk".[109]

This means that the design-related obligations applicable to providers of high-risk AI systems will not extend to the vast majority of AI technologies deployed in the marketplace. Thus, to a large extent, the GDPR will still continue to be relevant to AI systems that collect and process personal data. For this reason, the distinction that the GDPR draws between data controllers (i.e. those who make use of technologies, including AI systems and IoT devices, for the collection and processing of personal data) and producers of the products, services and applications (i.e. those who design and develop such technologies) for the purposes of the privacy by design and default requirement will remain a problem that needs to be addressed. We posit that there is an urgent need to extend obligations that achieve privacy by design and default to producers of technologies, including all forms of AI systems and IoT devices, that exclusively or as one of their functionalities entail the collection and processing of personal data.

7. CONCLUSION

Consent, transparency, and accountability are the fundamental principles of data protection. Consent is a rubber stamp that legitimises our interactions with others. In the context of privacy and data protection, a data subject's consent is vital for others, whether in the context of a contractual, social, or any other kind of relationship, to lawfully collect, process, and disclose personal information relating to the data subject. Therefore, it is not surprising that privacy and data protection laws around the world, including the EU GDPR, hold entities that collect and process personal data (often referred to as data controllers) accountable to ensure they maintain acceptable standards in how they collect and process personal data. In particular, these laws obligate data controllers to obtain the data subject's consent unless consent can be deemed under the law or the law permits the collection, processing, and disclosure of such data without the subject's consent. However, for consent to be valid from a normative standpoint, it must be voluntary, informed, and representative of

[109] European Commission, *Commission welcomes political agreement on Artificial Intelligence Act*, Press Release (9 December 2023), accessed 24 January 2025 at https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473.

a responsible choice. Consent is regarded as truly free and meaningful only if the act of giving consent is preceded by adequate notice enabling the data subject to determine by whom, for what purpose, and how their personal data will be collected, processed, and where necessary, disclosed. Therefore, privacy and data protection laws obligate data controllers to adhere to certain transparency obligations, without which it would not be possible for data subjects to exercise their consent in a free and meaningful manner. In essence, the requirement for consent and its interface with transparency has given rise to the notice and consent requirement.

However, the advancements we have achieved in technology have posed challenges in how data controllers comply with the notice and consent requirement at an operational level. Notices given to data subjects often embody complex legal and technical language and are presented to data subjects in real time, requiring a quick response. This does not truly enable data subjects to make informed choices regarding the collection and processing of their personal data. The adoption of IoT and the use of AI have only added to the complexity. Although IoT has enabled multiple devices to communicate with one another in real time, paradoxically, such devices lack basic interfaces that facilitate human interaction. Thus, this presents a problem from the point of view of notice and consent. Similarly, although AI has enabled automation, eliminating the need for human resources, AI-embedded technologies learn and evolve over time, at times leading to outcomes that cannot be predicted. Thus, even if consent is acquired from data subjects, such consent as given initially may not necessarily account for the evolving and unpredictable nature of AI. When data controllers are called upon to explain outcomes, especially when things go wrong (e.g. data breaches), the unexplainable nature of AI is bound to make things extremely difficult from an accountability point of view.

In view of these challenges, there is a greater need to ensure that technologies and devices that collect and process personal data are designed and developed to meet our expectations of privacy. In circumstances where notice and consent can no longer properly meet our expectations, the focus must shift to the design of technologies in view of the operational challenges. In other words, the concept of privacy by design and default has far more significance today than ever before. However, privacy and data protection laws, including the EU GDPR, focus on data controllers, imposing on them an obligation to ensure compliance with the privacy and data protection principles in respect of the choices they make regarding the use of technology, internal governance measures, and safeguards at an organisational level. In our view, this is not enough. This obligation must extend beyond data controllers to include entities that design and develop technologies that are subsequently used for the collection and processing of personal data. Although the recent AI Act addresses the concerns we have raised in this chapter by imposing design-related obligations

on developers of AI systems, its application is limited to high-risk AI systems. This means that the heightened design-related obligations set out in the AI Act do not extend to many other situations in which AI and automation are used to collect and process personal data. Thus, there is still a gap that needs to be addressed.