Information Polity 27 (2022) 193–217
DOI 10.3233/IP-211525
IOS Press

Visual and biometric surveillance in the EU. Saying ‘no’ to mass surveillance practices?[1,2]

Paul De Hert[a,b,*] and Georgios Bouchagiar[c,d]
[a] *Law Science Technology and Society, Vrije Universiteit Brussel, Belgium*
[b] *Department of Law, Technology, Markets, and Society, Tilburg Law School, The Netherlands*
[c] *Doctoral Researcher in Criminal Law and Technology, Faculty of Law, Economics and Finance, University of Luxembourg, Luxembourg*
[d] *Law, Science, Technology and Society, Free University of Brussels, Belgium*

Abstract. Earlier this year, the European Commission (EC) registered the ‘Civil society initiative for a ban on biometric mass surveillance practices’, a European Citizens’ Initiative. Citizens are thus given the opportunity to authorize the EC to suggest the adoption of legislative instruments to permanently ban biometric mass surveillance practices. This contribution finds the above initiative particularly promising, as part of a new development of bans in the European Union (EU). It analyses the EU’s approach to facial, visual and biometric surveillance,[3] with the objective of submitting some ideas that the European legislator could consider when strictly regulating such practices.

Keywords: Face recognition, visual data, biometric data, surveillance

Key points for practitioners:

- The US are clever in being honestly prohibitive. They see bad things that may happen; and they say with clarity ‘no’ to technologies, whose use can be dangerous and harmful in specific high-risk areas. This is the case with neither the GDPR nor the LED; these laws probably fail to detect ‘bad’ uses of technologies that should be prohibited and to distinguish them from others.
- The US moratorium-approach seems extremely promising. When Americans find a technology(aspect) unsafe or particularly intrusive, they prohibit any implementations to protect the data subject either until there is the infrastructure to accurately assess safety of the technology or until concrete laws are introduced to minimise risk and dangerousness. Laws that push the pause-button, to our knowledge, are nowhere to be found in Europe.
- Under the EU framework, everything is ‘done’ by using ‘data protection law’, an area of law that focuses heavily on processes and procedure, but misses substance and clear outcomes; or what we have addressed elsewhere as bright-line rules. But people want clear rules speaking to them comprehensively. This seems to be the case with the US. They do not see ‘data protection law’ everywhere. Rather when solving things by regulation, they take items from other (legal) fields, such as criminal law’s ‘probable cause’, ‘confidentiality’ known from commercial or professional contexts, industry-related ‘standards of care’ or market-related prohibitions.

[1] The authors would like to thank Stephanie Rossello for her constructive criticism on this paper.

[2] This article received a correction notice (Erratum) post publication with DOI 10.3233/IP-229012, available at http://doi.org/10.3233/IP-229012.

[*] Corresponding author: Paul De Hert, Law Science Technology and Society, Vrije Universiteit Brussel, Belgium. Tel.: +32 2 629 24 60; E-mails: paul.de.hert@vub.be and paul.de.hert@tilburguniversity.edu.

[3] For the purposes of this paper, we address ‘facial, visual and biometric data’ as information relating to characteristics of a natural person that can be captured by surveillance technologies and that can uniquely identify that person.

1570-1255 © 2022 – The authors. Published by IOS Press. This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial License (CC BY-NC 4.0).

1. Introduction: Europe wants to say ‘no’ but does not know how

On 7 January 2021, the EC registered the European Citizens’ Initiative (ECI) under the title ‘Civil society initiative for a ban on biometric mass surveillance practices’ (European Commission, 2021a).[4] Provided the organizers of the Initiative manage to collect enough supporting signatures, the EC may accept or reject the organizers’ call (European Commission, 2021a). The latter hold that indiscriminate and arbitrarily targeted uses of biometric technologies have led to mass surveillance that can seriously violate a wide array of fundamental rights and freedoms; they, thus, call the EC to propose strict regulation to ban such biometric implementations (ECI, 2021).

Biometric and visual surveillance technologies have been taking a greater place in everyday life. After initial implementations in workplaces (Maple & Norrington, 2006), schools (Hope, 2015) or nightclubs (Zhang, 2002, Chapter 2, p. 30), today’s biometrics are embedded within numerous devices, ranging from personal smartphones and laptops to police-worn cameras and other tools used by public actors. Contemporary technologies became ubiquitous and allow for new trends, such as state surveillance, authentication for physical and virtual access, as well as online or face-to-face payment (Ogbanufe & Kim, 2018; Setsaas, 2019). Biometrics play a key role in the evolution of video surveillance systems towards intelligent video analysis. This development towards biometric enhanced video surveillance (such as facial recognition systems) combined with algorithms raises particular concerns about stigmatization and discrimination, as well as risks to privacy and the protection of personal data, because of the very special nature of biometrics (EDPB, 2020).

Such risks can be materialised in various areas and situations. To name but a few: when used by the police, surveillance technologies can result in discriminatory policing, whose biases can outweigh any potential benefits (Berk, 2019); when deployed by Internet giants, such technologies may lead to deceptive practices or monitoring experiments (Van Eijk et al., 2017; O’Hara, 2015); when applied to schools, surveillance systems can watch the children’s behaviour (Hope, 2015). In the era of ‘just-in-case, watch everything’ and ‘more data is better’ (Walsh et al., 2017), when even intelligent dolls may be used for monitoring (Keymolen & Van Der Hof, 2019), people are becoming particularly vulnerable.

While the engagement in surveillance practices is, in general, an old subject of legal, political, sociological or philosophical discussions (Bennett, 2008; Shroff & Fordham, 2010; Webster, 2012; Bannister, 2005; Musik, 2011; Brayne, 2020) at both EU (Wright & Kreissl, 2015) and state level (Clavell et al., 2012; Fussey, 2012; Clavell, 2011; Bjorklund, 2011; Fonio, 2011; Svenonius, 2012; Heilmann, 2011), the situation becomes acute, in an era when the biometrics-market is growing fast pushed by the covid-pandemic (AlgorithmWatch & Bertelsmann Stiftung, 2020, p. 14).[5]

This contribution analyses the EU regulatory approach to facial, visual and biometric surveillance. More precisely, it addresses the EU legal regime, as framed under the General Data Protection Regulation (the ‘GDPR’; European Parliament & Council, 2016a) and the Data Protection Directive for Law Enforcement and Criminal Justice Authorities (the ‘LED’ or ‘Law Enforcement Directive’; European Parliament &

[4] Introduced by the Lisbon Treaty, the ECI is an ‘agenda-setting’ instrument for citizens. It is registered as admissible by the EC, when it does not manifestly fall outside the EC’s authority, it is not ‘manifestly abusive, frivolous or vexatious’ and it is ‘not manifestly contrary to the values’ of the EU. After registration, one million citizens from at least one quarter of Member States can call the EC to propose legislation in relevant areas. In this case, the ‘Civil society initiative for a ban on biometric mass surveillance practices’ was registered as admissible.

[5] This market-expansion *might* surprise, given the growing rate of false positives/negatives resulting from mask-wearing measures; but it also *does not* surprise: biometric-related technologies, aimed at preventing the spread of the virus, have been broadly implemented around the globe with few (if any) meaningful checks and balances.

Council, 2016b).[6] The overarching narrative is simple: the EU has failed to say a clear 'no' to certain surveillance practices that may have a particularly hostile impact on fundamental human rights and freedoms; in light of the EC's initiative, it is argued that some banning-techniques could assist the EU legislator in introducing bright-line prohibitions on certain technological uses.

More concretely, our analysis of the GDPR and the Law Enforcement Directive will show that their applicability is loaded with vagueness. On top of vagueness, we find state friendly exceptions and rules and little or no substantive hurdles to address concrete surveillance technologies. To defend the claim that substantive hurdles to surveillance are needed, we will highlight a series of elements (to us, absent in the EU legal framework) that could be considered by the EC when strictly regulating mass surveillance practices: concreteness and precision, bright-line bans and practical remedies.

Although there is literature on the need for bans in the EU, there are few (if any) studies on the way in which concrete prohibitions could be imposed. Our paper contributes to thus far debates by submitting a new paradigm for introducing desirable bans:

- first, the EU privacy/data protection framework, currently permissive, could become honestly prohibitive regarding technologies whose use may be particularly harmful or dangerous;
- second, certain techniques, like moratoria prohibiting certain technological uses until proven safe, could be adopted at EU level;
- third, the EU's approach to data protection, currently highly process- and procedure-based, could combine different elements known from other fields (like criminal law or the market sector) that can make applicable rules more comprehensively applied.

The discussion proceeds as follows. Section 2 analyses the EU's applicable data protection-instruments: the GDPR and the Law Enforcement Directive. Its goal is to stress uncertainty, stemming from the EU's abstract approach: that is, a permissive system not sufficiently regulating technological implementations. To highlight the EU's inefficiencies, we refer to concrete examples: the processing of sensitive data; and the use of drones and dash cams. Thereafter, Section 3 aims to detect vagueness in particular relation to biometric data: the processing is, here, 'prohibited'; albeit, a long list of exceptions makes the prohibition quite illusionary. Given these insufficiencies, Section 4 suggests a dynamic interpretation of Article 9(4) of the GDPR as an open call toward domestic regulators to introduce limitations on biometric processing. Then, Section 5 critically addresses the LED as, first, a police-friendly legal instrument and, second, an unjustifiably permissive tool regarding the processing of sensitive data, including biometrics. Moreover, two cases are discussed to stress the ubiquitous application of EU data protection laws (Section 6 on *Clearview*), as well as the broad discretion enjoyed by law enforcement in deploying technologies to process biometrics (Section 7 on *Bridges*). Furthermore, Section 8 analyses the EU framework in more detail to make the argument for the need for concrete rules and bans, currently absent in Europe. This need is more analytically tackled in Section 9 that recommends: concreteness, precision, bright-line bans and effective remedies. Last, Section 10 draws conclusions and makes some remarks, in light of latest trends in the EU.

2. GDPR and LED's key notions ('processing personal data') and surveillance technology

The GDPR was introduced together in the European Union with the Law Enforcement Directive (LED) to reform the legal regime established by the 1995 Data Protection Directive (European Parliament & Council, 1995) and the 2008 Framework Decision respectively (Council of the European Union, 2008).

[6] Now and then, we will also refer to the data protection rules of the Council of Europe as contained in Convention 108.

The person whose data are processed ('the data subject') has rights towards those that collect and process their data ('the controllers'),[7] has a right to an effective judicial remedy and to receive compensation (GDPR, art. 78–82). More important is the right (free of cost) to lodge a complaint with the supervisory authority (GDPR, art. 77). The GDPR provides for civil/administrative measures to tackle data breaches and other infringements on the data protection rules. Criminal sanctions can be introduced under the GDPR, if EU Member States consider this is useful, but only regarding special situations, such as severe breaches of the GDPR (GDPR, recital 152; Wright & De Hert, 2016, Chapter 16). Data protection law is applicable to all sectors of society, but not to the processing of personal data "by a natural person in the course of a purely personal or household activity" (Article 2(2)(c) GDPR).

