Volume **5** (2) 2023 https://doi.org/10.5204/lthj.2830

Biometric Harm

Sara Migliorini
University of Macau, Macau

Abstract

This article argues in favour of the recognition of biometric harm, which is a specific type of harm arising from the use of biometrics to identify and classify people without a valid legal justification. The importance and pervasiveness of biometric technologies have increased. The development of biometric systems is rapidly advancing; however, their potential negative implications for individuals and society are routinely dismissed or willingly ignored. Biometrics deeply affects some of the basic needs of humans, including the need to step out of one's social identities to enjoy unobserved time and the need to self-represent oneself in all social relationships. Such necessities are preserved by the legal system via high-ranked provisions that protect personhood, dignity, the right to private life and the right to express one's personality. Because of these negative effects on core human necessities and legal values, this paper submits that biometric identification should be considered harmful, unless justified by another equally fundamental legal value. In line with other restrictions of the involved fundamental values, necessity and law enforcement purposes may justify biometric identification. Conversely, it is submitted that consent, while essential, does not fulfil the requirements of a stand-alone justification for biometric harm.

***Keywords**:* Biometrics; biometric identification; identity; self-representation; private life; consent; freedom of expression.

Introduction

When the first instant cameras were developed, the legal implications of their power were instantly flagged. In their seminal article on *The Right to Privacy*, Warren and Bradeis, writing in 1890, foresaw that 'with the [arrival] of this technology and the growing popularity of print media, [covertly] taken photographs [would] threaten the "right to be let alone"'. [1] In our digital age, addressing the harms that may arise from unjustified intrusions into one's private life is one of the most crucial challenges facing the law. New technologies have exposed humans to risks of new harms by machines, and the role of the legal system is to understand such harms, to address them and to redress the losses related to them.

This paper focuses on systems that are able to identify humans based on their bodily or behavioural features, known as biometrics,[2] and tries to detail the ways in which biometrics is harmful to humans individually and to society generally.

The arguments developed in this paper presuppose the view that interpretations of technologies are grounded in society.[3] As Nissenbaum so aptly stated, 'systems and devices will embody values, whether or not we intend or want them to'.[4] Accordingly, this paper puts forward an interpretation of biometrics that allows us to preserve basic human values rather than one that focuses on the performance or accuracy of the technology without regard to the consequences.

The paper takes forward arguments developed in the field of privacy, which have maintained that privacy is essential to freedom, personhood and dignity,[5] and draws from conceptual reflections in legal and non-legal disciplines regarding the legal values upholding the need for unobserved time. The reflections in this paper also own a debt to authors who have highlighted

[1] Warren and Bradeis, "The Right to Privacy."
[2] A more detailed definition is provided in Section 1 of this paper.
[3] Graber, "How the Law Learns," 7.
[4] Nissenbaum, "How Computer Systems Embody Values."
[5] DeCew, "Privacy;" Gavison, "Privacy."

the complexity of the different situations that have come to be subsumed under the umbrella concept of 'privacy' and the different types of intrusions or privacy harms,[6] as well as to authors who have argued that seeking to define privacy takes the focus away from harm arising out of intrusions, which is what the legal system should be concerned about.[7] At the same time, this inquiry is also mindful of attempts to conceptualise data protection as a fundamental core provision of some legal orders (i.e., in the European Union [EU]) and of studies that have critically assessed the whole field of 'data protection',[8] in particular, the special regime applying to 'sensitive data' of the kind used by biometrics.[9] All these contributions are essential to the arguments developed in this paper, which attempts to provide a framework for assessing biometrics based on the potential harm that biometrics might cause to individuals and society.

Further, this paper shows that because of the way in which biometrics works and in light of its defining features, it affects certain basic needs of humans protected by the legal system; that is, personhood, human dignity, private life and freedom of expression. The core claim of this paper is that a specific 'biometric harm' needs to be recognised to continue to uphold such values in our digital society. This paper defines biometric harm as the harm arising from identification via biometrics without a valid legal justification and claims that, by recognising biometric harm in these terms, the legal system upholds an interpretation of biometrics that bolsters these values, rather than one that undermines them.

This paper argues for a switch from a subjective point of view that focuses on the harm suffered by one individual in a specific case of privacy invasion or data breach to one that focuses on how a technology, by its very features, systematically affects certain legally protected rights of the individual and interests of society as a whole. This switch justifies bypassing discussions regarding the threshold of what constitutes reparable harm in cases of biometric harm. The issue of compensation is also excluded from this paper and hopefully will be discussed in future research.

The paper briefly describes how biometrics works (Section 1) and how fundamental human needs (Section 2) that are protected by the legal system (Section 3) are negatively affected by biometrics (Section 4). It then considers what justifications for biometric harm should be admitted (Section 5).

1. Overview of Biometrics and Definitions

The word 'biometric' refers to measurements of the human body. Expressions such as 'biometric data' or 'biometric features' are used today to refer to such measurements. With respect to modern technologies, biometric data include biological characteristics, such as face, fingerprints, hand geometry and iris, and behavioural characteristics, such as signature, keystroke, voice and gait.[10]

In the engineering field, the term 'biometric' is also used to qualify a process; that is, the 'automated recognition of individuals based on their biological and behavioural characteristics'.[11] 'Recognition' includes both biometric identification, which is the process of searching against a biometric database to find a previous record with the purpose of extracting the identifier attributable to a single individual, and 'biometric verification', which is defined as the process of confirming a biometric claim (i.e., 'this person is John Smith') through comparison.[12] For simplicity, the term biometric 'identification' refers to both these processes in this paper. The technical definition of biometrics is retained in the paper, with the following specification: 'identification' is used in a broad sense and includes any attribution of identity: a civil identity, the membership to a societal group (e.g., 'female' or 'white'), a behaviour (e.g., 'smoker') or an emotion (e.g., 'sad').

A central element that emerges from these definitions is that biometric data do not have a stand-alone existence but are collected, stored and retrieved with the sole purpose of recognising a person. As will be explained later in this paper, this inextricable link between biometric data and the function of identifying a specific individual or assigning an individual to a specific group is crucial to the discussion of what kind of harm can arise from biometric technology.

[6] Solove, "A Taxonomy of Privacy."
[7] Kugler, "From Identification to Identity," 111.
[8] Renieris, Beyond Data.
[9] Solove, "Data is What Data Does."
[10] Micheli-Tzanakou, "Biometrics: Terms and Definitions."
[11] International Organization for Standardization, ISO/IEC 2382-37:2022(en), *Information technology — Vocabulary — Part 37: Biometrics* 2022.
[12] ISO/IEC 2382-37:2022(en), n 14. In this context, the term "comparison" means the "estimation, calculation or measurement of similarity or dissimilarity" between the biometric data points.

