3 Privacy

Nikolaos Ioannidis
Vrije Universiteit Brussel. E-mail: nikolaos.ioannidis@vub.be.

3.1 Introduction

3.1.1 Definition of privacy

While the adjective 'private' is an easily comprehendible term in everyday language (meaning that something is not intended for the public), its derivative noun 'privacy' is more complex to grasp. Dictionaries define it today, for example, as the "freedom from unauthorised intrusion" or the "state of being let alone and able to keep certain especially personal matters to oneself".[1] Privacy has been analysed from different perspectives such as legal, as a right, ethical, as a virtue or value,[2] economic, as a utility or interest, or political, as a public or private good.[3]

Nowadays, privacy is frequently intertwined with and threatened by novel and emerging technologies. For the purposes of integrated impact assessment for border control technologies, to which the present textbook is devoted, this Chapter mostly focuses on privacy as a legal right. In operationalising the right to privacy, this Chapter follows the structure below. In the next sub-sections, some further introductory notions on privacy (its importance for society, historical development and relevant regulatory instruments and actors involved) are provided, including the importance of privacy within the assessment process. Section 3.1.2 describes the content of the right to privacy, offering legal and theoretical conceptualisations.

3.1.2 Historical development of the right to privacy in Western legal systems

According to a general consensus among scholars, the history of privacy in modern Western legal systems dates back to a law review article published in 1890 by two Boston

DOI: 10.46944/9789461171375.3

lawyers, Samuel Warren and Louis Brandeis.[4] Their idea of privacy came as a reflection on the appearance of new technologies (more specifically, instantaneous photography) that newspapers used to cover gossip stories, "overstepping the limits of propriety and decency, causing harm both to the individuals portrayed and to the community, lowering – it was believed – social standards and morality".[5] At that time, the right to privacy was elaborated merely within the paradigm of tort (delict) law, conceptualised as a civil claim for damages, as opposed to a fundamental or constitutional right. Originally explicated as a "right to inviolate personality", the right to privacy meant that each individual had the right to choose to share or not to share with others information about their "private life, habits, acts, and relations".[6] Alternatively, it was conceptualised as "the right of each individual to protect his or her psychological integrity by exercising control over information which both reflected and affected that individual's personality".[7]

Today, as a civil right, privacy is protected in civil law, within a jurisdiction, or, as a fundamental right, in constitutional law, at a national or regional level. As a civil right, it distinguishes the person from the outside world and is essential for one's autonomy and protection of human dignity. As a fundamental right, privacy is known as the right to respect for private and family life, the home, and correspondence (hereinafter 'the right to privacy'). It encompasses the idea of positive freedom, where a person has the freedom to determine, for example, the extent to which they control their own intellectual activity, and negative freedom, as a demand that others refrain from interference.

3.1.3 The importance of the right to privacy in society

In recent years, the right to privacy in society has gained in importance due to the increased digitalisation and ubiquitousness of computers. As a result, in the online environment, privacy is alternatively called 'informational privacy', 'data privacy' (usually in US literature) or 'online privacy'. Participating in the interconnected world means that individuals are not characterised by their own choices alone; in a community, interaction with other individuals and the way in which information is shared with them is what defines a sphere of activity.

In the past, in small-scale communities, citizens were only able to interact with their neighbours and their immediate community, and on occasions when persons with influential status would receive public critique, privacy interferences were occasional and smaller in scale. Nowadays, by contrast, large-scale monitoring of individuals presents different dangers, and impacts them multi-dimensionally. For instance, personal information obtained via contemporary means is recorded and stored, while more and more aspects of everyday life are transformed into data (e.g. payments through cards, sales via e-commerce, activity upon social media, and interactions with the government online). The development of computer technology makes it possible to store data with virtually no limits to the scope of processing or the storage duration. Furthermore, the information collected can be organised and transferred in an instant.