Key notions in both the GDPR and the LED are 'personal data' and 'processing'. Pursuing the objective of technological neutrality, these texts do not pay any specific attention to individual technologies (like biometrics, drones, RFID and so forth), but define rules and principles applicable to whatever activity (via technology) that *processes* personal data. So, technologies fall under data protection law when they *process personal data*. In the area of surveillance, this is often the case. The concept of *processing* is therefore very powerful in the sense that it applies easily. The same goes for the term *personal data*. Whenever data identify or can identify individuals, they *are* personal data. This could be just about everything (from written text, numbers, sounds, odours to DNA). This equally applies to the collection of visual data: both the GDPR and the LED apply to the taking of images and the use of video surveillance systems, because filming is equal to 'processing personal data', granted that persons *are* filmed.[8]

There is not much really prohibited in the GDPR and the LED. As a rule, all activities are allowed when those setting up the technologies ('data controllers') abide to the general rules and principles (like lawfulness, necessity, proportionality and data minimization).[9] There is a stricter and more prohibitive regime for certain sensitive categories of data in Article 9(1) GDPR ('Processing of special categories of personal data').[10] But to illustrate the manageability of data protection law one only needs to turn to Article 9(2) GDPR where no less than ten broad exceptions are tabled that allow to process sensitive data.

[7] Under the EU legal framework, the citizen ('data subject') enjoys several individual rights: to information (GDPR, art. 13–14; LED, art. 13); to access her data (GDPR, art. 15; LED, art. 14–15); to rectification (regarding inaccurate data; GDPR, art. 16; LED, art. 16); to erasure of her data (GDPR, art. 17; LED, art. 16); to restrict processing (GDPR, art. 18; LED, art. 16); to data portability (GDPR, art. 20); to object to processing (GDPR, art. 21); or not to be subjected to automated decision-making. The right of the data subjects not to be subjected to automated decision-making is treated as a general prohibition; a duty of the controller who must abstain from subjecting individuals to decisions that are based solely on automated processing and that can significantly affect them. GDPR, art. 22.

[8] However, the Regulation does not apply to processing of data that has no reference to a person, e.g. if an individual cannot be identified, directly or indirectly (EDPB, Guidelines 3/2019 on processing of personal data through video devices, 7). The EDBP Guidelines give three examples. Example 1: The GDPR is not applicable for fake cameras (i.e. any camera that is not functioning as a camera and thereby is not processing any personal data). However, in some Member States it might be subject to other legislation. Example 2: Recordings from a high altitude only fall under the scope of the GDPR if under the circumstances the data processed can be related to a specific person. Example 3: A video camera is integrated in a car for providing parking assistance. If the camera is constructed or adjusted in such a way that it does not collect any information relating to a natural person (such as licence plates or information which could identify passers-by) the GDPR does not apply.

[9] Those that process citizens' data ('data controllers') must comply with general data protection principles, namely lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity/confidentiality and accountability (GDPR, art. 5). Several duties, including the obligation to conduct impact assessments, are imposed to safeguard compliance with these principles. For a more detailed analysis, see European Union Agency for Fundamental Rights and Council of Europe (2018, pp. 139–186).

[10] Art. 9(1) GDPR in principle prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. See also Article 10 of the LED.

If one looks closer at the text of the GDPR, there are indirect hints to certain technologies and also to technologies that help filming and picture-taking. Article 35(3)(c), for instance, requires the carrying out of a data protection impact assessment in case of systematic monitoring of publicly accessible areas on a large scale; and Article 37(1)(b) requires processors to designate a data protection officer, if the processing operation by its nature entails regular and systematic monitoring of data subjects.

Overall, the treatment of technologies capturing images in EU data protection law is sloppy, unsystematic and kept vague to avoid legal controversies. The soft law guidance offered by data protection authorities in Member States and by the European Data Protection Board (EDBP) is hardly any better. The result is a permissive system of rules and principles that in practice hardly impedes the out roll of these visual surveillance technologies. Two examples could support this argument:

> *Example 1:* The GDPR and the LED do not pay specific attention to the processing of visual data (contrary to their treatment of 'biometric data' (see *below*)). Apart from the more principled questions ('is CCTV not serious enough a threat to privacy to consider it more in detail?'), this raises all sorts of legal/technical questions, for instance, should visual data of persons be regarded as sensitive data because they always reveal something about skin colour and very often something about race or origins? Accepting that all pictures of persons reveal data about their skin colour, origins or ethnicity would put a serious filter of prohibition on the use of cameras and video surveillance technologies; albeit, this deduction is avoided by all legal (interpretative) authorities in Europe that seem to hesitate to initiate a discussion on people's growing addiction to the use and collection of visual data. At best when the issue is addressed, like in the guidelines of the EDPB, one may find rather weak arguments about the application of the household exception (processing data for strictly private purposes is exempt from the GDPR) and about intentionally or not capturing images to collect data on ethnicity.[11]
>
> *Example 2:* The GDPR and the LED do not pay specific attention to surveillance technologies. There is, for instance, nothing in it on drones and dash cams. The matter is simply referred to by interpretation and soft law guidance by the data protection authorities or the European Data Protection Board. Reading their interpretative work is hardly satisfactory (EDPB, 2020, p. 12). Never are citizens told that these technologies in the hands of private persons are prohibited; never are data subjects explained how to exercise their rights if they are not even aware of the way in which these technologies are used to capture their data. How can legal (interpretative) authorities, like data protection authorities, assume that these technologies are GDPR-compliant if it is impossible for data subjects to check compliance and if by the sheer nature of their application (without consent) compliance is highly unlikely. In the field, the result is one of uncertainty and contradictions (Štitilis & Laurinaitis, 2016): some European data protection authorities in their respective legal systems say 'yes' to dashboard cameras, others say 'no' but are not followed by their citizens and the EDPB avoids harmonizing; and, by doing that, it joins the first permissive interpretation.

[11] Compare the 'howevers' in EDPB (2019, p. 17). The Council of Europe (see further in the text) does not do better. In the recitals of the GDPR, there is another, probably not sufficiently substantiated, argument that makes use of the sophisticated definition of biometric data (that will be discussed *below*). In a nutshell, the base line argument is that a regular photograph that is taken does not amount to this sophisticated definition of processing of biometric data and is, hence, not 'sensitive data' (GDPR, recital 51); this argument is echoed by the Council of Europe in its Explanatory Report to the Convention 108+ (Council of Europe, 2018b, points 58–60). The argument is not convincing, because there are many categories of sensitive data – biometric data being only one of them – and all kinds of sensitive data can be implied from one simple photograph.

3. The GDPR on biometric data (surveillance): Clarity combined with vagueness

The regulatory attention to biometrics in European data protection law fares better. By their nature, biometrics allow to identify persons, so there appears to be no vagueness here: data protection law applies. However, complexities arise when trying to comprehend how European data protection law applies more concretely to biometrics. Needed are 'personal data' and 'processing activities'. Both the GDPR and the LED define biometric data and explain when these data are 'personal data' in the sense of data protection law: '*personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*' (GDPR, art. 4(14); LED, art. 3(13)).[12]

Therefore, facial data are explicitly mentioned in data protection law, but only in the context of biometric data.

It follows from this definition that the GDPR and the LED cover biometric data types, like facial images or fingerprints, when the processing of these data meets three cumulative pre-requisites (Kindt, 2018, pp. 529–531). *First*, this processing activity must be technology-based ('specific technical'; EDPB, 2019, paragraph 75; GDPR, recital 51; Jasserand-Breeman, 2019, pp. 66–68; Kindt, 2018, pp. 529–531; Jasserand, 2016, p. 303; Blair & Campbell, 2018). *Second*, the data must reveal ('relate to') physical, physiological or behavioral traits.[13] *Third*, personal data must 'allow or confirm the unique identification' of an individual.

The GDPR adds to this Article 4 GDPR-definition a somewhat strange sequel in Article 9. This provision on 'special' sensitive data, discussed in the preceding section,[14] identifies biometric data as one of the categories of sensitive data but, strikingly, deviates slightly from the definitional terms of Article 4 GDPR. Whereas the definition of biometric data refers to personal data that '*allow or confirm* the unique identification' of an individual, Article 9 GDPR sets apart biometric data as a special sensitive category of personal data 'when the purpose of processing this data is to uniquely identify a natural person' (GDPR, article 9(1); LED, article 10).[15] Present in both provisions is the idea of *allowing unique identification*, but missing in the second provision is the idea of *confirming unique identification*.

With 'unique identification' central to both provisions, it can be argued that biometric data are almost always a special category of personal data. In this context, any processing operation aimed at, for example, authenticating identity or drawing inferences on natural persons can fall under the prohibition of article 9 GDPR (ICO, n.d.). However, a strict reading of articles 4 and 9 GDPR does not exclude that some biometric data are 'ordinary' personal data, not sensitive data. The UK data protection authority, the ICO, rightly mentions the possibility, without however giving examples. We quote the relevant ICO passage

[12] The term 'dactyloscopic' data refers to fingerprint data. See ICO (n.d.).

[13] Faceprints and similar characteristics can qualify as physical or physiological traits; whereas the voice, the signature or the way one uses her keyboard, walks or sleeps can be classified as behavioural traits. See Kindt (2013, pp. 23–32). Thus, identification techniques may vary from face recognition, fingerprint verification or iris scanning (physical/physiological traits) to the processing of keystrokes or signatures (behavioural traits). See ICO (n.d.).

[14] We briefly discussed *above* the data protection distinction between ordinary personal (as we would like to call it) and more risky, special personal data. Following a risk-based approach, art. 9 GDPR groups the latter and as a rule prohibits their processing. More concretely, the GDPR presumes that such a special type of data merits a special type of protection – because its processing appears more likely to violate human rights. See ICO (n.d.). With regard to the risk-based approach of the GDPR, see Lynskey (2015, pp. 8–9).

[15] As the EDPB explains, if the goal is not to single out and uniquely identify a natural person, but to distinguish between groups, then data involved are not falling under the special category-provision of art. 9 GDPR. EDPB (2019, paragraph 79); Kindt (2018, p. 531).

in full, because it is illustrative for the more general narrative of this contribution: it nicely identifies a broad range of biometrics and clarifies the distinction between the processing of pictures/photos and the processing of biometric data:

ICO, 'What is special category data?', 5.

Examples of physical or physiological biometric identification techniques:

- facial recognition;
- fingerprint verification;
- iris scanning;
- retinal analysis;
- voice recognition; and
- ear shape recognition.

Examples of behavioral biometric identification techniques:

- keystroke analysis;
- handwritten signature analysis;
- gait analysis; and
- gaze analysis (eye tracking).

If you process digital photographs of individuals, this is not automatically biometric data even if you use it for identification purposes. Although a digital image may allow for identification using physical characteristics, it only becomes biometric data if you carry out "specific technical processing". Usually this involves using the image data to create an individual digital template or profile, which in turn you use for automated image matching and identification.

All biometric data is personal data, as it allows or confirms the identification of an individual. Biometric data is also special category data whenever you process it "for the purpose of uniquely identifying a natural person".

This means that biometric data will be special category data in the vast majority of cases. If you use biometrics to learn something about an individual, authenticate their identity, control their access, make a decision about them, or treat them differently in any way, you need to comply with art. 9.