The technology that enables the collection and analysis of biometric data today is extremely advanced; however, the idea of measuring, storing and classifying biometric information of individuals to facilitate their future identification is rather old. The first biometric identification system is attributed to Parisian police officer Alphonse Bertillon, who, in 1879, created a method to take and store biometric measurements of individuals with a criminal record.[13] Bertillon made it his life mission to perfect a standardised and teachable method to identify individuals based on their bodily measurements.[14] Bertillon's endeavour eventually failed, and his system was gradually replaced by the use of fingerprints.[15] As it has been suggested, the historical and logical association between Bertillon's system of identification and the attempts to link the bodily characteristics of individuals to their proclivity to crime and more generally to classify humans into races[16] should alert us to the risks associated with modern biometric technology.[17] Instead, oblivious to this warning, companies and governments are routinely employing biometrics[18] to identify personality traits and skills, and categorise people into groups.

Because of the push from both the public and the private sector towards ever-more-accurate biometrics, the field has evolved dramatically. On the one hand, biometric technology is routinely employed to make common, repeated tasks (e.g., unlocking one's phone with fingerprints or facial recognition) smoother. On the other hand, research into biometrics has also pursued the aim of reducing the need to obtain the subject's collaboration – and even consent – to the collection of biometric data for identification purposes. As described earlier, the process of biometric identification requires a previous collection of data and the storage of that data in a database, against which future samples are compared. In most cases, collecting the biometric data of a person requires the cooperation or at least their consent. In addition, when the samples of a person are collected a second time to facilitate identification, the person is usually required to cooperate and consent again.

However, research in biometrics seems to view the need to obtain collaboration from a data subject as an 'inconvenience': custom clearings and other operations would be smoother if identification could be done without asking people to stop by a counter and show their face.[19] Pursuing this idea, systems have been developed to identify people in public spaces from a distance. Research has produced different systems that allow for 'on-the-fly' or even 'in-the-wild' acquisition of biometric data, which allow people to be identified with minimal or no collaboration at all. The main consequence of allowing such biometric identification is that it occurs without consent or even awareness. with the main consequence of allowing biometric identification without consent or even awareness. For example, techniques to recognise individuals using images of eye movements taken on smartphones were developed after the use of face masks became widespread during the Coronavirus Disease 2019 pandemic, as face masks impaired the use of classic facial recognition technology.[20] Other examples are systems capable of identifying people by analysing their finger knuckles from a distance[21] or assigning gender to people using different reference points without the cooperation of the subject.[22] Needless to say, once developed, these technologies are not only used in law enforcement settings; rather, once they exist, they are deployed widely by public and private entities for law enforcement and commercial purposes alike.[23]

Another important development in the field of biometrics has been the perfecting of techniques to exploit soft-biometric data (i.e., data that identifies not a single individual but a group), relying on categories naturally used by humans to describe each other, such as 'tall' or 'short'.[24] Though less accurate, these data can still enable the identification of individuals when different data points are collected and combined or when these data can be combined with other types of data. The use of soft biometrics also allowed humans to recognise other humans in instances in which software cannot (e.g., in blurred images).[25] Another type of soft biometrics uses clothing to identify people.[26] While clothes may be changed, clothing descriptions can be standardised and used for recognition within a limited time frame.

[13] Bertillon, La Photographie Judiciaire; Bertillon, Identification Anthropometrique.
[14] Helfand, Face.
[15] Arbab-Zavar, "On Forensic Use of Biometrics."
[16] For example, Lombroso, L'Uomo Delinquente.
[17] Helfand, Face; Gray, "Bertillonage."
[18] As reported by Raposo, "(Do Not) Remember My Face," 4.
[19] Dvořák, "On the Fly;" Bilan, "Interactive Biometric Identification System."
[20] Alonso-Fernandez, "Facial Masks."
[21] Cheng, "Contactless."
[22] Roxo, "Is Gender 'In-the-Wild' Inference Really a Solved Problem?."
[23] See Raposo, "(Do Not) Remember My Face."
[24] Reid, "Soft Biometrics."
[25] Reid, "Soft Biometrics."
[26] Jaha, "Soft Biometrics for Subject Identification."

In addition, sensitive soft-biometric information (e.g., gender, race or age) can be directly derived from facial embeddings.[27] Unlike facial recognition, where one's facial features are compared to pre-existing facial templates to establish if a person is known, face detection and analysis do not recognise people but 'detect' and classify them into categories, including categories for gender, age and emotion, based on the processing of their facial features. For example, smart billboards use these techniques to display advertisements tailored to the specific group to which the person passing by is assigned by the biometric system.[28] Worryingly, methods to encrypt and protect such information appear to be less effective than usually stated in the scientific literature.[29]

This brief overview of the great variety of biometric technology, allows us to grasp the extent of the intrusiveness and potential harms that these technologies carry within them.

2. Unobserved Time and Self-Representation as Basic Human Needs

Many scholars of privacy have long argued that it is essential for human beings to be sure that some instances of life are private. One aspect of this fundamental need relates to the necessity to be able to enjoy unobserved time, away from the gaze of others, to maintain our natural status of mental health.[30] Allen argued that privacy – in the forms of anonymity, seclusion, solitude and secrecy – entails 'a condition of inaccessibility of the person, his or her mental states, or information about the person to the senses or surveillance devices of others'.[31] It may be added that such conditions of inaccessibility also need to be perceived as such by the individual. Studies have shown that the perception of an external gaze or the fear of being observed can also negatively affect the mental health of a person.[32]

Another aspect of the need of private time and space, which is closely connected to the first one, relates instead to our social self: privacy in the form of a private enclosure and control of one's personal information has been considered essential to intimacy and intimate relations[33] and consequently to the possibility of developing healthy social relationships with others.[34] Humans are social animals and view connection to others and community as fundamental needs.[35] Yet, withdrawing from the social arena is an equally important requirement for humans. Crucially, studies in social psychology have clarified that withdrawing from others allows us to withdraw from the role that we fulfil in our relationship with them.[36] We routinely alter our behaviour based on the people that we know are present at any given time.[37] For example, we behave differently with our friends than with our employer.[38] Private time and the possibility of shielding ourselves or our personal information from others allows us to maintain these different identities and behaviours[39] and to retain control of our social relationships. Under this perspective, the need for unobserved time can be construed as a right to 'selective self-representation'.[40]

This ability of stepping in and out of our multiple social roles allows us to function as human beings. As sociologist Barry Schwartz pointed out, role and identity are deeply intertwined from the point of view of our relationship with others: 'the very act of placing a barrier between oneself and others is self-defining, for withdrawal entails a separation from a role and, tacitly, from an *identity* imposed upon one-self by others via that role'.[41] Since biometrics attributes an identity to individuals, the need to withdraw from the identity that we are assigned in our different social roles is very important to understand how biometrics can harm humans.