In sum, the online privacy of individuals is continuously threatened in many ways, for instance, when people share personal information with other users and entities, via the internet, smartphones, social networks, drones, biometric identification terminals or the Internet of Things (IoT). In such scenarios, the right to privacy protects individuals against arbitrary and unjustified use of power by reducing what can be known about them by others, such as public authorities or technology companies.

3.1.4 The importance of the right to privacy in the PERSONA benchmark

The inclusion of privacy as an element of the benchmark of an integrated impact assessment process is therefore indispensable in gaining an adequate understanding of the impacts on the right to privacy in the area of border control.

On the one hand, certain practices in the realms of border control affect the right to privacy of certain religious groups. An example is the obligation to temporarily remove clothing while performing security checks or while taking photos destined for official identity documents. This obligation is particularly sensitive and controversial when it comes to removing religious clothing, such as in the case of Sikhism. A practicing Sikh complained of an interference with his right to freedom of religion by airport authorities, who had obliged him to remove his turban as part of a security check imposed on passengers entering the departure lounge. Defending his freedom of religion and his right to privacy, he argued that there had been no need for the security staff to make him remove his turban, especially as he had not refused to go through the walk-through scanner or to be checked with a hand-held detector.[8] In this case, the same Court held that security checks in airports were necessary in the interests of public safety, however it stressed that, due to the occasional character of the incident, states may decide otherwise. In another case, a practicing Sikh claimed that the requirement for him to appear bareheaded in the identity photograph on his driving licence amounted to interference with his private life and with his freedom of religion and conscience.[9] This self-determination as to how an individual publicly appears falls within the scope of protection of the freedom of religion and the right to privacy. However, the driving licence is an official document which, upon request, could be presented to identify the individual. The European Court of Human Rights (ECtHR) stated that such photos were required by authorities in charge of public safety and law and order, particularly in the context of checks in public places. It held that the interference had been justified in principle, and was proportionate to the aim pursued. The same requirements could be extended to the issuance of an identity card or travel documents.

On the other hand, the increasing use of digital technologies in border control exacerbates existing impacts on the right to privacy. An example is facial recognition. Modern airports have progressively chosen to install automated border gates (or 'smart borders') with hundreds of 'touchpoints' that track travellers in their interactions with airlines and

border agencies. Most organisations acknowledge that the potential of facial recognition technology is significant, and its upcoming applications could provide benefits to public safety and security. However, if mismanaged, this technology may potentially lead to a perception of widespread surveillance, and could affect individuals differently, depending on their belonging to specific categories or groups, culminating in 'chilling effects' (e.g. causing distress and anxiety to individuals about the use of such technology), and ultimately eroding their right to privacy or other interconnected fundamental rights.

Additionally, facial recognition technology relies on the collection and processing of biometric information that is unique and permanent. The capacity and sophistication of this technology is continuously evolving (e.g. through self-improving algorithms) and can be used in unforeseen ways or linked with other next-generation technological tools in a manner that creates risks of harm to individuals and distortion of public confidence.[10] Frequently, actors involved in the deployment of such technologies use large-scale datasets, which are often collated. Decisions made about individuals using these identifiers, potentially without their knowledge or consent, may lead to serious risks to their rights and freedoms. Discriminatory effects are frequently given rise to; there could be a non-negligible impact in the ability to exercise certain other fundamental rights, such as the freedom of expression and association. Lastly, damage to reputations or social disadvantages are also possible consequences, sometimes without adequate avenues for recourse.

3.1.5 Relevant regulatory instruments and actors involved

3.1.5.1 Protection and promotion of fundamental rights

In liberal democratic societies, basic principles and rules pertaining to the protection of privacy – as well as other important societal concerns – enjoy a special status in legal systems, and hence are situated at the top of the hierarchy of legal norms, as human (fundamental) rights, heavily intertwined with the essential principles of such a system.[11] Human rights are the rights that "every person has by virtue of merely existing and that aim to secure for such a person certain benefits or freedoms that are of fundamental importance to any human being".[12]

The right to privacy is protected and promoted by a network of legal instruments, supplemented by an enforcement machinery consisting of predominantly international and national courts, yet no single one is solely designated to deal with issues of privacy. In general, the protection of privacy by rulemaking follows a tripartite and hierarchical pattern, namely international, regional and national. International legislation tends to be declarative and less enforceable, while regional and national legislation usually produces tangible legal effects and can be adequately enforceable.