In its Guidelines, the EDBP does not elaborate on this theoretical possibility of a category of 'ordinary' biometric personal data (as opposed to the art. 9-sensitive biometric data); albeit, it does give an example (in our view quite dubious)[16] of a shop owner that films its customers to know their gender or age, but not to identify them.[17]

Aside from these EU legal technicalities, it is learnt that *in most cases* biometric data processing is 'special' and restricted in the sense of article 9 GDPR. This also resonates with the 'other' European text on data protection, as developed by the Council of Europe, the Convention 108+ (Council of Europe, 2018a).[18]

[16] The example raises our eyebrows and contributes to a feeling that citizens should get 'over it' and accept filming for all kinds of purposes.

[17] EDPB, Guidelines 3/2019 on processing of personal data through video devices, 19: "However, when the purpose of the processing is for example to distinguish one category of people from another but not to uniquely identify anyone the processing does not fall under art. 9. Example: A shop owner would like to customize its advertisement based on gender and age characteristics of the customer captured by a video surveillance system. If that system does not generate biometric templates in order to uniquely identify persons but instead just detects those physical characteristics in order to classify the person then the processing would not fall under art. 9 (as long as no other types of special categories of data are being processed). However, art. 9 applies if the controller stores biometric data (most commonly through templates that are created by the extraction of key features from the raw form of biometric data (e.g. facial measurements from an image)) in order to uniquely identify a person".

[18] In 2018, two years after the adoption of the GDPR, the Convention 108 was modernised to address personal data-related challenges emerging from more recent technological developments, as well as to enhance its follow-up mechanism (a critical discussion in: De Hert & Papakonstantinou, 2014). The final outcome of the reform, Convention 108+, organizes processing of personal data in general, without containing more specific rules for technologies or data. Like the GDPR, it addresses 'biometric data uniquely identifying a person' as a special category of data (Convention 108+, art. 6). Under point 58 of the Explanatory Report to the Convention 108+, 'processing of biometric data, that is data resulting from a specific technical processing of data

But where does this finding bring us? A closer look at the article 9 GDPR-prohibition reveals no absolute restriction. The provision suggests a prohibition on the processing of sensitive data, but then allows to bypass the prohibition by requiring explicit consent from the individual (article 9(2)(a)),[19] or, among others, when the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (article 9(2)(g)). Interesting for our purpose is the fourth paragraph of article 9 GDPR:

> **Art. 9(4) GDPR**
> *Member States can maintain or introduce further conditions, including limitations with regard to the processing of genetic data, biometric data or data concerning health.*

4. Art. 9(4) GDPR: allowing domestic laws and bans on biometric data processing

In the past, we have defended the regulatory option that we find in article 9(4) GDPR-creating additional legislation on the specific technology of biometrics (De Hert, 2005; also Alterman, 2003; Campisi, 2013, Chapter 15). Member States should go beyond the GDPR and use this paragraph in article 9 GDPR to introduce restrictive laws on biometrics. Biometric data are the most unique data that data subjects have as individuals. Fraud with raw biometric data is, for example, critical, since one cannot change or fall back on alternative biometric data. A closer look at biometric technologies reveals a wealth of possible policy choices for an Enlighted regulator. In a 2005 study on biometrics, a series of possible clarifications, additional rights and prohibitions were identified to embed biometrics within a foreseeable human rights-friendly framework that recognizes as a starting point a right to biometric anonymity, enhances consumer law with consumer protective ideas for private uses of biometric systems (e.g. consent can never be given immediately at the spot, but is only acceptable after a week of reflection), enriches evidence law with prohibitions to use biometric data in court and regulates the use of these technologies with specific ‘no-go’s’.[20]

concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual, is also considered sensitive when it is precisely used to uniquely identify the data subject’. Again, and like the EU texts, it can be assumed that there is in the eyes of the authors of the Convention on the one hand sensitive biometric data (used to identify) and on the other hand normal biometric data (not meant to identify). Only the former is considered sensitive, but there is less vagueness about this category as compared with the GDPR that uses different terminology in art. 4 and art. 9 GDPR (see *above*). Compare Explanatory Report to the Convention 108+, points 58–60 and, in particular, point 59 mentioning that ‘(. . .) (t)he processing of images will not generally involve processing of sensitive data as the images will only be covered by the definition of biometric data when being processed through a specific technical mean(s) which permits the unique identification or authentication of an individual (. . .)’. Repurposing of the processing that was initially not targeted at unique identification could easily transform normal biometric data into sensitive biometric data. This could, for example, occur, if the controller using a particular technical means directed its technology toward unique identification.

[19] Consent is defined as ‘any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’ (GDPR, art. 4(11)).

[20] Such prohibitions on possible uses, e.g. for ordinary financial transactions (as opposed to, say, access to ATM machines), for social benefits or employment, or for potentially dangerous uses such as ‘keyless entry’ into hotel rooms; prohibitions on multi-model biometrics; prohibitions on central storing of biometrics; prohibitions on storing ‘raw images’; prohibitions on using financial rewards to promote participation in biometric identification programs; prohibitions on non-encrypted processing and transmitting of biometric data; prohibitions on biometric technology that generates sensible data when alternatives exit; incriminations for theft and unauthorised use of biometric data.

The foregoing shows that only general data protection will not do (good) and that satisfactory regulation of technologies requires a broader pallet of legal techniques in addition to the GDPR tools and in particular bright line rules that are technology-specific and take into account the properties of biometric practices.[21] Both the EU with the GDPR and the Council of Europe with the Modernized Convention 108+ have ignored this message, although the reports that prepared the ground for reform of the Convention 108+ had called for biometric-specific rule-making (Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2005; Parliamentary Assembly of the Council of Europe, 2011).

The data protection authorities in Europe – always strong defenders of technology neutral data protection rules – are aware of the dangers associated with biometrics and the need for specific rules, a need they try to address with soft law guidance. The EDPB (2019; 2020) in its *Guidelines* has inserted a noteworthy paragraph '*Suggested measures to minimize the risks when processing biometric data*' with clear rules on how to apply biometric technologies that move into the direction of the set of bright line rules enumerated *above*: a suggestion to avoid further use; ownership of the data through decentralization rather than central storage; a distinction between templates and raw data, with as a rule the prohibition of minimization of the use of the latter. Article 9(4) GDPR (discussed *above*) should therefore be read as an open invitation to national regulators 'to introduce further conditions, including limitations' on biometric processing.

5. The 2016 Law Enforcement Directive: State and surveillance friendly

The GDPR was introduced in 2016 together with the Law Enforcement Directive. Textual analysis of both documents reveals a government-friendly attitude. Both lay the foundations for state friendly legal ecosystems. The GDPR does this in a general way for all public authorities, whereas the LED only focusses on law enforcement authorities.

- The GDPR contains countless exceptions to its rules and principles, by allowing Member States to vote laws to exempt themselves to a fare-going degree from these rules and principles (Hildén, 2019, pp. 180, 187). It also makes sharing of data with law enforcement authorities very flexible. All possible data collected under the GDPR can easily be disclosed to law enforcement agencies based on article 6(1)(c) GDPR that justifies these kinds of transfers and disclosures 'for compliance with a legal obligation to which the controller is subject' (EDPB, 2020, p. 15).
- The Law Enforcement Directive 'serves' law-enforcement authorities[22] with specific data protection rules and is clearly a result of compromise, even more so than the GDPR. Big data policing, predictive

[21] Consumer rights are, for instance, often better enforced and recognized than data protection rules. Consumer law is also an ideal instrument to discourage voluntary biometric schemes, since voluntary schemes have a funny way of turning into compulsory ones in all but name. Consumer law can make it clear that anyone who is asked to voluntarily submit biometric identifiers should be fully informed of the potential risks; competent to understand the impact of their actions; and under no threat of harm to agree to such an action. Harm should be interpreted very broadly here, to include such things as the inconvenience of having to wait in a much longer line. To inhibit pressured or hasty decision-making a waiting period between application and recording of biometric ID's should be required. This also serves to encourage serious deliberation, and also partially offsets the public tendency to assume that any commercial technology that is permitted by law must not pose a serious risk to a person. Some of these consumer law ideas and ideas taken from other legal areas can be introduced in data protection acts. The Belgian data protection Act contains interesting rules about the reversal of burden of proof and incepts a swift civil law procedure allowing the data subject to obtain judicial review within very short time delays.

[22] The Directive targets public authorities and private entities performing public functions, related to the 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' (LED, art. 3(7)). In this context, the LED can cover data processing at EU and

> policing and other possible police models for the twenty first century – all requiring processing of vast amounts of data – are not mentioned as such, but are clearly not rejected if one adds up the small concessions to pragmatism in the Law Enforcement Directive: the principle of transparency is simply not included among the list of basic principles governing data processing (LED, art. 4(1)(a)); other principles, such as data minimization and purpose limitation, are phrased in more flexible terms (LED, art. 4(1)(b–c)); there are limitations to data subjects' rights (European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 282–286); there is vagueness about the legal grounds for law enforcement data processing and its justification; and there seem to be pragmatic lenient rules on the processing of sensitive data. Let us take a closer look at these two last points (on legality-vagueness and on pragmatic acceptance of sensitive data processing).

Firstly, there is pragmatism in the Law Enforcement Directive about the legality requirements for police-data processing. The Law Enforcement Directive does not expressly specify what kind of legal basis is needed for law enforcement authorities to process data. This Directive applies to 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'. These are all considered valid and justified purposes. The Law Enforcement Directive does not go into more detail (for instance is 'prevention' as important as 'prosecution' and 'where does prevention stop?').

For all these purposes a legal basis is required (article 8(1)) that at least identifies the objectives of the processing, the personal data to be processed and the purposes of the processing (article 8(2); see also recital 33). However, this legal basis does not necessarily require a legislative act adopted by a national parliament. It can be something else or hierarchically 'lower'; but this, only if domestic law allows this ('without prejudice to requirements pursuant to the constitutional order of the Member State concerned'; recital 33).[23]

Secondly, there is Law Enforcement Directive-pragmatism about sensitive data and policing. European data protection is very firm about the riskfulness of the processing of certain data-categories. Like the GDPR in article 9 (*above*), the Law Enforcement Directive recognizes these special categories of personal data (article 10). The Law Enforcement Directive-list is identical with the GDPR-list, including 'biometric data for the purpose of uniquely identifying a natural person'. However, the similarities halt there. Contrary to the GDPR (biometric processing for the purpose of unique identification is prohibited, albeit with a long list of exceptions), the Law Enforcement Directive stipulates that such a processing 'shall be allowed' where certain stringent requirements are met: 1) strict necessity of processing, 2) appropriate safeguards and 3) where authorized by Union or Member State law *or* when the processing is necessary to protect the vital interests of the data subject or of another person *or* the processing relates to data which are manifestly made public by the data subject (LED, article 10).

domestic level, including data storage on national databases or relevant processing operations performed by national forces. Contrary to the GDPR (directly applicable to and binding Member States without the need for transposition), the LED requires incorporation into domestic law. The vast majority of the EU Member States today have transposed it. The exception is Denmark (European Union, n.d.). Despite different national traditions and cultures, not much disharmony is expected, in light of the adoption by the LED of the GDPR's terminology on basic concepts.

[23] Therefore, in principle, unless national constitutions block this, the police does not have to 'go to parliament' to organize its data processing. The recitals of the Law Enforcement Directive usefully remind us that law enforcement authorities should also respect the human rights-case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) on the legality requirements, demanding that the legal basis for privacy infringements in domestic laws, whatever its nature, be 'clear and precise and its application foreseeable for those subject to it' (LED, recital 33; De Hert in Mitsilegas & Vavoula, 2021, Chapter 10).