Studies have examined whether the needs outlined above are found across cultures, which would support the idea that these needs are basic needs of all humans, at all times and in all places. In the negative, such needs would only pertain to certain cultures and historical moments. For example, some studies have described how apparently close cultures have a very different

[27] Terhörst, "On Soft-Biometric."
[28] Purtova, "From Knowing by Name," 163.
[29] Osorio-Roig, "An Attack."
[30] Calo, "The Boundaries."
[31] Allen, Uneasy Access.
[32] Calo, "Boundaries."
[33] Gerstein, "Intimacy and Privacy."
[34] Gerstein, "Intimacy and Privacy."
[35] Rachels, "Why Privacy."
[36] Schwartz, "Social Psychology."
[37] Rachels, "Why Privacy."
[38] Rachels, "Why Privacy."
[39] Hughes, "A Behavioural Understanding."
[40] Baghai, "Privacy as a Human Right," at 956.
[41] Schwartz, "The Social Psychology," 747.

understanding of 'what should be kept private'.[42] Accordingly, the temptation may be strong to dismiss the need for unobserved time and to step out of our social roles as a mere question of cultural attitude. However, this view is somewhat misleading. Solid arguments support the idea that humans share a need to enjoy unobserved time and to self-represent themselves in their social relationships. However, such needs may be mediated by cultural elements and beliefs. Studies rooted in anthropology have found that even civilizations living in a state of 'continuity between the individual and the community' had their ways of ensuring some form of privacy.[43] Such studies showed that at the core, humans have a universal need to shield themselves from the external gaze and retain control over their self-representation.

In addition, it has been convincingly argued that 'in each civilization, as it advanced, those who could afford it chose the luxury of a withdrawing place'.[44] If a shield from public observation is worth paying for, the fact that some cultures may be more open than others regarding public information or public nudity does not prove that humans do not feel the need to withdraw from society from time to time. Indeed, poverty is usually associated with the use of communal spaces and thus less privacy, while more affluent individuals tend to pay for increasing levels of seclusion. Allen argued that women, as a vulnerable group in society, experienced less privacy than men.[45] It seems then that economic and social conditions play a crucial role in the possibility to afford and enjoy unobserved time, seclusion and withdrawal from society. Accordingly, the lack of enjoyment of unobserved time should more correctly be associated with a lack of means rather than a lack of need.

From a different perspective, studies in the field of philosophy have highlighted the importance of preserving our informational space because it is deeply entrenched with our own identity and dignity.[46] As Floridi pointed out, humans are 'essentially made of information'[47], insofar as the information about each individual determines who that individual is and who they can become. A fundamental feature of the human conceived as an informational being is to be able to keep their 'identities and [their] choices open'. This concept echoes the idea of self-determination in our social relationships and the need for a private space. Against this backdrop, Floridi also clarifies the role and the limit of technology: 'any technology or policy that tends to fix and mold such openness [of our identities] risks dehumanizing us'.

This reality – that human beings need private, unobserved time and space to preserve their own humanity – is one of the reasons why the collection, processing and storing of personal data, including biometric data, may expose human beings to harm. As mentioned, this paper subscribes to the idea that technology should be interpreted in a way that allows us to uphold the fundamental values that pertain to our humanity. In addition, as it will be explained in the next section, the need for private time and space, the need to self-represent socially and the relationship these needs have to our very essence as human beings is protected in various forms by the legal system across jurisdictions.

3. The Legal Protection of Unobserved Time, Self-Representation and Human Dignity in the Age of Biometrics

When identifying a person, biometrics may or may not run afoul of privacy or data protection laws. Indeed, in many instances, biometric identification will be perfectly legal, depending largely on consent or other requirements.[48] However, this paper discusses the higher level of the hierarchy of norms. Indeed, if all humans need unobserved time and the opportunity to withdraw from their different social roles, and if such needs are fundamental for our very own survival as individuals, it is natural to investigate how the legal system protects these needs. Logically, legal provisions protecting these needs must be of a fundamental nature if they are to protect some of the core requirements of humans. This paragraph explores this issue further.

Broadly conceived, the essential needs of human beings discussed in the preceding paragraph are found in the legal system under different names, such as the right to private life or privacy, human dignity and freedom of expression. Legal systems across the globe protect these values differently. This paper refers to the provisions of the European Convention on Human Rights (ECHR), which are part of the legal systems of the Council of Europe's members and thus apply in roughly 20% of countries in the world. I acknowledge that this reference only provides a partial view of how these basic human needs are

[42] Whitman, "The Two Western Cultures of Privacy."
[43] Amply documented in Moore, "Privacy."
[44] Moore, "Privacy," 222.
[45] Allen, Uneasy Access.
[46] Floridi, "On Human Dignity."
[47] Floridi, "On Human Dignity.", at 310.
[48] For example, under the General Data Protection Regulation (GDPR), biometric information is subject to an enhanced regime, but the collection, processing and storing of such information (Art. 9) is legal if it meets all the requirements of the regime.

protected by legal systems globally, and I hope that this contribution initiates a dialogue on how other legal cultures approach the same basic human needs and how a given legal system protects them.

The first category of provisions that are relevant to the basic needs of humans described above comprises those protecting private life, personhood and dignity. [49] In the ECHR, these provisions are all found in Art. 8, and the reading of it by the European Court of Human Rights (ECtHR). Article 8 of the ECHR has a strict formulation and provides that 'everyone has the right to respect for his private and family life, his home and his correspondence', and that public authorities should refrain from interfering with this right, except under the conditions laid down by law.[50] However, the ECtHR has expressed the view that the concept of 'private life' under Art. 8 of the ECHR should be interpreted broadly and is not susceptible to exhaustive definition. It is meant to protect the overall moral and physical integrity of an individual,[51] including the right to be let alone, away from unwanted attention.[52] The guarantee afforded by Art. 8 of the ECHR in this regard is primarily intended to ensure the development, without outside interference, of the personality of each individual in their relationships with other human beings.[53] There is thus a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life.[54]

In relation to individuals' images in particular, in *Hannover*, the ECtHR affirmed that 'a person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from their peers. The right to the protection of one's image is thus one of the essential components of personal development'.[55] The mere storing of data relating to the private life of an individual amounts to an interference with the right to private life under Art. 8 of the ECHR,[56] and the subsequent use of the stored data has no influence on such qualification.[57] In relation to biometrics, the ECtHR has held that fingerprints and deoxyribonucleic acid (DNA) constitute data pertaining to one's 'private life' and their retention amounts to an interference with the right to respect for one's private life within the meaning of Art. 8 of the ECHR.[58] In a more recent case concerning pictures taken and stored by law enforcement officers, the ECtHR also empathised that the rapid development of increasingly sophisticated techniques allowing facial recognition and facial mapping from individuals' photographs, makes the taking of their photographs, the storage and possible dissemination of the resulting data problematic from the point of view of Art. 8 of the ECHR.[59]