3.1.5.2 International level

Several instruments protect the right to privacy at an international level. At the UN level, Article 12 of the Universal Declaration of Human Rights[13] (UDHR, 1948) reads: "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation […]". Further, the 1966 UN International Covenants – one on Civil and Political Rights,[14] the other on Economic, Social and Cultural Rights,[15] which together bind more than 170 countries around the world – stipulate the same provision at Article 17, with the key difference being that the Covenant is binding for contracting parties. Lastly, privacy is specifically protected in the Convention on the Rights of the Child[16] under Article 16: "No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation."

3.1.5.3 Regional level

In Europe, human rights are protected:

A. At the level of the Council of Europe (CoE), where the main instrument is the European Convention on Human Rights (ECHR, 1950) enforced by the European Court on Human Rights in Strasbourg. The Convention broadly defines the right to private and family life of every person living within the Council of Europe's territorial scope of application (Article 8 ECHR), which is further analysed in Section 1.2.1.
B. At the level of the European Union (EU), where the main instrument is the Charter of Fundamental Rights of the European Union (CFR, 2009)[17] enforced by the Court of Justice of the European Union (CJEU). The right guaranteed in Article 7 of the Charter corresponds to that guaranteed by Article 8 of the ECHR. Article 7 of the CFR is more concise, however, and reads: "Everyone has the right to respect for his or her private and family life, home and communications". It is worth noting here that, in order to take account of developments in technology, the word 'correspondence' from the ECHR has been replaced by the broader word 'communications'.[18] To conform with the Council of Europe standards, the Charter implies that the meaning and scope of this right are the same as those of the corresponding Article of the ECHR.[19] Lastly, the extent to which limitation criteria apply to all fundamental rights recognised in the Charter, are laid out in Article 52(1).[20]

Further regional legal instruments for the protection of privacy include 1969 American Convention on Human Rights[21] (enforced by the Inter-American Court on Human Rights in San Jose, Costa Rica) and the 1981 African Charter on Human and Peoples' Rights[22] (enforced by the African Court on Human and Peoples' Rights in Arusha, Tanzania).

3.1.5.4 National level

At the national level, privacy laws are usually enacted and positioned within a state's founding document, the national constitution, where fundamental principles are enshrined. Constitutions enjoy higher protection within a given jurisdiction and are observed by dedicated supreme courts. The way in which the scope of protection and interpretation of a constitutional right is articulated principally depends on the nation's history, culture and values. For instance, the notion of 'secrecy of correspondence', present in almost every constitution, is protected under the Belgian constitution in Article 29.[23]

Besides its constitutional protection in national law, privacy is further enshrined in virtually any civil code, both within the European Union and beyond. A civil code is a legal instrument, applicable in a given jurisdiction, which codifies and regulates the private law (legal relationships among individuals), indicatively, the law of contracts, law of torts, property law, family law and the law of inheritance. Provisions in the civil code usually protect privacy directly, under the protection of one's image, one's name and one's reputation, or indirectly, through the law of torts (e.g. one person's harmful behaviour against another person's honour, reputation, and privacy).

3.2 The contents of (the right to) privacy

3.2.1 Legal conceptualisations

In relation to conducting the process of integrated impact assessment, the protection of the right to privacy is relevant in situations where a private interest, or the 'private life' of an individual, could be compromised. The concept of 'private life' has been interpreted broadly in case law, as covering intimate situations, sensitive or confidential information, information that could prejudice the perception of the public against an individual, and even aspects of one's professional life and public behaviour. The scope of private life in border control is difficult to define; no general pattern can be drawn. The assessment of whether or not there is, or has been, an interference with private life depends on the context and facts of each individual case.[24]

What is protected by the right to respect for private and family life can be principally understood through the ways in which the European Courts (the ECtHR and the CJEU) have interpreted this fundamental right. There is no standard, universal scope of protection; rather, the interpretation is contextual. Both Courts' opinions on the scope of protection converge. The limitations that may legitimately be imposed on the right to privacy by the Charter are comparable to those in the ECHR. The similarities between the two instruments permit for a simultaneous comparison and research of this right.