The proposed system allows for the processing of biometric data in various situations and scenarios: national laws can easily be adopted; the Law Enforcement Directive is silent on the meaning of the term 'vital interests' (that, in our view, should be read restrictively);[24] and the term 'public' could be misunderstood (for example, are data relating to a person who is walking on the street personal information that is 'manifestly made public'?).[25] Defenders of the Law Enforcement Directive-system might observe that the Directive seems a bit more demanding in terms of human rights, as compared to the Convention 108+. Article 6 of this Convention (on 'Special categories of data') only mentions the need for a legal basis and for appropriate safeguards and does not refer to a strict necessity test. However, the Directive can easily turn into an empty shell by creating a legal basis for whatever governmental processing (and voting laws is what governments do).

6. The mixed performance of the European framework: *Clearview*

To underpin the foregoing analysis of the EU legal rules on visual/biometric data and on facial recognition, we now move on to two recent cases: *Clearview* and *Bridges*. The first case demonstrates the generous scope of European data protection that seemingly always applies and the equally generous enforcement system where NGO-actions are complemented with actions by the EU data protection authorities. The second case reveals that law enforcement authorities seem to enjoy wide discretion in using technologies processing biometric data.

Clearview: In May 2021, several national data protection authorities and organizations (namely, Privacy International, ICO, CNIL, Hermes Centre for Transparency, Digital Human Rights, Homo Digitalis and noyb – the European Center for Digital Rights) filed complaints against *Clearview AI*, an American, facial recognition-tech firm. The company has created the (allegedly) biggest known database of more than three billion face images. With its automated tools, the firm searches the web and collects human (facial) images. It then stores them on its private repository and sells access to other firms, as well as law enforcement authorities (EDRi, n.d.). A closer look reveals two critical issues.

Firstly, what are the grounds for data collection by this American private firm? Can it rely on consent or legitimate interests or just consider that the processing of images is lawful, because relevant data are manifestly made public? Are the principles of transparency and purpose limitation respected? Although, to Clearview, relevant images come from public-only web sources (like news or public social media), it can be claimed that the fact that something is available online does not necessarily authorise/legitimise anyone to appropriate it in any way they wish (this claim can be supported by the CNIL's recent order against Clearview to stop gathering data of French citizens and comply with delete-requests, CNIL, 2021).

Secondly, does the use of Clearview's tool by European law enforcement authorities respect the Law Enforcement Directive and, in particular, the requirement for a proper legal basis and the Article 10-demands on biometric data? We recall that this LED-provision allows processing of biometric data solely under a strict necessity test, with appropriate safeguards in place and if there is a legal basis (Union or national law), when the processing is necessary to protect the vital interests of the data subject or of

[24] Recital 46 GDPR offers some clarity on the term 'vital interests'.

[25] It is noted that art. 11 LED sets out a clear prohibition on discriminative profiling that is based on sensitive data, including biometric data that are processed to uniquely identify an individual. Yet, that law enforcement (or other competent) authorities are bound by a general duty not to discriminate on the basis of such sensitive grounds is, in our view, a requirement stemming from general principles present in any democratic society (rather than a requirement introduced by the LED).

another person *or* the processing relates to data which are manifestly made public by the data subject (LED, art. 10).

As we know from case law of the ECtHR and the CJEU, a more rigorous version of the necessity test needs to be applied in cases where the interference with the right to the protection of personal data is serious (De Hert & Bouchagiar, 2021a, pp. 313–316). In the Clearview-case, it seems that the interference is particularly heavy: the private database with more than three billion images is gigantic allowing for a blanket surveillance regime, where everyone, not only criminals or suspects, may be monitored or stigmatised (Neroni Rezende, 2020). Hence, a fully-fledged version of the necessity test would demand: the existence of a pressing social need; suitability and appropriateness of the measure to address the pressing social need; an assessment of whether there are less harmful measures to achieve the desired purpose; and proportionality of the interference to the aim pursued, including a balancing exercise (private versus public interests) and looking for appropriate safeguards.

While the need to effectively fight against crime might constitute a pressing social need, it is extremely doubtful whether the other necessity-requirements, mentioned *above*, are met. On suitability and the existence of less harmful measures, law enforcement authorities do have various tools, from surveillance cameras to automated fingerprinting or profiling technologies that can assist in effectively fighting against crime. Moreover, on the balancing exercise (public interest versus individual rights), there are *neither* concrete, detailed rules (eg, on access or deletion) governing the measure (should not only expert police officers be granted access to Clearview's database? For how long are data retained?) *nor* adequate safeguards (should Clearview's database be used for any crime or only for serious offences? Is there adequate, independent review of the measure? Are there organisational and technical measures to ensure security of the system?). At least one author has doubted that Clearview could pass the strict necessity test (Neroni Rezende, 2020).

What else can be learned from the *Clearview* case? Not much yet. There is nervosity in Europe both about private companies offering this kind of facial recognition tools *and* about the use by law enforcement authorities of these tools. With regard to both issues the outcome of the legal procedures need to be awaited. What this does show is that Europe's general data protection rules offer a first grid to assess new technologies. This seems to be lacking in the US. Clearview AI's primary remaining market is indeed the US, where a lack of federal data protection laws allows it to be taken up by hundreds of law enforcement agencies in spite of its legal issues in certain States. As of 2020, the company was believed to have about 2,200 clients internationally including the FBI, Immigration and Customs Enforcement (ICE) and the Department of Justice (Ikeda, 2021).

7. The mixed performance of the European framework: *Bridges*

Moving on to *Bridges*, a case brought before the England and Wales High Court (the 'EWHC'), one may see how shaky the European legal framework is and how easy it can be bended to allow European law enforcement authorities to actually do whatever they wish (Stock, 2019). The Appellant was Edward Bridges, a civil liberties campaigner. The Respondent was the Chief Constable of the South Wales Police ('South Wales Police'). This force made use of facial recognition software ('NeoFace Watch'), which was developed by North Gate Public Services (UK) Ltd that compares pictures with faces on a 'watchlist' derived from a police database of existing facial images. The system was used between May 2017 and April 2019, mostly at large public events, whereby the public was informed via social media messages on Facebook and Twitter, notices on police vehicles, handed out postcard notices to members of the public and information put on its website.

The Divisional Court found no violation of the right to privacy. It was satisfied by, among others: the fact that the processing was (to the court) necessary to conduct a data protection impact assessment; the fact that, where there was no matching to information stored on the police's database, relevant data were deleted (hence, the principle of data minimisation was, to the court, not prejudiced); the existence of codes of practice and policies; transparency of the pilot project; and human intervention (by police officers) (*Bridges*, 2019).

However, these considerations were rejected by the England and Wales Court of Appeal. The appellate court found, among others, that the technology deployed by the police was not 'in accordance with the law' (as demanded by Article 8 paragraph 2 of the European Convention on Human Rights). Insufficiency of the scheme was supported by 'fundamental deficiencies' with the legal regime, granting police officers unfettered discretion, as well as: the novelty of the technology; the fact that it processed data of a large number of individuals, most of whom would be of no interest; the fact that information involved was sensitive; and the fact that the process was automated (*Bridges*, 2020, paragraphs 86–9l; Tomlinson, 2020; Ryder & Jones, 2020).[26] In this context, *Bridges* may demonstrate that existing provisions, including common law, can afford much latitude and discretion risking arbitrary intervention on citizens' rights.

The *Bridges* case teaches us that European data protection laws, combined with non-discrimination law, have relevance in questioning non-thoughtful implementation of facial recognition in the public area. Judges apply criteria taken from human rights law-related case law (on foreseeability and accessibility of the legal basis and proportionality) in conjunction with the rules of data protection and English non-discrimination law on impact assessments and transparency. All that does not amount in itself to a formal and absolute 'no' to facial recognition. On the contrary, the ease with which the Divisional Court found the South Wales Police compatible with these legal requirements and rules confirms our earlier finding that notwithstanding the obvious tensions with principles on legality, accountability, minimization, more is needed to take away all ambiguity of this technology. A similar position is taken by Wojciech Wiewiórowski, the EDPS, who runs through all objections against facial recognition (especially having regard to the principles of data minimization and data protection by design and by default), but calls for complementary regulatory steps, possibly including a ban or at least a moratorium, since there is clear political pressure in Europe to deploy and use the technology resulting in projects and police use that take advantage of all loopholes and vagueness in the European data protection rules. Crucial is his understanding that 'there was no great debate on facial recognition during the passage of negotiations on the GDPR and the law enforcement data protection directive' (Wiewiórowski, 2019).

The EDPS has rightly understood the necessity of its intervention and the necessity for a regulatory debate. The EU has not hesitated to create a legal basis for a full use by border *and* law enforcement authorities of biometric visual data in the migration and border policies.[27] These laws are loaded with

[26] The appellate court also found violation of: the Data Protection Act 2018 (there was no proper data protection impact assessment); as well as the 'public sector equality duty' (the police had offered no guarantees that the technology was not biased).

[27] On migration policies, the EU seems to have opened all gates. In September 2020, the EC released the amended Eurodac proposal as part of the New Pact on Migration and Asylum (European Commission, 2020a; 2020b). Focusing on migrants-surveillance (in particular, digitisation of migration management and border security), the EC appears to pay special attention to minors; this, by proposing a lower age-threshold for biometric data collection (6 years old, instead of 14; a discussion in: Marcu, 2021). The target is not only vulnerable groups (like minors), but everyone. These developments and the case law quoted in the next footnote are particularly relevant, in light of recent discussions on digital green certificates and vaccine passports (European Commission, 2021b). And they can support the argument that, instead of having national limitations to certain uses of technologies (on the basis of, for example, the *above*-analysed open invitation of art. 9(4) GDPR), what national lawmakers enjoy is the power to create more legal grounds allowing for data tsunamis to be processed.

data protection guarantees and have not met fundamental problems in court.[28] So, how to explain the controversy of facial recognition if the legal precedent has been created? The EDPS bravely attempts to do just this,[29] but it will be hard to forbid a tool to authorities in one context and allow it in another one. Rightly, he ends his position paper with the remark that 'it would be a mistake, however, to focus only on privacy issues. This is fundamentally an ethical question for a democratic society'.

8. European data protection rules are not enough to frame biometric recognition

The foregoing teaches us that, under the EU legal framework, the regulation of biometric data is well organized via hard law, binding private and public entities, as well as soft law, offering useful guidance on the interpretation of relevant biometric provisions. Still, the EU framework has been voted in times without facial recognition controversies and is clearly lacking a political message on the limits of this technology, in particular about biometric technologies in specific contexts, such as surveillance practices via face recognition deployed by law enforcement. The UK Surveillance Camera Commissioner has recently stressed insufficiencies of the GDPR, as well as the need for primary law (and an, until then, moratorium) to regulate face recognition-implementations by the police (Linkomies, 2020, pp. 14–15):

> 'I have asked for a fundamental review on surveillance. *The GDPR is not enough. Primary legislation* is required for this field," (...) For now, a *temporary moratorium is needed. Facial recognition is only good if used in certain circumstances*' (own emphasis).