The second category of provisions that are relevant with respect to the need to enjoy unobserved time and be able to self-represent oneself relates to freedom of expression. Most commonly, freedom of expression is understood as referring to the right to free speech and the limits of what can be said or published without infringing on the rights of others. Nonetheless, this is not the primary meaning of freedom of expression that is relevant for the present inquiry. Instead, at its core, the freedom to express oneself that is relevant to the need to be shielded from reachability is the idea highlighted previously by Warren and Bradeis more than a century ago: the right to 'simply be'.[60] It is the right of the individual to own their own personality and to express it 'in writing, or in conduct, in conversation, in attitudes, or in facial expressions'[61]. Along this line, Art. 10 of the ECHR covers ideas and forms of expressions of different natures, including political communications,[62] artistic expressions of

[49] Bloustein, 'Privacy;" Floridi, "On Human Dignity."
[50] More specifically, Art. 8(2) of the ECHR provides "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."
[51] *X and Y v the Netherlands* [1985] Eur Court HR (ser A) no. 91, 22–27.
[52] *Smirnova v Russia* [2003] Eur Court HR 95.
[53] *Couderc and Hachette Filipacchi Associés v France* [GC] [2015] Eur Court HR; recently reiterated in *Sağdiç v Turkey*, 9142/16, [2021] ECHR 048
[54] *Couderc and Hachette Filipacchi Associés v France*[GC] [2015] Eur Court HR.
[55] *Von Hannover v Germany* [2004] Eur Court HR IV 96.
[56] *Leander v Sweden*, 26 March 1987, Series A no. 116. 48. See also Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), to which the ECtHR refers in these judgments.
[57] *Amann v Switzerland [GC]*, ECHR 2000-II, 69.
[58] *S. and Marper v the United Kingdom* [2008] ECHR 1581.
[59] *Gaughran v United Kingdom* [2020] ECHR 144, 70. See also the elaboration made in the Guide to the Case-Law of the of the European Court of Human Rights – Data Protection, 31 August 2022, https://echr.coe.int/Documents/Guide_Data_protection_ENG.pdf.
[60] Warren, "The Right to Privacy."
[61] Warren, "The Right to Privacy." at 206.
[62] *Markt intern Verlag GmbH and Klaus Beermann v Germany*, § 26

various kind,[63] the publication of photographs,[64] the choice of items of clothing[65] or other symbols,[66] as well as the use of the 'Like' button on social media.[67]

This aspect of freedom of expression is highly relevant to biometric identification. By recording the unique physical features or external manifestations of individuals, biometrics appropriates and exploits forms of expression of one's 'inviolable personality'. At the same time, biometrics infers personality or psychological traits from the physical or behavioural features of a person. In so doing, biometrics overreach into an individual's core building blocks, the ones that cannot be changed, and put a label on them by proceeding to biometric identification.

Any interference with the fundamental rights to a private and family life and to freedom of expression protected under Arts. 8(1) and 10(1) of the ECHR, respectively, may be justified by the conditions set forth in the same articles, which have both been applied and refined by the ECtHR.[68] At its very essence, justification is dependent on an assessment of necessity with respect to a public interest aim and the relationship of proportionality with such an aim. In practice, justification often involves balancing with other equally fundamental rights.

A human-centric interpretation of biometrics cannot but uphold the values of private life and freedom to express one's personality as conceived in the ECHR and which corresponds to some of the most basic human needs. If such an interpretation is not adopted, we are at risk of developing and normalising a technology that runs counter not only to our very essence as humans but also to values and rights that sit above all other legal provisions.. Following this line of reasoning, this paper claims that the relationship between technology, fundamental rights and the legal system can be framed in terms of harm and justification: for the legal system to maintain its coherence, any technology that is able to interfere with fundamental rights, both at the individual and societal level, must be considered harmful, unless it is possible to find a justification for such harm in an equally fundamental right that must be upheld in a particular situation.

4. Biometric Identification as Detriment

The detrimental effect of biometric identification, framed as interference with basic human needs that are protected by highly ranked provisions, such as Arts. 8 and 10 of the ECHR, can be characterised with respect to both individuals and to society as a whole when many individuals are systematically subject to biometric identification.

As mentioned previously, biometrics search a sample against a database to find a corresponding previous record of the same, with the purpose of extracting from the database the identifier matching the sample.[69] This process leads to an identity being attributed to the individual. The word 'identity' must be understood in a broad sense as referencing the uniqueness or distinctiveness that allows a biometric system to categorise a person. Thus, it can be a civil identity, constituted by the name or the social security number of a person, or a group identity, such as 'woman' or 'Caucasian', or a profiling identity that relates to personal, political or commercial behaviour, such as 'heterosexual', 'left-leaning voter', or 'smoker', or finally an emotion. Therefore, the key feature of biometrics is that it uses the unique characteristics of an individual's body – physical or behavioural – to assign that individual a corresponding identity among those that have been pre-entered in the database. Accordingly, the notion of 'biometric identification' used in this paper covers a vast array of situations in which the unique, external appearance of a human or their unique bodily features (such as DNA) are connected to a certain distinctiveness that determines part of how that individual is perceived in a public space (i.e., 'John Smith' or 'a white male'). Biometric identification is thus a process that relies on the appearance or bodily information of a person, most of which are unique and unchangeable, and allows a third party (i.e., the entity who compiled the database) to define (part of) the self of that person and their role in the public sphere. In this context, the expression 'public sphere' here means any subset of society (e.g., the digital or physical word, a small gym circle, the borders of a country or any other large or small social *locus*), the access to which is made dependent on biometric identification. Admittedly, much of this process recalls Berthillon's early attempts to classify human beings.

[63] *Müller and Ors v Switzerland*, § 27; *Ulusoy and Others v Turkey*
[64] *Axel Springer AG v Germany* [GC]; *Verlagsgruppe News GmbH v Austria* (no. 2)
[65] *Stevens v the United Kingdom*, Commission decision.
[66] *Vajnai v Hungary*, § 47.
[67] *Melike c/Turquie*, 15 juin 2021, n°35786/19.
[68] Generally, on this test see: Gerards, "How to Improve the Necessity Test" and the many references cited therein.
[69] See above, footnote 10.

Because biometrics simply looks for a match in a pre-established database, biometric identification takes place in a closed system: it can only be 'accurate' or 'false' with respect to the database.[70] Biometric identification does not depend on any objective truth (e.g., my correct civil identity) or any subjective truth (e.g., the identity that I choose for myself). Biometric identification pays no regard to the real-world identity of the individual or to their self-determination and autonomy. To the contrary, the individual has no control over their attributed identity, which depends entirely on the classifications in the database, made by a third party, and on how accurate or how biased the compilers of the database have been, on whether the sample was correctly collected or labelled and on all other variables that can affect the database.