This legal provision is divided into two paragraphs, providing for the rule and the exception (conditions for interference therewith), stating that: "1. Everyone has the right

to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[25]

Article 8 of the ECHR entails both a negative obligation on public authorities to refrain from any actions that may creep upon private life, but, at the same time, a positive obligation to actively secure the respect for privacy. Not being an absolute right, it may be limited, provided that restrictions fulfil the conditions mentioned in the second paragraph. The ECtHR examines two cumulative conditions in its decisions: a) whether there was an interference with the right to respect for private life under Paragraph 1, and b) whether the interference was legitimate according to Paragraph 2. In the assessment of the test of necessity in a democratic society, the Court often needs to balance the applicant's interests protected by Article 8 and a third party's interests protected by other provisions of the Convention. The same Article protects at least one of the four interests identified in it, namely: (i) private life, (ii) family life, (iii) home, and (iv) correspondence. For the purposes of this Chapter, only private life is directly relevant.

'Private life' is a broad concept not susceptible to any exhaustive definition, and may "embrace multiple aspects of the person's physical and social identity".[26] It involves personal information, which individuals can legitimately expect to not be published without their consent. The notion of private life is not limited to an 'inner circle' in which individuals may live their own personal lives as they choose and exclude the outside world: Article 8 of the ECHR protects the right to personal development, whether in terms of personality or of personal autonomy, and encompasses the right of each individual to approach others in order to establish and develop relationships with them and with the outside world.

The same logic extends to professional and business activities.[27] Private life encompasses the right of an individual to form and develop relationships with other human beings, including relationships of a professional or business nature. Therefore, restrictions imposed on access to a profession have been found to affect 'private life'.

As well as the general sphere of private life, the scope of private life also concerns three more specific categories, i.e. a) physical, psychological and moral integrity, b) identity and autonomy and c) privacy in a strict sense.[28] Under the first category fall, for instance, sexual orientation, disability issues, mental diseases and reproductive rights, and any personal information relating to these. Within the boundaries of the second category are, indicatively, the right to gender, ethnic and racial identity, the choice of a desired appearance, the right to a name, marital or parental status, and the right to citizenship and residence. Lastly, aspects of privacy in a strict sense are, among others: the pivotal right to one's image and photographs about oneself, the publishing of photos, images, and articles, the defence against defamation, claims relating to data protection, the right to access one's personal information, police surveillance, stop and search police powers, and information about one's health.

3.2.2 Theoretical conceptualisations

To assess the various impacts of an initiative on the right to privacy, assessors can benefit from theoretical conceptualisations, which could be done in different ways. One could articulate privacy, for example, as descriptive, normative or reductionist, control or use-based, and/or property or privacy-based, resulting in "a right to control access to and uses of places, bodies, and personal information",[29] or "the ability to determine for ourselves when, how, and to what extent information about us is communicated to others".[30] For the purpose of performing the process of integrated impact assessment, this Section adopts the typology of Koops et al., as illustrated in the template (under 'privacy screening'). Organising privacy-related theory via a typology is an explanatory step by which the application of (notions of) privacy in border control may be better understood.

The analysis of the identified types of privacy is structured in a two-dimensional model, consisting of eight basic types of privacy (bodily, intellectual, spatial, decisional, communicational, associational, proprietary and behavioural privacy), with an overlay of a ninth type (informational privacy) that overlaps, but does not coincide with, the eight basic types (Fig. 1). Furthermore, demarcating various aspects of privacy helps explain why privacy cannot merely be reduced to informational privacy, how the concept of privacy relates to the right to privacy, and how the right to privacy varies depending on the context of use.