In addition to the remarks made by EDPS-head Wiewiórowski (discussed *above*), three points can be highlighted to back up the 'GDPR is not enough' and 'we need at least a moratorium'-positions. *First*, the GDPR's abstract provisions may indeed fail to address particularities of specific technological implementations in national contexts. With the GDPR and the Law Enforcement Directive, the EU legislator has opted for a broad regulatory framework (Lynskey, 2015, p. 10) that is binding Member States. The baton is by necessity passed to national regulators, but in particular the GDPR does not

[28] First, in *Bochum*, the CJEU considered the storage of fingerprints within the passport lawful, under the Regulation (EC) No 444/2009, for the purpose of preventing illegal entry into the EU; and it clarified that this Regulation does not in itself allow for centralised storage of such fingerprints. Then, in *Willems*, the Court appears to grant broad discretion to national legislators in setting out the legal basis for the establishment of centralised databases. See: *Michael Schwarz v Stadt Bochum*, paragraph 61 ('(...) The regulation not providing for any other form or method of storing those fingerprints, it cannot in and of itself, as is pointed out by recital 5 of Regulation No 444/2009, be interpreted as providing a legal basis for the centralised storage of data collected thereunder or for the use of such data for purposes other than that of preventing illegal entry into the European Union (...)'); *W. P. Willems et al. v. Burgemeester van Nuth et al.*, paragraphs 9, 48 ('(...) In accordance with Recital 5 in the preamble to Regulation No 444/2005, which amended Regulation No 2252/2004: 'Regulation ... No 2252/2004 requires biometric data to be collected and stored in the storage medium of passports and travel documents with a view to issuing such documents. This is without prejudice to any other use or storage of these data in accordance with national legislation of Member States. Regulation ... No 2252/2004 does not provide a legal base for setting up or maintaining databases for storage of those data in Member States, which is strictly a matter of national law.' (...) It follows, in particular, that Regulation No 2252/2004 does not require a Member State to guarantee in its legislation that biometric data will not be used or stored by that State for purposes other than those mentioned in art. 4(3) of that regulation (see, to that effect, judgment in Schwarz, C-291/12, EU:C:2013:670, paragraph 61) (...)'). These considerations may run counter to case law of the ECtHR and, in particular, *Marper*'s holding that the retention of fingerprints and DNA-related information of individuals suspected (but not convicted) of certain crimes was a disproportionate interference with the right to privacy.

[29] "The purposes that triggered the introduction of facial recognition may seem uncontroversial at a first sight: it seems unobjectionable to use it to verify a person's identity against a presented facial image, such as at national borders including in the EU. It is another level of intrusion to use it to determine the identity of an unknown person by comparing her image against an extensive database of images of known individuals".

give them powers to prohibit in general certain uses of technologies. Hence, all the weight falls on the shoulders of data protection authorities that either do not act or act in a non-coordinated way with confused outcomes (see on dash-cams, Štitilis & Laurinaitis, 2016). It would make sense, as pointed out by the UK Commissioner, to have primary law, such as an Act of the UK Parliament,[30] regulating and prohibiting in certain contexts face recognition applications by the UK police. *Second*, a moratorium, halting such applications for an agreed amount of time (be it until the introduction of primary law or until the use of face recognition technologies by the police is proved safe and citizen-protective), would be a reasonable instrument to tackle risks posed by these technologies. *Third*, it is doubtful whether the Law Enforcement Directive can address these risks in case of facial recognition used by law enforcement authorities. More so than the GDPR, the Law Enforcement Directive demonstrates some tolerance toward biometric data processing.[31] This is understandable: the goals pursued by 'competent authorities' are related to the 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties' (LED, art. 1(1), 3(7)). Yet, how could the LED, demanding national transposition, guarantee that the interference and intrusiveness of latest technological implementations are proportionate to the crime-related purposes pursued, especially in the absence of technology-specific rules? This and similar questions are important for any biometric data processing operation. As we have witnessed in landmark cases of the ECtHR, mere retention of personal data could be seen as a particularly heavy interference with individual rights (see, for example, *Marper*, paragraphs 67, 121, cited *above* in note 27). Such an interference may become even more serious where biometric data, a special category of personal data, are further processed (for instance, shared with third parties) in the name of crime prevention. Thus, special attention need be paid to vulnerabilities that could emerge from biometric data processing in concrete contexts.

In our view, there is a need for more specific rules and bright line bans. As analysed above, both the GDPR and the Law Enforcement Directive in general do not embrace the concept of prohibitions on certain technologies. Imagine what would happen if such a step stifled innovation or hampered governmental policies. Remarkably, the EU seems to opt for bans, not through *lex generalis* (like the GDPR) but, via *lex specialis*; and this is law distant from the data protection key instruments, like the Digital Services Act.[32] It might well be that a similar step will be taken with facial recognition. Rather

[30] For examples of primary legislation in the UK, see UK Parliament. (n.d.). We assume that the UK Surveillance Camera Commissioner was not referring to primary law in the EU context (a treaty). For the EU primary and secondary legal instruments, see Craig & De Búrca (2015, p. 103 et seq.).

[31] Compare: LED, art. 10 (using the terms 'shall be allowed') with GDPR, art. 9(1) (using the phrasing 'shall be prohibited'). Still, it is reminded that the LED allows biometric data processing only if strict conditions are met.

[32] To illustrate, we refer to the EDPS' recent opinion calling for a ban on surveillance-based targeted ads having regard to the Commission's Digital Services Act (DSA). We welcome the EDPS' opinion and find it particularly promising in an era: when advertising and commercial surveillance can lead to, among others, manipulation, undue discrimination or privacy and data protection breach; when the use of certain technologies, such as systems visually tracking and capturing biometric data (physiological responses), can disproportionately interfere with fundamental rights; and when receiving commercial services in exchange for personal data (including biometric data) is expressly permitted under the Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. See European Parliament & Council, 2019, art 3(1) ('(...) This Directive shall apply to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price. This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader (...)'). Interestingly, similar proposals on banning surveillance advertising have been submitted by the US privacy, consumer, competition and civil rights organisations. See, among others, Lomas (2021b). On the EDPS' opinion, see EDPS (2021a; 2021b); European Commission. (2020c); Lomas (2021a). On surveillance-based ads, see: Forbrukerradet (2021).

than complementing the GDPR and the Law Enforcement Directive with specific prohibitions[33] and calling facial recognition by name, the data protection community is now looking at the proposed AI regulation to address some, not all, facial recognition issues.[34]

9. A need for concreteness, precision, bright-line bans and effective remedies

In light of the above analysis, the following regulatory starting points could be taken into account by the European lawmakers to strictly regulate surveillance practices:[35]

- ***Concreteness:*** The EU misses unambiguous clarity: legal provisions having clear objectives and targeted at concrete technologies. Its tech-neutral regime, based on generic rules and abstract principles, can, on the one hand, be positive as covering any technology (and reducing workload of lawmakers). However, on the other hand, it lacks enhanced legal certainty. Can developers of face recognition tools really foresee the way in which and the circumstances under which the law may apply to their case and be more certain about whether and how to enter the market? Are individuals subjectable to face recognition truly aware of how they may be protected against any possible violation? In our view, no. Examples from other jurisdictions can demonstrate that a piece-meal regulation can better establish and maintain legal certainty. In the US, for instance, legal provisions analytically describe the '*whether's*' and the '*how's*' regarding entering the market or the protection of individuals concerned.[36]
- ***Precision:*** The EU legal scheme lacks precision in key topics and, in particular: consent, the duty to inform, function creep and absence of certain prohibitions/duties. On consent, the EU focuses on specific requirements, like that consent be informed or specific; yet, further demands could make our regime more individual-friendly. For instance, special attention could be paid to the will of the person under surveillance; does she/he consent with independent, uninfluenced and genuine will? The EU could learn from other legal instruments, like the (US) federal 2020 National Biometric Information

[33] Art. 11 LED could serve as a model. This provision sets out a clear prohibition on discriminative profiling that is based on sensitive data, including biometric data that are processed to uniquely identify an individual.

[34] See the EDPB and the EDPS' 5/2021 Joint Opinion on the proposal for an Artificial Intelligence Act, where they stressed the lack of concrete prohibitions (European Commission, 2020d; EDPB & EDPS, 2021a, pp. 2, 3, 11, 12; 2021b). This proposed Act forbids (in art. 5): the 'placing on the market, putting into service or use' of AI-technologies that affect people's behaviour in a way that leads or may lead to individual 'physical or psychological harm'; the 'placing on the market, putting into service or use' of certain AI-technologies by public actors; and the use of certain biometric technologies in public areas for law enforcement goals (unless this is considered necessary, for example, to prevent crime). In our opinion, these prohibitions are not real prohibitions (see also Malgieri & Ienca, 2021). Rather, it is a system tolerating various biometric implementations, like the selling of technologies by European designers to third countries or the use of systems processing biometrics after-the-fact (not 'real-time') or for purposes other than law enforcement (such as public health) (Veale & Borgesius, 2021). In addition, the requirement of 'physical or psychological harm' of a *person* excludes situations where the detriment goes beyond the individual level or is difficult to be connected with a concrete person or occurs at another level. Experience from the environment has taught us how the public, the people (rather than a concrete individual) may suffer detriment (including future detriment) due to certain practices not targeted at a particular person. Moreover, the prohibition related to law enforcement is conditional upon many *if's* and may not apply where the AI-practice is deemed necessary to achieve certain goals, like crime detection. Interestingly, although the proposed Act provides for a detailed authorisation process (including an independent body), this rigorous process may not apply in certain cases of urgency (art. 5); and, in any event, Member States are granted discretion in permitting by law such AI-practices in the law enforcement context (art. 5).

[35] These starting points are partly lessons learned from our working paper on US laws. For a more detailed analysis of these laws (twenty in total), see De Hert and Bouchagiar (2021b).

[36] By way of example, see section 20 of the California Privacy Rights Act (2020) addressing businesses and imposing various duties, from cybersecurity audits to regular reporting and risk-evaluations.

Privacy Act aiming to tackle biometric data exploitation by private entities and requiring consent be 'informed', 'specific' and so forth (terms also present in the GDPR), but also focusing on the independent, genuine will of the person concerned, who must be free from outside control.[37] On the duty to inform the data subject, further requirements could be introduced, such as the obligation to conduct regular accountability reports, thus making relevant information available to the individuals concerned.[38] Moreover, the EU scheme could become more shielding when prohibiting function creep. Here, cumulative requirements could apply; in particular, there could be a demand that the purpose of the processing at hand be explicit *and* presented to the end-user *and* remain unaltered *and* conditioned upon prior review and consultation (requirements present in other regimes, like the US).[39] Last, certain duties and prohibitions that are completely absent in the EU scheme could be introduced: the prohibition to use surveillance for unfair discrimination;[40] the prohibition to profit from engaging in surveillance;[41] the application of standards of care (known from industry-areas) or the treatment of biometric data as particularly (both) sensitive *and* confidential information.[42]

- ***Bright-line bans:*** The EU lacks bright-line rules. To support the argument for the need for such rules, one may refer to the US regime, where explicit prohibitions on certain technological uses or surveillance practices can be detected. Remarkably, in the US, certain principled prohibitions reach the level of unconditionality: a Californian Act prohibits in an absolute manner all law enforcement actors from engaging in biometric surveillance through cameras;[43] the federal 2020 Facial Recognition and Biometric Technology Moratorium Act prohibits any exercise of biometric surveillance by the federal government until precise laws are in place;[44] the proposed Data Protection Act of 2021 (section 12) prohibits data aggregators and service providers from engaging in certain activities (like the commission of 'unlawful, unfair, deceptive, abusive, or discriminatory acts or practices' or re-identifying 'an individual, household, or device from anonymized data'); New York's Assembly Bill A6787D (subdivision 2) bans the purchase and use of biometric technologies in public and private schools; Portland's Ordinance bans face recognition outright; and Baltimore's ordinance prohibits the city from obtaining a face recognition system and contracting other entities with a view to using such systems, but also private actors from obtaining, retaining, accessing or using a face recognition system or information gathered from such a system. Notably, in the US, not only states and/or cities have banned or aim to ban certain technological implementations, but also police departments have banned the use of face recognition; and this, voluntarily (MacCarthy, 2021).
- ***Practical organisation of remedies:*** Although the GDPR and the LED recognise the right to access to justice and the right to an effective remedy, first, they do not go into detail on how one may

[37] See 2020 National Biometric Information Privacy Act, sections 3(b)(1) and 2(4).