Just by focusing on this basic feature of biometrics, it becomes clear that the process is at odds with the framework emerging from a review of human needs and fundamental rights. Under this framework, an individual should be the master of their own 'informational narrative' and any technology that restricts such freedom to self-determine in our social relationships is dehumanising'. .[71]This is true even in situations where the harm suffered by society and by the individual does not appear to be obvious. For example, one may contend that there is hardly any detriment in revealing someone's correct civil identity via biometric identification. However, counterintuitively, several red flags are raised in such a situation.

First, security is a real issue when it comes to relying on biometric data. Biometrics relies on collecting, processing and storing the bodily or behavioural characteristics of a person, which are truly unique and unchangeable: humans only have one set of fingerprints or retinas. As the Illinois Supreme Court pointed out, applying the Biometric Information Privacy Act (BIPA), a specific statute regulating biometric data use, 'technology now permits the wholesale collection and storage of an individual's unique biometric identifiers – identifiers that cannot be changed if compromised or misused'. [72] Consequently, the Supreme Court was of the view that when biometric data are mishandled 'the right of the individual to maintain [his or] her biometric privacy [vanishes] into thin air'.[73] Therefore, it is exactly when biometric identification is used to attribute a correct civil identity that it exposes the individual to a very high cybersecurity risk. As it has been correctly pointed out, the risks associated with privacy loss are crucial in understanding different types of privacy harms,[74] and in a digital society should be the way in which we conceptualise harms related to it.

Leaving aside the cybersecurity risks, it could be argued that correct biometric identification can hardly be detrimental to an individual. This argument is unconvincing. Even when the attributed civil identity is correct, the person subject to the biometric identification is still classified or given a specific identity, which will then determine their place in the relevant social space and their prerogatives within it. For example, entrance to a venue, such as a gym, may be subject to facial recognition. Biometric identification in this case would be something along the lines of 'this person is John Smith, a gym member'. It is submitted here that in terms of harmfulness, it is not the correct/incorrect nature of a biometric statement that is crucial but the process itself'.

In a related situation and to take the argument further, one may argue that there is hardly any detriment in being subject to biometric identification when an identification document, such as a passport, would have to have been presented anyway. This is another situation in which the harm is not obvious but quite substantial, both for the individual and for society as a whole. First, the same cybersecurity risks that exist in any situation in which biometric data are used to match a sample with a civil identity and all information that may be linked to such identity in a database, still exist in this situation. Second, the detrimental aspect in this situation relates to the repetitive and systematic use of this technology in situations in which a piece of identification is required, as if it were interchangeable with other types of identification that do not rely on data storage and software. In a recent decision,[75] the Court of Justice of the European Union (CJEU) reviewed under applicable EU law a piece of national legislation that provided for the systematic collection and recording of biometric and genetic data of any person accused of an intentional offence subject to public prosecution. In the CJEU's view, such automatic biometric identification and collection of data interfered with the rights and freedoms of the person concerned and had to be limited. In particular, the collection and recording of biometric data for people accused of a criminal offence should only be allowed under certain conditions; that is, 'collection is strictly necessary for achieving the specific objectives pursued' and 'those objectives cannot be achieved by measures constituting a less serious interference with the rights and freedoms of the person concerned'. In short, in the CJEU's view, a form of identification that is less invasive should be routinely preferred. This solution appears rooted in

[70] In cases in which a biometric system uses the internet to search a collected sample, the system it is still to be considered "closed" in the sense of the example of Clearview AI.
[71] Floridi, "On Human Dignity."
[72] *Rosenbach v Six Flags Entertainment Corp.,* 34.
[73] *Rosenbach v Six Flags Entertainment Corp.,* 34.
[74] Solove, "A Taxonomy of Privacy."
[75] CJEU, Case C-205/21, *Criminal proceedings against V.S.*, ECLI:EU:C:2023:49

the idea that it is not so much the result of biometric identification that counts (i.e., identifying and keeping a record of a person) but rather the process itself and how it affects the rights and freedoms of an individual that is detrimental.

In other scenarios, one may argue that there is hardly any detriment when an 'identity' is attributed to someone (e.g., 'this person is white' or 'female'). First, as mentioned earlier, this process, which is done automatically and systematically when biometrics are in place, violates the need of humans for self-determination in their relationships and control their own 'informational narrative'. Further, and rather counterintuitively, allocating a person to a certain social group, carved out arbitrarily based on ethnicity or other features, seems to carry with it even more negative consequences than assigning a person a civil identity. This type of situation appears to be particularly dangerous with respect to individuals that may belong or be assigned to groups that are traditionally marginalised or discriminated in society, thus crystalising the divides that characterise our societies. For example, let us imagine a facial recognition software program in a mall or a commercial venue that assigns passers-by to a group for the purposes of showing advertisements on a smart billboard and that identifies one of these passers-by as follows: 'the person is female'. Another example would be placing a biometric system in a public venue for the purposes of law enforcement that identifies someone as follows: 'the person is a white male'. This process may seem neutral and not harmful, as, after all, our own brains are wired in the same way, and we explain the world based on categories that we have inherited or built from our past experience. Yet, there are very important red flags to notice. Let us now imagine that the biometric statements in the examples above are completed by decisions such as, in the first case, 'the person is female, so she has limited spending potential' or, in the second case, 'the person is a white male, so he must not be searched'. In these situations, it is clear how biometric identification coupled with the biases that affect our society can lead to certain groups being relegated to a position of subalternity and others to a position of privilege, perpetrating existing inequalities.

These examples are worrying enough as they are, but they become worse when we switch perspective from the individual level to the societal level. Biometric features, even those exploited by 'soft biometrics', are non-modifiable. We are still in the dark regarding the chilling effects of biometrics on individuals who may be assigned to groups that are traditionally marginalized or discriminated. Some research has shown that surveillance, even in the mere form of observation, engenders a loss of creativity and anxiety.[76] As a result of the embedding of biometric identification and biases, individuals pertaining or perceived to pertain to one or more of such groups may refrain from participating in certain social activities, or from attempting certain social endeavours, such as applying for a job, and overall self-limit their creative potential. As Cohen noted, the ability to remain anonymous and to represent oneself enables humans 'to develop intellectually and emotionally by giving us breathing room to embrace risks and make mistakes without the stigma of being forever associated with failures and fads'.[77] More generally, coding people's public identity - and the way in which they should experience the word - into biometric systems used by authorities and commercial actors condemns them to never be able to change society's perception of them as individuals and their place in the world.