1. *Bodily (physical) privacy*: Bodily privacy encapsulates the right to protect the physical body of the individual. It connotes a negative freedom for anyone except for the concerned individual: one can exclude the others from unsolicited touching, restraining or restricting one's body (sometimes including mental integrity). It further protects any unreasonable search and seizure, supplemented with additional restrictions for certain parts of the body, in particular the 'private parts'. A relevant illustration of this type of privacy is the compulsory provision of samples of body fluids and body tissue, as well as fingerprints. This type therefore concerns the physical body *per se*, and not clothing, bags, pockets etc., which fall within the scope of another type of privacy.
2. *Spatial privacy*: Spatial privacy is the interest of a person to mark the existence of a reasonably understood private space or territory (individually controlled), by excluding and/or restricting other people's access to it or managing its use. It is comprised of an intimate zone (around the person) and an extended zone, in which the person is residing or inhabiting and is supposed to be acting privately (e.g. the area of the house). In both the intimate and extended zone, the individual sets the conditions for exposure. This type of privacy is triggered by, for example, the performance of unlawful 'searches' that enable law enforcement to observe activities as they are taking place inside the home. A person should be able to (stressing the ability/control to do so) control (increase/decrease) the degree of openness to others by 'tweaking' the modalities of their intimate zone, this referring to a limited information flow within trusted relationships. An interference with spatial privacy in border control is rare, since it is

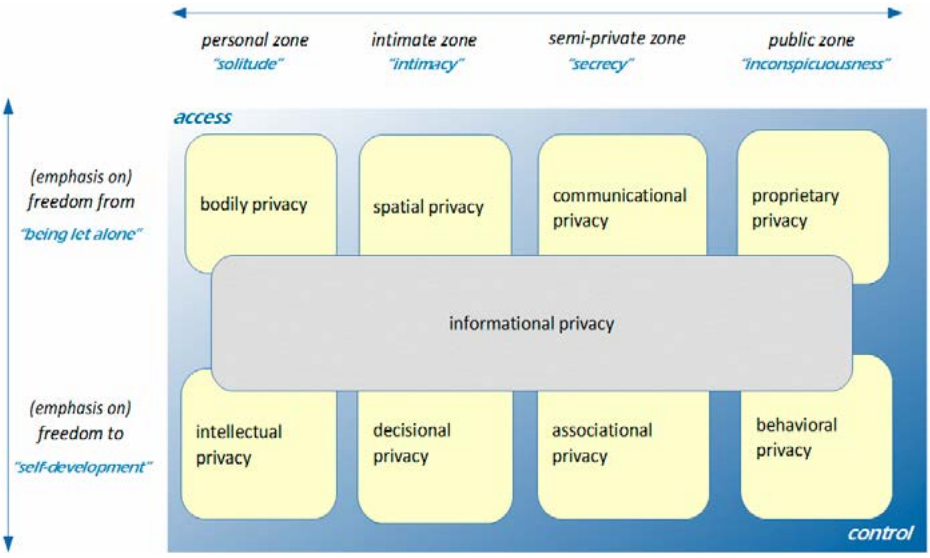
connected to the private property (home). Nonetheless, interrogation about how one acts at home and preferences in terms of social engagement, intimate partners, family members or close friends could fall within the scope of this type of privacy.