[38] Again, lessons could be learnt from the US, such as the Washington's Engrossed Substitute Senate Bill 6280 (section 3(1) and (2)), imposing duties to prepare accountability reports.

[39] See, for example, the proposed federal 2019 Commercial Facial Recognition Privacy Act (section 3(a)(3)); Virginia Senate Bill 1392, section 59.1–574; or Washington's Engrossed Substitute Senate Bill 6280, section 3(7).

[40] For such prohibitions in the US, see, among others: the proposed Commercial Facial Recognition Privacy Act of 2019, section 3(a)(2); the proposed 2020 Genetic Information Privacy Act, section 56.181(e); Virginia Senate Bill 1392, section 59.1–574; Washington's Engrossed Substitute Senate Bill 6280, section 6; or New Jersey's Assembly Bill 989.

[41] Such bans exist in the US. See for instance: the federal 2020 National Biometric Information Privacy Act, sections 3(c) and 3(d); the 2008 Illinois Biometric Information Privacy Act, section 15(c); or Texas Business and Commerce Code (Sec 503.001), point (c).

[42] Such standards can be found in the US: the federal 2020 National Biometric Information Privacy Act, section 3(e); the 2008 Illinois Biometric Information Privacy Act, section 15(e); or Texas Business and Commerce Code (Sec 503.001), point (c).

[43] California's Assembly Bill No 1215 (section 2(b)).

[44] Section 3(a) and (b) 2020 Facial Recognition and Biometric Technology Moratorium Act.

exercise these rights and, second, the approach is monolithic, solely based on data protection law. Contrary, the US seem to better clarify their justice-routes, as well as combine several legal fields with a view to enhancing effectiveness of their remedy-scheme. To illustrate, the proposed federal 2019 Commercial Facial Recognition Privacy Act expressly classifies any breach of its provisions as unfair or deceptive act/practice;[45] or the recent legislative support for a new FTC privacy bureau to assist in accomplishing tasks concerning unfair or deceptive acts and practices (Committee on Energy and Commerce, 2021; Kurth, 2021) can render competition laws applicable (in conjunction with data protection laws) and thus better and more effectively protect individuals.

10. Conclusion and take homes: honest bans, moratoria and substance

To sum up, the analysis of the GDPR and the LED (in section 2) showed that the EU's general and tech-neutral approach may result in uncertainty. Vagueness was further demonstrated by the discussion (in section 3) in particular relation to the processing of biometric data: this processing is, on the one hand, prohibited and, on the other hand, permitted under a long list of exceptions. Thereafter, although a dynamic reading and interpretation of Article 9(4) of the GDPR (as argued in section 4) could lead to the introduction by national lawmakers of domestic measures to limit or ban certain technological implementations, to our knowledge, no national regulatory entity has relied upon this provision to prohibit risky and intrusive technological implementations. In addition, police-friendliness of the LED (analysed in section 5) that is, moreover, permissive regarding the processing of biometric data might heavily interfere with the right to privacy, especially in an era when law enforcement-databases may be expanded to include more and more sensitive data (like face recognition data; see: EDRi, 2021). The situation becomes acute where law enforcement is directly granted access by private firms to sensitive items of information in the absence of a clear legal basis, as well as where police enjoy more and more power and discretion in using technologies to process biometric data (as shown in sections 6 and 7 on *Clearview* and *Bridges*). Reflecting on the need for bright line rules (an argument that was substantiated in section 8), this contribution submitted four recommendations (section 9) to enhance protection of the citizens by framing surveillance practices in a more satisfactory way:

- ***Concreteness***, in the sense of unambiguous clarity; laws with clear objectives, targeted at concrete technologies.
- ***Precision*** regarding the EU's consent-scheme; the duty to inform the data subject; function-creep; and certain duties/prohibitions, such as bans on using technologies to unduly discriminate against citizens.
- ***Bright-line bans*** on certain surveillance practices that can reach the level of unconditionality.
- ***Practical organisation of remedies***, meaning detailedness on how to exercise the right to an effective remedy and combination of several legal fields (like competition law) to more effectively exercise this right via different possible judicial avenues.

By looking at various jurisdictions (such as the US referred to above), it seems that there is a common interest in regulating surveillance-related practices and technologies. Although principles, ranging from accountability and transparency to reason-giving, appear present in different laws/jurisdictions, some regulators, like in the US, have gone further to describe in more detail how to apply such principles to

[45] See section 4(a).

concrete technological contexts. In light of the above considerations and given that the EC has recently been urged to permanently ban biometric mass surveillance practices, the EU could be inspired by jurisdictions, like the US, and set out some bright-line rules to protect its members, its citizens, from bad things that are likely to occur. After having established a broad regime that could, at least in theory, cover any specific technology or general purpose-technologies, the EU could further opt for specific rules on concrete technologies with a view to tackling urgent (including near-term and practical) issues posed by contemporary implementations and threatening fundamental rights and freedoms of citizens.

It is clear from the foregoing, we believe, contrary to some commentators,[46] that the EU could learn several things from the development in the US with regard to biometric processing of data and surveillance:

> First, the EU legal regime on surveillance could become honestly prohibitive. It could identify risks that might materialise; and it could say with clarity 'no' to technologies, whose use can be dangerous and harmful in specific high-risk areas. Neither the GDPR nor the Law Enforcement Directive adopt such an approach. These EU legal instruments probably fail to detect 'bad' uses of technologies that should be prohibited and to distinguish them from others.[47] In this context, the EU legal scheme may lack honesty: its 'no' appears fake, followed by many *if's, but's and when's* that, in the end, make it permissive.[48]
>
> Second, a moratorium-approach, like in the US, may seem promising. When finding a technology-aspect/use unsafe or particularly intrusive, the EU could prohibit any implementations to protect the data subject either until there is the infrastructure to accurately assess safety of the technology or until concrete laws are introduced to minimise risk and dangerousness. Laws that push the pause-button are, to our knowledge, nowhere to be found in Europe.
>
> Third, under the EU framework, everything is 'done' by using 'data protection law', an area of law that focuses heavily on processes and procedure, but misses substance and clear outcomes. Whenever there is a technology that processes data, the supervisory data protection authorities are the first 'on it' but never, at least to our knowledge, arrive at conclusions like '*this is too complex for data protection law, we need additional support from civil law, or from criminal law of from any other legal area*'. By seeing everything only through one lens, comprehensive solutions might be lost out of sight. But people want clear rules speaking to them comprehensively. In our view, the EU reliance on data protection law should be enriched with ideas, concepts and ideas found in other (legal) fields, such as criminal law's 'probable cause', 'confidentiality' known from commercial or professional contexts, industry-related 'standards' or market-related prohibitions.

To conclude, in the EU, regulators have remained focused on the very law of 'data processing', instead of citizen-protection. It may be advisable to look at the broader picture. The issue of surveillance exercised by anyone (be it the state, the firms or the very citizens) over anyone (including vulnerable groups, like

[46] For example, in a 2018 publication, Meyer (2018) advocates for supremacy of EU data protection laws (compared to the US regime). In our opinion, the arguments set forth are inadequately substantiated: alleged 'slapping' with 'stratospheric fines' can also be the case in the US (and may hardly work as counterincentive in case of Internet giants engaging in serious breaches); the risk based-perspective (adopted by the EU legislator in data protection areas) is often emphasised over the claimed (by Meyer) human rights-approach; and, on the Nazi-argument, one may hardly draw linkages between the 'collective' memories of war victims and their contribution to the drafting of the GDPR.

[47] In this regard, see Štitilis and Laurinaitis (2016, pp. 323–325), where the idea of banning dashcams (in the EU context) is almost laughed at. See also Bennett and Grant (1999, Chapter 2, p. 39), discussing fair information practice norms that may fail to offer sufficient criteria to determine ethical acceptability of processing operations.

[48] For the EU legal regime as a 'legitimizing' framework, as well as arguments for (and against) its 'permissive' nature, see Lynskey (2015, pp. 30 et seq.).

kids) is not just a matter of data protection law. Rather, it is a fundamental question on the kind of society that people want to live in.[49] Then, maybe, it is desirable that regulators properly deal, not only with the legal status of sensitive data (eg, by opening up lists to include more and more data in legal provisions that, in the end of the day, allow for the processing),[50] but primarily with the spying society and its picture-taken citizens. This surveillability of everything and by anyone can thus be properly addressed, not (only) by cost-benefit assessments and risk-based approaches, often considering the legitimate (including the economic) interests of stakeholders, but (mainly) via fundamental evaluations of what is at stake and against what it need be balanced. In case of biometric mass surveillance, the stake is people's privacy and dignity. This must be balanced against 'something bigger' than the economic interests of firms, sharing people's data with law enforcement. If this 'something bigger' is the need to fight against crime and to protect national security; and if these latter needs are prioritised over privacy and dignity; then, it may be disappointing that people are, to a great extent, losing their right to privacy, because innocent citizens 'have nothing to hide'. Is this a proper justification? Is this not like restricting the freedom of speech, because one may have nothing to say?[51]

Acknowledgments

Supported by the Luxembourg National Research Fund FNR PRIDE17/12251371.

The Open Access publication of this paper was supported by the Panelfit project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

References

AlgorithmWatch & Bertelsmann Stiftung. (2020, September 1). *Automated Decision-Making Systems in the COVID-19 Pandemic: A European Perspective – Automating Society Report 2020. AlgorithmWatch & Bertelsmann Stiftung*. https://algorithmwatch.org/en/automating-society-2020-covid19/.

Alterman, A. (2003). A piece of yourself: Ethical issues in biometric identification. *Ethics and Information Technology*, *5*, 139–150. doi: 10.1023/B:ETIN.0000006918.22060.1f.

Bannister, F. (2005). The panoptic state: Privacy, surveillance and the balance of risk. *Information Polity*, *10*, 65–78.

Bazen, A., & Gerez, S. (2002). Achievements and Challenges in Fingerprint Recognition. In D. Zhang (Ed.), *Biometric Solutions: For Authentication in an E-World*, pp. 23–57. Springer. doi: 10.1007/978-1-4615-1053-6_2.