All the previous examples break down how a society in which biometrics are routinely used to identify and classify people and eventually make decisions about who they are and how they should experience the world, runs contrary to basic needs and fundamental rights and is ultimately dehumanising, especially for those who already experience exclusion and marginalisation. On a more general level, we can say that what leads to harm is that biometric identification breaks the anonymity or inaccessibility of the person subject to it by using their irreplaceable physical features. In Nissenbaum's terms, a person subject to biometric identification becomes 'reachable', in the sense that someone can potentially come knocking on their door 'demanding explanations, apologies, answerability, punishment, or payment'.[78] More precisely, in our data-driven, digital society, after biometric identification, we become reachable by a government agency, a technology company or an advertiser. Some part of our self, or the perception of it by the dominant external gaze of society, as revealed by our unique biometric manifestations, becomes known to a third party, which will act on it, affecting our place in the world and our interactions with the public sphere.

In addition, the time spam of reachability following biometric identification can potentially be unlimited, as can the geographical and personal reach of those who have access to the biometric statement made after biometric identification – even though under data protection law, they may be denied access to the biometric information itself. In 'reaching' a person, using unique physical features, and then by fashioning an environment that is thought to be adapted to them, biometrics uses our very basic essence as humans to affect our basic human need to withdraw from the social arena, potentially fixing such identification in space and time.

[76] Solove, "Risk and Anxiety."
[77] Cohen, "What Privacy;" Selinger, "The Inconsentability."
[78] Nissenbaum, "The Meaning of Anonymity," 142.

5. Competing Values and Consent as Justifications For Biometric Identification

Intrusions in one's private life or limitations of freedom of expression are possible in instances where a balance must be struck with other equally fundamental values. In a similar fashion, we can imagine cases in which, to preserve another competing value, biometric identification could be justified, and thus the harm suffered by the individual subject to biometric identification must be accepted.

At the outset, situations of blunt necessity may be easily qualified as apt to justify biometric identification. An example is the biometric identification of an individual who arrives at an emergency room department, requiring an emergency or life-saving treatment. In other instances, the necessity of biometric identification is more contentious; for example, in the case of biometric identification for law enforcement purposes. Indeed, this use of biometric identification has been debated by legislators, courts and society at large. The degree to which biometric identification for law enforcement purposes can be tolerated gives rise to warrants different opinions and may lead legislators and courts to diverge in their determinations of how to strike a fair balance between security and respect of private life, freedom and dignity. Nevertheless, it is not the most contentious point, insofar as public security or the need to ensure the prosecution of criminal offences are generally accepted fundamental needs of society that do lead to restrictions of fundamental rights, such as personal freedom or private life, to different degrees according to the political and legal system of a given jurisdiction.

Conversely, an easily accepted justification for biometric identification appears extremely problematic to conceptualise – consent. Liberal democracies associate consent with the idea of individual self-determination. Under this perspective, privacy has been construed, under the United States Constitution, as shielding people's intimate decisions from the intrusion of the Federal State. This vision of freedom and autonomy has also led to a very restrictive view regarding the extent to which the commercial exploitation of one's own biometric features can be limited. For example, as a consequence of the right of everyone to decide autonomously how to monetise their own appearance, French courts remain reluctant to apply the limit of human dignity to contractual stipulations when someone has ceded the right to their image, including in instances in which the images taken as part of the contract may be considered embarrassing or damaging of that person's dignity.[79] In the field of data, in many jurisdictions, the legal framework has been built around the possibility of giving consent to the collection, storing and processing of all kinds of personal data, including those of a sensitive nature,[80] which has given rise to very successful business models that rely on the monetisation of the personal data of others.

Yet, the consentability of biometrics has also been heavily questioned by scholars. Selinger and Hartzog argued that facial recognition technologies that seek 'to monitor behaviour, identify people, or gain insight or information for the purposes of influencing, managing, directing, or deterring people' should not be consentable.[81] Building on their previous work and work by others, they argue that consent is flawed in our digital era, because of the many, unpredictable and multifaceted ways in which data can be used via digital technologies.[82] In addition, they argue that face recognition should not be consentable because of the systemic effect that many individuals consenting to it may have on our collective autonomy. They also point to the triviality of the arguments that are usually put forward to bolster the use of facial recognition, such as convenience and the simplification of mundane tasks.[83] Allen argued that, while this may be seen as paternalistic or unpopular, people should not be allowed to consent to limitations of privacy for trivial reasons, such as convenience, as privacy is a primary or foundational good 'on which access to many other goods rests'.[84]

Custers and Margieri recently argued that the consentability of transfers of one's own personal data to access commercial services, such as search engines and social media, is untenable within the legal order of the EU, as the right to data protection is a fundamental right protected by the Charter and is thus inalienable.[85] Finally, others have argued that in many instances, the use of biometric systems makes it practically impossible to obtain consent, which has more to do with the way in which the technology is evolving and the uses to which it is put than any technical impossibility. For example, a home security camera that deploys facial recognition makes it practically impossible to obtain consent from all passers-by.[86] It should be added to these critiques that biometrics uses the unchangeable bodily features of individuals and thus represents a damage to their personhood, especially when coupled with the risks associated with loss or theft.

[79] Cour de cassation, Civ. 1, 20 octobre 2021, 20-16.343, Inédit.
[80] See, for example, the GDPR and BIPA.
[81] Selinger, "The Inconsentability."
[82] Richards " The Pathologies."
[83] Selinger, "The Inconsentability.", at 49.
[84] Allen, Unpopular Privacy.
[85] Custers, "Priceless Data."
[86] Kugler, "From Identification to Identity," 117.

If we wish to uphold a value-preserving interpretation of biometrics, we need to push for a review of their consentability. This paper argued that biometric identification is detrimental to basic human needs; that is, the need to enjoy unobserved time and the need to be able to step in and out of the roles that we fulfil in our social relationships and the identities attached to them. It also found that other core values may be able to offset biometric harm and offer it a legal basis. In line with the findings of Selinger, Hartzog and Allen, it is submitted that consent should not be considered a stand-alone legal basis for biometric identification, justifying biometric harm.

At the same time, it is argued that even in cases where a core value provides a valid justification for biometric harm, consent shall remain an important element of the legal regime upholding such justification. For example, in certain jurisdictions, it may be legal to collect the biometric data of people convicted of certain criminal offences but the consent of such persons to do so should also be necessary. If consent is denied, an intervention by the relevant judicial authority must be required before collection takes place.[87] Thus, even if 'on-the-fly' or 'in-the-wild' biometric identification is technically possible, it should not be allowed to prescind from the individual's consent. This is because consent remains an important part of the legal framework of allowing access to our bodies to others be it in the form of touching, medical procedures or photography. Under this perspective, it seems that, with all its flaws,[88] consent should still be required in our digital age. Indeed, the legal system routinely accepts that consent can be given in situations of uncertainty. For example, we may grant others (e.g., doctors) access to our body, even if we understand that we could not realistically predict any possible future consequence of a medical procedure. Certainly, doctors strive to explain to us the possible risks and share medical information regarding a procedure, but unforeseen and unlikely events can always occur. Yet, we are of the view that people undergo medical procedures having given 'informed consent'. Such fiction is necessary for the medical system to function and provide the care that people need.