3. *Communicational privacy*: Communicational privacy is the ability of a person to restrict access to communications or to control the use of information communicated to third parties. The meaning of (tele)communications is continuously evolving, and is arguably one of the cornerstones of constitutional privacy protection, linked also to the freedom of expression. Historically, it would be solely associated with written (i.e. postage) letters and telegraphy, but nowadays it is interpreted broadly, in order to accommodate newer forms of communicating at a distance, such as telephone calls, emails, instant messages and voice messages. This list is constantly expanding and evolving. Communicational privacy protects the secrecy of such communications, including their contents, channels and the traffic data. Communications may be mediated or unmediated, resulting in different practices of controlling such messages. Relevant examples of communicational privacy in the area of border control are those of law enforcement guards intercepting personal communications, confiscating and accessing others' electronic devices, 'eavesdropping', or generally checking the content of stored communications without due reason.
4. *Proprietary privacy*: Proprietary privacy is the interest of an individual in their use of property as a means to shield activity, facts, things, or information from public view. At its core, it is closely associated to spatial privacy, being similar in the fact that the user has the right to exclude others from their property. They differ, however, in that proprietary privacy concerns tangible objects, while spatial privacy concerns a 'defined' area. Proprietary privacy is interfered with when, for instance, a person is compelled by a third party to reveal content in their purse, wallet, backpack, pockets, against their will. In other words, people choose to conceal certain objects, facts, situations or even body parts behind their (mobile) property and, thus, choose whether and to which extent they expose to public view what they have concealed. The nature of computer devices (including smartphones, laptops, wearables and IoT objects) is hybrid, and falls first of all within the scope of proprietary privacy, on the basis of being hardware.
5. *Intellectual privacy*: Intellectual privacy is the right of an individual to privacy of thought and mind, and the development of opinions and beliefs. This type of privacy, although separate, could be included in the scope of protection of several associated privacy rights, such as the freedom of thought. The direct influencing of a person's mind is not within the abilities of today's technologies, however indirect methods of inspecting people's minds though electromagnetic signals (or at least identifying patterns by tracing brain activity) is a technique that is widely used. However, in border control scenarios, it is not expected that people's minds be interfered with; the mind is censed to be an inviolable area.

6. *Decisional privacy*: Decisional privacy is the right of a person to defend against (state) intrusions into citizens' rights to hold or make certain choices pertaining to the intimate sphere; these could regard their lives and how they live them, such as choices about same-sex marriage, abortion or assisted suicide. Generally, decisional privacy protects human autonomy and expresses the intellectual privacy, mentioned above, with this being deemed the thought process and decisional privacy being the execution process, i.e. the manifestation of thought. All facts in relation to proactive, sexual and family choices, as well as disclosure of information about these, therefore fall within its scope of protection. In border control, this type of privacy is tangibly interfered with when technologies reveal sensitive information or facts about such situations, e.g. an obligation to reveal a tattoo upon the torso, illustrating upsetting or appalling images.
7. *Associational privacy*: Associational privacy is the right of individuals to choose their interactions and acquaintances, i.e. friendships, communities and groups they belong to (akin to the freedom of assembly). Such choices are protected under the concept of associational privacy, which can materialise in strictly private places, intimate settings or semi-public spaces, depending on the degree of exposure chosen. Associational privacy does not constitute the core of private life, but is an emanation thereof, while in the context of border control, it can be interfered with when multiple individuals are associated, i.e. a group of travellers from a certain country or with certain shared characteristics, friends belonging to the same organisation, religion, community etc.
8. *Behavioural privacy*: Behavioural privacy is the right of individuals to choose their public demeanour, which cannot be hidden from others observing it. Characteristics that fall under this type of privacy are facial characteristics, clothes, smell, gait, gestures, voice, language, mood, etc., that also, to a certain extent, cannot be instantly identified unless particular attention is given to the individual. Borders are representative of places, where natural persons would be compelled to protect their behavioural privacy, especially where they have to briefly undress or uncover areas of their body and thus make gestures that they would otherwise not need to do in public. Behavioural privacy is also related to the level of transparency and exposure chosen, yet some characteristics of the person cannot be hidden from public view (e.g. religious outfit). This type of privacy is interfered with when a technology substantially hinders or excludes a person from choosing how they behave publicly, due to a fear of being criticised about such mannerisms, e.g. how they walk, how they speak, how they move their hands or face, etc.
9. *Informational privacy*: Informational privacy is considered an interest of an individual in preventing information about themselves being collected and in controlling information about themselves that others may have a legitimate access to. It is both a type and meta-type of privacy, in the sense that, firstly, it refers to a distinctive type of privacy and, secondly, it overlaps with all other types. Interference with informational privacy essentially entails that the affected person lacks control over how information

about the eight aforementioned types is managed. Informational privacy is bifurcated into a positive freedom (informational self-determination) and a negative freedom (exclusion of others to information). This type of privacy has served as the foundation for the recent development of the distinct right to personal data protection, to a great extent also overlapping with it. The right to data protection is assessed separately, in the process of a data protection impact assessment (DPIA), and is a vital part of the integrated impact assessment. In border control, virtually all personal data fall, additionally, under the scope of informational privacy.