Bennett, C.J. (2008). *The Privacy Advocates. Resisting the Spread of Surveillance*. MIT Press.

Berk, R. (2019). Accuracy and fairness for juvenile justice risk assessments. *Journal of Empirical Legal Studies*, *16*(1), 175–194. doi: 10.1111/jels.12206.

Bjorklund, F. (2011). Pure Flour in your Bag: Governmental Rationalities of Camera Surveillance in Sweden. *Information Polity*, *16*, 355–368

Blair, T., & Campbell, P. (2018, July 9). What Is Personal Data under the GDPR? The Edata Guide to GDPR. *Morgan Lewis*. https://www.morganlewis.com/pubs/2018/07/the-edata-guide-to-gdpr-what-is-personal-data-under-the-gdpr.

Brayne, S. (2020). *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford University Press.

Bridges. (2019). *Bridges, R (On Application of) v The Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) (2019, September 4). https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Admin/2019/2341.html&query=(2019.)+AND+(EWHC)+AND+(2341).

[49] In this regard, see: Klovig Skelton (2021).

[50] For recommendations to open up the list of sensitive data, see: European Parliament (2021).

[51] As aptly put by Snowden (n.d.), 'arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say'.

Bridges. (2020). *Bridges, R (On the Application Of) v South Wales Police* [2020] EWCA Civ 1058 (2020, August 11). https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html.

California Assembly Bill No. 1215, Chapter 579 (2019). https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1215.

California Genetic Information Privacy Act, Senate Bill 980 (2020). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200SB980.

California Privacy Rights Act of 2020. https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf.

Clavell, G.G. (2011). Local Surveillance in a Global World: Zooming in on the Proliferation of CCTV in Catalonia. *Information Polity*, *16*, 319–338.

Clavell, G.G., Lojo, L.Z., & Romero, A. (2012). CCTV in Spain: An empirical account of the deployment of video-surveillance in a Southern-European country. *Information Polity*, *17*, 57–68.

CNIL. (2021, December 16). *Facial recognition: the CNIL orders CLEARVIEW AI to stop reusing photographs available on the Internet*. https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet.

Commercial Facial Recognition Privacy Act of 2019, S. 847 (2019). https://www.congress.gov/bill/116th-congress/senate-bill/847/text.

Committee on Energy and Commerce. (2021). Budget Reconciliation Legislative Recommendations Relating to FTC Privacy Enforcement. https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2021/09/BILLS-117pih-SubtitleO.pdf.

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (2005). *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005 Progress Report). Council of Europe. https://rm.coe.int/16806840ba.

Council of Europe. (2018a). Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

Council of Europe. (2018b). Explanatory Report to the Convention 108+. *Council of Europe*. https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

Council of the European Union. (2008). Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977.

Craig, P., & De Búrca, G. (2015). *EU Law: Text, Cases, and Materials*. Oxford University Press 2015. doi: 10.1093/he/9780198714927.001.0001.

Data Protection Act of 2021, S. (2021). https://www.gillibrand.senate.gov/imo/media/doc/DPA%20Bill%20Text.pdf.

De Hert, P. (2005). Biometrics: legal issues and implications. *European Commission*. https://www.statewatch.org/media/documents/news/2005/apr/jrc-biometrics-paul-de-hert.pdf.

De Hert, P. (2013). Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions. In P. Campisi (Ed.), *Security and Privacy in Biometrics*, pp. 369–413. Springer. doi: 10.1007/978-1-4471-5230-9_15.

De Hert, P. (2016). The Future of Privacy – Addressing Singularities to Identify Bright-Line Rules that Speak to Us. *European Data Protection Law Review*, *2*(4), 461–466. doi: 10.21552/EDPL/2016/4/5.

De Hert, P., & Bouchagiar, G. (2021a). Adding and removing elements of the proportionality and necessity test to achieve desired outcomes. Breyer and the necessity to end anonymity of cell phone users. *EDPL*, *7*(2), 304–318. doi: 10.21552/edpl/2021/2/23.

De Hert, P., & Bouchagiar, G. (2021b). Facial Recognition, Visual and Biometric Data in the US. Recent, Promising Developments to Regulate Intrusive Technologies. *Brussels Privacy Hub*, *7*(29). https://brusselsprivacyhub.eu/publications/wp729.

De Hert, P., & Boulet, G. (2016). The co-existence of administrative and criminal law approaches to data protection wrongs. In D. Wright & P. De Hert (Eds.), *Enforcing Privacy. Regulatory, Legal and Technological Approaches*, pp. 357–394. Springer. doi: 10.1007/978-3-319-25047-2_16.

De Hert, P., & Malgieri, G. (2021). One European Legal Framework for Surveillance: The ECtHR's Expanded Legality Testing Copied by the CJEU. In V. Mitsilegas & N. Vavoula (Eds.), *Surveillance and Privacy in the Digital Age. European, Transatlantic and Global Perspectives*, pp. 255–295. Hart Publishing. https://www.bloomsburyprofessional.com/uk/surveillance-and-privacy-in-the-digital-age-9781509925179/.

De Hert, P., & Papakonstantinou, V. (2014). The Council of Europe Data Protection Convention Reform: Analysis of the New Text and Critical Comment on its Global Ambition. *Computer Law & Security Review*, *30*(6), 633–642. doi: 10.1016/j.clsr.2014.09.002.

ECI. (2021, January 7). Civil society initiative for a ban on biometric mass surveillance practices. *European Union*. https://europa.eu/citizens-initiative/initiatives/details/2021/000001_en.

EDPB. (2019, July 10). Guidelines 3/2019 on processing of personal data through video devices. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf.

EDPB. (2020, January 29). Guidelines 3/2019 on processing of personal data through video devices. *EDPB*. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

EDPB & EDPS. (2021a, June 18). EDPB-EDPS 5/2021 Joint Opinion on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en.

EDPB & EDPS. (2021b, June 21). EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination. *EDPB*. https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en.

EDPS. (2021a, February 10). Opinion 2/2021 on the Proposal for a Digital Markets Act. *EDPS*. https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf.

EDPS. (2021b, February 10). Opinions on the Digital Services Act and the Digital Markets Act. *EDPS*. https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opinions-digital-services-act-and-digital_en.

EDRi. (2021, December 8). European Commission jumps the gun with proposal to add facial recognition to EU-wide police database. *EDRi*. https://edri.org/our-work/press-release-ec-jumps-the-gun-on-prum/.

EDRi. (n.d.). Challenge against Clearview AI in Europe. *EDRi*. https://edri.org/our-work/challenge-against-clearview-ai-in-europe/.

European Commission. (2020a). New Pact on Migration and Asylum. *European Commission*. https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/new-pact-migration-and-asylum_en.

European Commission. (2020b). Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulations (EU) 2018/1240 and (EU) 2019/818. https://ec.europa.eu/info/sites/default/files/proposal-regulation-biometric-data_en.pdf.

European Commission. (2020c). Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN.

European Commission. (2020d). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

European Commission. (2021a, January 7). European Citizens' Initiative: Commission decides to register an initiative for 'a ban on biometric mass surveillance practices'. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_22.

European Commission. (2021b, March 17). Coronavirus: Commission proposes a Digital Green Certificate. *European Commission*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1181.

European Parliament. (2021, November 18). Parliamentary questions – Subject: Risks in respect of the use of biometrics. *European Parliament*. https://www.europarl.europa.eu/doceo/document/E-9-2021-005185_EN.html.

European Parliament & Council. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

European Parliament & Council. (2016a). 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). https://eur-lex.europa.eu/eli/reg/2016/679/oj.

European Parliament & Council. (2016b). Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG.

European Parliament & Council. (2019). Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770.

European Union. (n.d.). National Transposition (Document 32016L0680). https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32016L0680.

European Union Agency for Fundamental Rights and Council of Europe (2018). *Handbook on European Data Protection Law*. European Union Agency for Fundamental Rights and Council of Europe. https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition.

Facial Recognition and Biometric Technology Moratorium Act of 2020, H. R. 7356 (2020). https://www.congress.gov/116/bills/hr7356/BILLS-116hr7356ih.pdf.

Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084 (2020). https://www.congress.gov/116/bills/s4084/BILLS-116s4084is.pdf.

Fonio, C. (2011). The silent growth of video surveillance in Italy. *Information Polity*, *16*, 379–388.

Forbrukerradet (2021, June 22). International coalition calls for action against surveillance-based advertising. *Forbrukerradet*. https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/.

Fussey, P. (2012). Eastern Promise? East London Transformations and the State of Surveillance. *Information Polity*, *17*, 21–34.

Heilmann, E. (2011). Video Surveillance and Security Policy in France: From Regulation to Widespread Acceptance. *Information Polity*, *16*, 369–377.

Hildén, J. (2019). *The Politics of Datafication: The influence of lobbyists on the EU's data protection reform and its consequences for the legitimacy of the General Data Protection Regulation*. University of Helsinki. https://researchportal.helsinki.fi/en/publications/the-politics-of-datafication-the-influence-of-lobbyists-on-the-eu.

Hope, A. (2015). Governmentality and the 'Selling' of School Surveillance Devices. *The Sociological Review*, *63*(4), 840–857. doi: 10.1111/1467-954X.12279.

ICO. (n.d.). What is special category data?. *ICO*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/.

Ikeda, S. (2021, July 3). *EU Privacy Groups File Complaint, Assert Clearview AI Facial Recognition Software Violates Data Protection Laws. CPO Magazine.* https://www.cpomagazine.com/data-privacy/eu-privacy-groups-file-complaint-assert-clearview-ai-facial-recognition-software-violates-data-protection-laws/.

Illinois Biometric Information Privacy Act, Act 14 §§14/1-14/99 (2008). https://casetext.com/statute/illinois-compiled-statutes/rights-and-remedies/chapter-740-civil-liabilities/act-14-biometric-information-privacy-act.

Jasserand, C. (2016). Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data – Which Changes Does the New Data Protection Framework Introduce? *European Data Protection Law Review*, *2*(3), 297–311. doi: 10.21552/EDPL/2016/3/6.

Jasserand-Breeman, C. (2019). *Reprocessing of Biometric Data for Law Enforcement Purposes: Individuals' Safeguards Caught at the Interface Between the GDPR and the Law Enforcement Directive*? University of Groningen. https://research.rug.nl/en/publications/reprocessing-of-biometric-data-for-law-enforcement-purposes-indiv.

Keymolen, E., & Van Der Hof, S. (2019). Can i still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust. *Journal of Cyber Policy*, *4*(2), 143–159. doi: 10.1080/23738871.2019.1586970.

Kindt, E. (2013). *Privacy and Data Protection Issues of Biometric Applications: A Comparative Analysis*. Springer. doi: 10.1007/978-94-007-7522-0.

Kindt, E. (2018). Having Yes, Using No? About the New Legal Regime for Biometric Data. *Computer Law and Security Review*, *34*(3), 523–538. doi: 10.1016/j.clsr.2017.11.004.

Klovig Skelton, S. (2021, November 12). Oversight of biometrics and surveillance should not go to ICO. *Computer Weekly*. https://www.computerweekly.com/news/252509416/Oversight-of-biometrics-and-surveillance-should-not-go-to-ICO.