In terms of consent to biometric identification, a similar approach should be adopted. Therefore, in cases in which a person needs to undergo biometric identification for a reason justified by the need to protect another competing fundamental right or high-ranked public interest, such as to allow the storing of data of people who have committed certain criminal offences, consent to biometric identification can be considered possible, under the conditions that the security of the stored data is ensured and the uses to which the biometric record can be put, at least as far as predictable, are clearly explained to the individual.

Conclusion

Authors have warned against the danger of humanity slowly sleepwalking into a science-fiction-like society, where unobserved time is minimal, an obscure elite or an artificial intelligence system determine everybody's place in the word according to a pre-ordained system and individuals live in a status of pure conformism, relinquishing all creativity, diversity and the very essence of what makes us humans. Such warning maybe deemed catastrophic; however, biometric technology is being steered and deployed along a similar path.

This paper argued in favour of an interpretation of biometrics that is able to protect and sustain the core needs of all human beings. Such an interpretation must protect people's ability to retain instances in which they are and feel unobserved and their ability to self-represent themselves in all their social relationships. If biometrics needs to bolster such values, rather than undermine them, biometric identification needs to be considered harmful as a general rule, unless an equally fundamental value is able to justify its use. This paper argued that consent shall not be deemed to reach the threshold of a stand-alone justification for biometric identification, unless it is coupled with fundamental values, such as the need to undergo a medical procedure or certain law enforcement purposes.

Raising the collective awareness of citizens of the risks of biometric identification is a crucial task for the sake of the present and all future generations. The law could take the lead and show the way towards a human-centric version of biometric technology.

[87] See CJEU, Case C-205/21, *Criminal proceedings against V.S.*, ECLI:EU:C:2023:49.
[88] Richards " The Pathologies."

Bibliography

Allen, Anita. *Uneasy Access: Privacy for Women in a Free Society*. Totowa: Rowman & Littlefield, 1988.

Alonso-Fernandez, Fernando, Kevin Hernandez-Diaz, Silvia Ramis, Francisco J. Perales, and Bigun, Josef. "Facial Masks and Soft-Biometrics: Leveraging Face Recognition CNNs for Age and Gender Prediction on Mobile Ocular Images." *IET Biometrics* 10, no 5 (2021): 562–580. https://doi.org/10.1049/bme2.12046.

Baghai, Katayoun. "Privacy as a Human Right: A Sociological Theory." *Sociology* 46, no 5 (2012): 951–965. https://doi.org/10.1177/0038038512450804.

Banafshe, Arbab-Zavar, Xingjie Wei, John D. Bustard, and Mark S. Nixon. "On Forensic Use of Biometrics." In *Handbook of Digital Forensics of Multimedia Data and Devices*, edited by Anthony T. S. Ho and Shujun Li, 207–304. Wiley-Blackwell, 2015.

Bertillon, Alphonse. *Identification Anthropométrique: Instructions Signalétiques*. Vol. 1. Impr. administrative, 1893.

Bertillon, Alphonse. *La Photographie Judiciaire: Avec un Appendice sur la Classification et l'Identification Anthropométriques*. Paris: Gauthier-Villars, 1890.

Bilan, Stepan, Mykola Bilan, and Andrii Bilan. "Interactive Biometric Identification System Based on the Keystroke Dynamic." *Biometric Identification Technologies Based on Modern Data Mining Methods* (2021): 39–58. http://dx.doi.org/10.1007/978-3-030-48378-4_3.

Bloustein, Edward J. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser." *New York University Law Review* 39 (1964): 962–1007.

Calo, Ryan. "The Boundaries of Privacy Harm." *Indiana Law Journal* 86, no 3 (2011): 1131–1162

Cheng, Kevin HM, and Ajay Kumar. "Contactless Biometric Identification Using 3D Finger Knuckle Patterns." *IEEE Transactions on Pattern Analysis and Machine Intelligence* 42, no 8 (2019): 1868–1883. https://doi.org/10.1109/TPAMI.2019.2904232.

Cohen, Julie E. "What Privacy is For." *Harvard Law Review* 126, no 7 (2013): 1904–1933.

Custers, Bart, and Gianclaudio Malgieri. "Priceless Data: Why the EU Fundamental Right to Data Protection is at Odds with Trade in Personal Data." *Computer Law and Security Review* 45 (2022): 105683. https://doi.org/10.1016/j.clsr.2022.105683.

DeCew, Judith. "Privacy." In *The Stanford Encyclopedia of Philosophy*, edited Edward N. Zalta, 2018. https://plato.stanford.edu/archives/spr2018/entries/privacy/.

Dvořák, Michal, Martin Drahanský, and Waleed H. Abdulla. "On the Fly Biometric Identification System Using Hand-Geometry." *IET Biometrics* 10, no 3 (2021): 315–325. https://doi.org/10.1049/bme2.12024.

Floridi, Luciano. "On Human Dignity as a Foundation for the Right to Privacy." *Philosophy and Technology* 29 (2016): 307–312. https://doi.org/10.1007/s13347-016-0220-8.

Gavison, Ruth. "Privacy and the Limits of Law." *Yale Law Journal* 89, no 3 (1980): 421–471.

Gerards, Janneke. "How to Improve the Necessity Test of the European Court of Human Rights." *International Journal of Constitutional Law* 11, no 2 (2013): 466–490. https://doi.org/10.1093/icon/mot004.

Gerstein, Robert S. "Intimacy and Privacy." *Ethics* 89, no 1 (1978): 76–81.

Graber, Christoph B. "How the Law Learns in the Digital Society." *Law, Technology and Humans* 3, no 2 (2021): 12-27. https://doi.org/10.5204/lthj.1600.

Gray, David. "Bertillonage in an Age of Surveillance: Fourth Amendment Regulation of Facial Recognition Technologies." *SMU Science and Technology Law Review* 24 (2021): 3–64.

Helfand, J. *Face: A Visual Odyssey* Boston: MIT Press, 2019.

Hughes, Kirsty. "A Behavioural Understanding of Privacy and its Implications for Privacy." *The Modern Law Review* 75, no 5 (2012): 806–836. https://doi.org/10.1111/j.1468-2230.2012.00925.x.

International Organization for Standardization, ISO/IEC 2382-37:2022(en), Information technology — Vocabulary — Part 37: Biometrics 2022, https://www.iso.org/standard/73514.html.