Figure 1: *A typology of privacy*



Koops, B. J., Newell, B. C., Timan, T., Škorvánek, I., Chokrevski, T., & Galič, M. (2017). *A typology of privacy*. In University of Pennsylvania Journal of International Law (Vol. 38, Issue 2, pp. 483–575).

Endnotes

1. Merriam-Webster, *Privacy*, https://www.merriam-webster.com/dictionary/privacy#synonyms.
2. Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (California: Stanford University Press, 2010).
3. Mireille Hildebrandt, *Law for Computer Scientists and Other Folk* (Oxford: University Press, 2020), https://lawforcomputerscientists.pubpub.org/.
4. Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193-220. https://doi.org/10.2307/1321160.
5. Ibid.
6. Glancy, D.J. The Invention of the Right to Privacy, *Arizona Law Review* 21, 4 (1979), http://law.scu.edu/wp-content/uploads/Privacy.pdf.
7. Ibid.
8. ECtHR, *Phull v. France*, Application no. 35753/03.

9. ECtHR, *Mann Singh v. France*, application no. 24479/07.
10. Global Privacy Assembly, *Adopted resolution on facial recognition technology*, 42nd Closed Session, 2020, https://edps.europa.eu/sites/edp/files/publication/final_gpa_resolution_on_facial_recognition_technology_en.pdf.
11. Serge Gutwirth, *Privacy and the Information Age* (Lanham, Md.: Rowman & Littlefield, 2002).
12. Gustavo Arosemena, "Human Rights," in *Introduction to Law* (Cham: Springer, 2017), 303–29, https://doi.org/10.1007/978-3-319-57252-9_13.
13. United Nations, Universal Declaration of Human Rights (UDHR), 10 December 1948.
14. United Nations (UN), International Covenant on Civil and Political Rights, 16 December 1966.
15. United Nations (UN), International Covenant on Economic, Social and Cultural Rights, 16 December 1966.
16. Convention on the Rights of the Child, New York, 20 November 1989.
17. The Treaty of Lisbon amended the Treaty of the European Union (TEU), in which Article 6(1) now reads: "The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties."
18. Article 7 ('Respect for private and family life') of the Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391-407.
19. Article 52(3) of the Charter reads: "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."
20. Article 52(1) of the Charter reads: "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."
21. American Convention on Human Rights, San Jose, Costa Rica, 22 November 1969.
22. African Charter on Human and Peoples' Rights, Nairobi, Kenya, 01 June 1981.
23. Article 29 of the Belgian Constitution reads: "Le secret des lettres est inviolable. La loi détermine quels sont les agents responsables de la violation du secret des lettres confiées à la poste", http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&table_name=loi&la=F&cn=1994021730.
24. European Union Agency For Fundamental Rights, European Court of Human Rights, and European Data Protection Supervisor, *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2018), 6.
25. Article 8 ECHR.
26. ECtHR, *S. and Marper v. the United Kingdom*, No. 30562/04 and 30566/04, 4 December 2008.
27. ECtHR, *Bărbulescu v. Romania*, No. 61496/08, 5 September 2017.
28. European Court of Human Rights, "Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence," (2020), https://www.echr.coe.int/documents/guide_art_8_eng.pdf.
29. Adam D. Moore, "Defining Privacy," *Journal of Social Philosophy* 39, no. 3 (2008): 411-428, https://ssrn.com/abstract=1980849.
30. Alan F. Westin, "Privacy and Freedom", *Washington and Lee Law Review* 25, no. 1 (1967): 166-170, https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?Article=3659&context=wlulr.