Kurth, H.A. (2021, September 16). U.S. House Committee Votes to Create New FTC Privacy Bureau and Appropriate $1 Billion to the Agency. *Hunton Privacy Blog*. https://www.huntonprivacyblog.com/2021/09/16/u-s-house-committee-votes-to-create-new-ftc-privacy-bureau-and-appropriate-1-billion-to-the-agency/.

Linkomies, L. (2020). Data Protection and Artificial Intelligence in the Spotlight. *Privacy Laws & Business International Report*, *163*, 14.

Lomas, N. (2021a, February 10). EU's top privacy regulator urges ban on surveillance-based ad targeting. *Techcrunch*. https://techcrunch.com/2021/02/10/eus-top-privacy-regulator-urges-ban-on-surveillance-based-ad-targeting/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAK7bfazhQHBPEqlefstkuDqWfie4AqfmAGGsu27Ne-9HzS6Nx7zpvAyWkAOL1jLolYIGI31PigEIfURBS5CAfieB9ioek4sZDBSaLiMrZKPgAzAZsEtR0oa27n3-CVqQIyfxb03cNy4b_D7C4cYoa1psnw–6IYIduW3xMN8lrW9.

Lomas, N. (2021b, March 22). US privacy, consumer, competition and civil rights groups urge ban on 'surveillance advertising'. *Techcrunch*. https://techcrunch.com/2021/03/22/us-privacy-consumer-competition-and-civil-rights-groups-urge-ban-on-surveillance-advertising/.

Lynskey, O. (2015). *The Foundations of EU Data Protection Law*. Oxford University Press. https://global.oup.com/academic/product/the-foundations-of-eu-data-protection-law-9780198718239?cc=gr&lang=en&.

MacCarthy, M. (2021, May 26). Mandating fairness and accuracy assessments for law enforcement facial recognition systems. *Brookings*. https://www.brookings.edu/blog/techtank/2021/05/26/mandating-fairness-and-accuracy-assessments-for-law-enforcement-facial-recognition-systems/.

Malgieri, G., & Ienca, M. (2021, July 7). The EU regulates AI but forgets to protect our mind. *European Law Blog*. https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/.

Maple, C., & Norrington, P. (2006, April 20–22). *The Usability and Practicality of Biometric Authentication in the Workplace* [Conference presentation]. Proceedings of the First International Conference on Availability, Reliability and Security, Vienna, Austria. https://ieeexplore.ieee.org/document/1625410.

Marcu, B.I. (2021, April 29). Eurodac: Biometrics, Facial Recognition, and the Fundamental Rights of Minors. *European Law Blog*. https://europeanlawblog.eu/2021/04/29/eurodac-biometrics-facial-recognition-and-the-fundamental-rights-of-minors/.

Marx, G. (1999). Ethics for the New Surveillance. In C. Bennett & R. Grant (Eds.), *Visions of Privacy: Policy Choices for the Digital Age*, pp. 39–67. University of Toronto Press. doi: 10.3138/9781442683105.

Meyer, D. (2018, March 21). Opinion: How Europe is better at protecting data than the U.S. – and what the Stasi and Nazis have to do with it. *Market Watch*. https://www.marketwatch.com/story/why-europe-does-a-better-job-of-protecting-online-privacy-than-the-us-does-2018-03-20.

Michael Schwarz v Stadt Bochum, C-291/12 (CJEU, 17 October 2013). https://curia.europa.eu/juris/liste.jsf?num=C-291/12.

Musik, C. (2011). The thinking eye is only half the story: High-level semantic video surveillance. *Information Polity*, *16*, 339–353.

National Biometric Information Privacy Act of 2020, S. (2020). https://www.merkley.senate.gov/imo/media/doc/20.08.04%20National%20Biometric%20Information%20Privacy%20Act.pdf.

Neroni Rezende, I. (2020). Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective. *New Journal of European Criminal Law*, *11*(3), 375–389. doi: 10.1177/2032284420948161.

New Jersey Assembly Bill 989 (2020). https://www.njleg.state.nj.us/2020/Bills/A1000/989_I1.PDF.

New York Assembly Bill A6787D (2020). https://legislation.nysenate.gov/pdf/bills/2019/a6787d.

O'Hara, K. (2015). Data, legibility, creativity ... and power. *IEEE Internet Computing*, *19*(2), 88–91. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7061804.

Ogbanufe, O., & Kim, D. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. *Decision Support Systems*, *106*, 1–14. doi: 10.1016/j.dss.2017.11.003.

Parliamentary Assembly of the Council of Europe. (2011). *The Need for a Global Consideration of the Human Rights Implications of Biometrics* (Doc 12522). Council of Europe. http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-EN.asp?fileid=13103.

Portland Ordinance Prohibit the Acquisition and Use of Face Recognition Technologies by the City of Portland Bureaus (Ordinance) (2020). https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2020/09/Portland-Ordinance-Government-Agency-2.pdf.

Portland Ordinance Prohibit the Use of Face Recognition Technologies by Private Entities in Places of Public Accommodation in the City (Ordinance; add Title 34) (2020). https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2020/09/Portland-Ordinance-Private-Entities-1.pdf.

Ryder, M., & Jones, J. (2020, August 14). Facial recognition technology needs proper regulation. *Ada Lovelace Institute*. https://www.adalovelaceinstitute.org/blog/facial-recognition-technology-needs-proper-regulation/.

S and Marper v the United Kingdom. Nos. 30562/04 and 30566/04. (ECtHR, 4 December 2008). https://rm.coe.int/168067d216.

Setsaas, J.E. (2019). Rethinking customer on-boarding: Why banks should embrace biometrics. *Biometric Technology Today*, *2019*(9).

Shroff, M., & Fordham, A. (2010). "Do You Know Who I Am?" Exploring Identity and Privacy. *Information Polity*, *15*, 299–307.

Snowden, E. (n.d.). Just days left to kill mass surveillance under Section 215 of the Patriot Act. *Reddit*. https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/crglgh2/.

Štitilis, D., & Laurinaitis, M. (2016). Legal regulation of the use of dashboard cameras: Aspects of privacy protection. *Computer Law & Security Review*, *32*(2), 316–326. doi: 10.1016/j.clsr.2016.01.012.

Stock, M. (2019, November 27). R (Bridges) v Chief Constable of South Wales Police and Others [2019] EWHC 2341 (admin): A Summary (Use of Facial Recognition Technology (UK)). *Privacy Law Barrister*. https://privacylawbarrister.com/2019/11/27/r-bridges-v-chief-constable-of-south-wales-police-and-others-2019-ewhc-2341-admin-a-summary-use-of-facial-recognition-technology-uk/.

Svenonius, O. (2012). The Stockholm Security Project: Plural policing, security and surveillance. *Information Polity*, *17*, 35–43.

Texas Business and Commerce Code, Sec. 503.001 (2009). https://texas.public.law/statutes/tex._bus._and_com._code_section_503.001.

Tomlinson, H. (2020, August 17). Case Law: R (on the application of Bridges) v Chief Constable of South Wales, Police use of "automatic facial recognition technology unlawful. *Inforrm*. https://inforrm.org/2020/08/17/case-law-r-on-the-application-of-bridges-v-chief-constable-of-south-wales-police-use-of-automatic-facial-recognition-technology-unlawful-hugh-tomlinson-qc/.

UK Parliament. (n.d.). Primary legislation. *UK Parliament*. https://www.parliament.uk/site-information/glossary/primary-legislation/.

Van Eijk, N., Hoofnagle, C.J., & Kannekens, E. (2017). Unfair commercial practices: A complementary approach to privacy protection. *European Data Protection Law Review*, *3*, 325–337. https://lawcat.berkeley.edu/record/1128108?ln=en.

Veale, M., & Borgesius, F.Z. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, *22*(4) (forthcoming).

Virginia Senate Bill No. 1392 (2021). https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+SB1392H1.

W. P. Willems et al. v. Burgemeester van Nuth et al., Joined Cases C-446/12 to C-449/12. (CJEU, 16 April 2015). https://curia.europa.eu/juris/liste.jsf?num=C-446/12.

Walsh, D., Parisi, J., & Passerini, K. (2017). Privacy as a right or as a commodity in the online world: The limits of regulatory reform and self-regulation. *Electronic Commerce Research*, *17*(2), 185–203. doi: 10.1007/s10660-015-9187-2.

Washington's Engrossed Substitute Senate Bill 6280 (2020).

Webster, C.W.R. (2012). Surveillance as X-ray. *Information Polity*, *17*, 251–265.

Wiewiórowski, W. (2019, October 28). Facial recognition: A solution in search of a problem?. European Data Protection Supervisor. https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en.

Wright, D., & Kreissl, R. (2015). *Surveillance in Europe*. Routledge.

Authors biographies

Paul De Hert's work addresses problems in the area of privacy & technology, human rights and criminal law. A human rights approach combined with a concern for theory is the common denominator of all his work. In his formative years, De Hert studied law, philosophy and religious sciences (1985–1992). After a productive decade of research in areas such as policing, video surveillance, international cooperation in criminal affairs and international exchange of police information, he broadened up his scope of interests and published a book on the European Convention on Human Rights (1998) and defended a doctorate in law in which he compared the constitutional strength of eighteenth and twentieth century constitutionalism in the light of contemporary social control practices ('Early Constitutionalism and Social Control. Liberal Democracy Hesitating between Rights Thinking and Liberty Thinking' (2000, Promoter: Prof. dr. Bart De Schutter (VUB)). De Hert has (had) a broad teaching portfolio: Past: 'Human Rights', 'Legal theory', 'Historical constitutionalism' and 'Constitutional criminal law'. Currently, at Brussels, 'Criminal Law', and 'International and European Criminal Law' and at Tilburg University, 'Privacy and Data Protection'. He is Director of the Research group on human rights (FRC) and Vice-Dean of the Faculty and former Director of the Research group Law Science Technology & Society (LSTS), and of the Department of Interdisciplinary Studies of Law. He is board member of several Belgian, Dutch and (other) international scientific journals such as The Computer Law & Security Review (Elsevier), The Inter-American and European Human Rights Journal (Intersentia) and Criminal Law & Philosophy (Springer). He is co-editor in chief of the Supranational Criminal Law Series (Intersentia) and the New Journal of European Criminal law (Sage). Since 2008 he has edited with Serge Gutwirth, Ronald Leenes and others annual books on data protection law (before Springer, now Hart) that, -judging sales numbers, quotations and downloads, attack a massive readership and have contributed to creating the legal, academic discipline of data protection law. De Hert is now series editor of The Computers, Privacy and Data Protection series, now published by Hart.

Georgios Bouchagiar is a doctoral researcher in criminal law and technology at the University of Luxembourg and the Free University of Brussels. He holds a Law degree (Athens Law School 2011), a Master of Science degree in Information Technology (High Honours, Ionian School of Informatics and Information Science 2018) and a Master of Laws degree in Law and Technology (With Distinction, Tilburg Institute for Law, Technology, and Society 2019). After an 8-year-period of practicing Information Law, he engaged in the academia. Since 2018, his professional experience has included tutoring and lecturing on Information Law and General Principles of Law (Ionian University 2018); research on Information Law and Distributed Ledger Technology (University of Amsterdam/University of Antwerp 2018); and practice on face recognition and spying technologies (Tilburg University 2019).