Jaha, Emad Sami and Mark S. Nixon. "Soft Biometrics for Subject Identification Using Clothing Attributes" In *IEEE International Joint Conference on Biometrics* (2014): 1–6. https://doi.org/10.1109/BTAS.2014.6996278.

Kugler, Matthew B. "From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms" *UC Irvine Law Review* 10, no 1 (2019): 107-152.

Lombroso, Cesare. *L'Uomo Delinquente: In Rapporto All'Antropologia, Alla Giurisprudenza ed Alle Discipline Carcerarie*. Vol. 2. Bocca, Milan, 1896.

Micheli-Tzanakou, Evangelia and Plataniotis, Konstantinos "Biometrics: Terms and Definitions." In *HCA Encyclopedia of Cryptography and Security*, edited by Henk C. A. van Tilborg and Sushil Jajodia. Springer New York, NY, 2011.

Moore, Adam D. "Privacy: Its Meaning and Value." *American Philosophical Quarterly* 40, no 3 (2003): 215–227.

Nissenbaum, Helen. "The Meaning of Anonymity in an Information Age" *The Information Society* 15, no 2, (1999): 141–44. https://doi.org/10.1080/019722499128592.

Nisenbaum, Helen. "How Computer Systems Embody Values." *Computer* 34, no 3 (2001): 120-119.

Osorio-Roig, Dailé, Christian Rathgeb, Pawel Drozdowski, Philipp Terhörst, Vitomir Štruc, and Christoph Busch. "An Attack on Facial Soft-Biometric Privacy Enhancement." *IEEE Transactions on Biometrics, Behavior, and Identity Science* 4, no 2 (2022): 263–275. https://doi.org/10.1109/TBIOM.2022.3172724.
Purtova, Nadezhda. "From Knowing by Name to Targeting: The Meaning of Identification under the GDPR." *International Data Privacy Law* 12, no 3 (2022): 163–183. https://doi.org/10.1093/idpl/ipac013.
Rachels, James. "Why Privacy is Important." *Philosophy and Public Affairs* 4, no 4 (1975): 323–333.
Raposo, Vera Lúcia. "(Do Not) Remember My Face: Uses of Facial Recognition Technology in Light of the General Data Protection Regulation." *Information and Communications Technology Law* 32, no 1 (2022): 45-63. https://doi.org/10.1080/13600834.2022.2054076.
Reid, Daniel A., Mark S. Nixon, and Sarah V. Stevenage. "Soft Biometrics; Human Identification Using Comparative Descriptions." *IEEE Transactions on Pattern Analysis and Machine Intelligence* 36, no 6 (2013): 1216–1228. https://doi.org/10.1109/TPAMI.2013.219.
Renieris, Elizabeth M. *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse*. MIT Press, Boston, 2023.
Richards, Neil, and Woodrow Hartzog. "The Pathologies of Digital Consent." *Washington University Law Review*. 96 (2018): 1461–1503.
Roxo, Tiago, and Hugo Proença. "Is Gender 'In-the-Wild' Inference Really a Solved Problem?" *IEEE Transactions on Biometrics, Behavior, and Identity Science* 3, no 4 (2021): 573–582. https://doi.org/10.1109/TBIOM.2021.3100926.
Selinger, Evan, and Woodrow Hartzog. "The Inconsentability of Facial Surveillance." *Loyola Law Review* 66, no 1 (2020): 33–54.
Solove, Daniel J. "A Taxonomy of Privacy, 154 U." *University of Pennsylvania Law Review* 477 (2006): 487–88.
Solove, Daniel J., and Danielle Keats Citron. "Risk and Anxiety: A Theory of Data-Breach Harms." *Texas Law Review* 96 (2017): 737–786.
Solove, Daniel J. "Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data (January 11, 2023). 118 *Northwestern University Law Review*, Forthcoming. http://dx.doi.org/10.2139/ssrn.4322198
Schwartz, Barry. "The Social Psychology of Privacy." *American Journal of Sociology* 73, no 6 (1968): 741–752. https://psycnet.apa.org/doi/10.1086/224567
Terhörst, Philipp, Daniel Fährmann, Naser Damer, Florian Kirchbuchner, and Arjan Kuijper. "On Soft-Biometric Information Stored in Biometric Face Embeddings." In *IEEE Transactions on Biometrics, Behavior, and Identity Science* 3, no 4 (2021): 519–534. https://doi.org/10.1109/TBIOM.2021.3093920.
Warren, Samuel and Brandeis, Louis. "The Right to Privacy." *Harvard Law Review* (1890): 193–220.
Whitman, James Q. "The Two Western Cultures of Privacy: Dignity Versus Liberty." *Yale Law Journal* (2004): 1151–1221.

Primary Sources

International Conventions

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, 28.01.1981)
European Convention of Human Rights (ECHR)

Decisions of the ECtHR

Amann v Switzerland [GC], no. 27798/95, § 65, ECHR 2000-II
Axel Springer AG v Germany [GC] no. 39954/08, § 83, ECHR 227
Couderc and Hachette Filipacchi Associés v France 42811/06 [2012] ECHR 1790
Couderc and Hachette Filipacchi Associés v France [GC], no. 40454/07, ECHR 2015
Gaughran v United Kingdom [2020] ECHR 144
Leander v Sweden [1987] Eur Court HR (Ser A) no. 116
Markt Intern Verlag GmbH and Beermann v Germany [1990] Eur Court HR (Ser A) no. 165
Melike v Turquie, no. 35786/19, 15 June 2021
Müller and Ors v Switzerland [1988] Eur Court HR (Ser A) no. 133
S. and Marper v the United Kingdom, [2008] ECHR 1581
Sağdiç v Turkey, 9142/16, [**2021**] ECHR 048

Smirnova v Russia [2003] ECHR 2003-IX
Stevens v the United Kingdom, no. 11674/85, Commission decision of 3 March 1986, DR 46
Ulusoy and Others v Turkey, no. 42571/98, ECHR 2005-VIII
Vajnai v Hungary, no.33629/06, § 57, ECHR 2008
Verlagsgruppe News GmbH v Austria (no. 2) [1990] Eur Court HR (Ser A) no.165

Von Hannover v Germany [2004] Eur Court HR IV 96
X and Y v the Netherlands [1985] Eur Court HR (ser A) no. 91

Decisions of the Court of Justice of the EU (CJEU)
Case C-205/21, *Criminal proceedings against V.S.*, ECLI:EU:C:2023:49

National Legislation
Illinois Biometric Information Privacy Act (BIPA) of 2008, 740 ILCS 14
EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

Decisions of National Courts
Rosenbach v Six Flags Entertainment Corp., 2019 IL 123186
Cour de cassation, Civ. 1, 20 octobre 2021, 20-16.343, Inédit.