BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 7 • N° 29 • OCTOBER 2021

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

FACIAL RECOGNITION, VISUAL AND BIOMETRIC DATA IN THE US. RECENT, PROMISING DEVELOPMENTS TO REGULATE INTRUSIVE TECHNOLOGIES

by Paul De Hert* and Georgios Bouchagiar**

Biometric and visual surveillance has taken new forms and sizes. While private and public actors deploy intrusive technologies that are more and more specific, the European Union's approach to the processing of biometric and visual data remains rather abstract and tech-neutral. This working paper discusses various initiatives and regulations of the United States that could become a useful source of inspiration for European audiences. We detect five elements; namely, concreteness of the law when targeting specific technologies, clarity on its scope, precision regarding certain requirements, banning certain technologies or uses of them and organisation of remedies. In our view, these features could be particularly useful and help to protect more effectively biometric and visual data in the European Union.

Key Words: face recognition, visual data, biometric data, surveillance

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html
ISSN N° 2565-9979. This version is for academic use only.

1. Introduction:[1] Biometric and visual surveillance

Biometric and visual surveillance has taken new directions.

Firstly, it became more precise. A prime example is automated fingerprinting analysis that can rapidly deliver more accurate results[2] and significantly reduce the workload of public authorities that may no longer engage in manual processing of scans.[3] ***Second***, it became cheaper and easy to use. For instance, inexpensive DNA processing technologies, readily applicable in combination with other profiling instruments, have boosted and are still boosting surveillance practices.[4] ***Third***, it benefits from function creep: biometric or visual data gathered for purpose or goal A may be further analysed for purpose B. In surveillance contexts, processing-goals can move quietly and stealthily[5] from identification to control and, then, back to identification. The endeavour to identify has been transformed into attempts to monitor, govern or otherwise control individuals via new forms of automated surveillance,[6] which, in turn, pass the baton back to (or become intertwined with novel) identification functions[7] –eg, tasks performed by facial recognition technologies. ***Fourth***, it has become an integral, indispensable part of everyday life. Personal devices, from laptops to iPhones, can be armed with in-screen finger and/or face scanners ready to capture and process their owners' samples.[8] ***Fifth***, it is pushed by public/private partnerships. More and more private entities can gather and analyse data tsunamis, engage in surveillance and build proprietary databases,[9] valuable and, often, vulnerable to cyber-attacks.[10] ***Sixth***, it has become remote, obscure and passive.

* Professor, Law Science Technology & Society, Vrije Universiteit Brussel, paul.de.hert@vub.be; Associate Professor, Tilburg Law School, Department of Law, Technology, Markets, and Society, paul.de.hert@tilburguniversity.edu.
** Doctoral Researcher in Criminal Law and Technology, Faculty of Law, Economics and Finance, University of Luxembourg, georgios.bouchagiar@uni.lu; Law, Science, Technology & Society, Free University of Brussels, georgios.bouchagiar@vub.be.
Supported by the Luxembourg National Research Fund (FNR) (PRIDE17/12251371).
1 The authors would like to thank Stephanie Rossello for her constructive criticism on this paper.
2 A good example is Lifescan for digital processing of fingerprints: Herwig Willaert, 'Lifescan-Apparatuur Biedt Heel Wat Voordelen: Politie Neemt Digitaal Vingerafdrukken' (***Nieuwsblad***, 8 March 2006) <https://www.nieuwsblad.be/cnt/g0rp722p> accessed 6 September 2021. For contemporary mobile scanning applications that are said to be in the agenda, see: Wired, 'UK police are now using fingerprint scanners on the streets to identify people in less than a minute' (***Wired***, 10 February 2018) <https://www.wired.co.uk/article/uk-police-handheld-fingerprint-scanner-database-biometric-security> accessed 6 September 2021.
3 See for instance: Nancy Singla, Manvjeet Kaur and Sanjeev Sofat, 'Automated Latent Fingerprint Identification System: A Review' (2020) 309 Forensic Science International 1, 2; Gemalto, 'Automated Fingerprint Identification System (AFIS) – A Short History' (***Gemalto***, 28 January 2020) <https://www.gemalto.com/govt/biometrics/afis-history> accessed 6 September 2021.
4 Yves Moreau, 'Crack Down on Genomic Surveillance' (2019) 576 Nature 36.
5 Among its many meanings, 'creep' in 'function creep' can refer to a move, which is 'stealthy, eluding (or intended to elude) observation'. For an analysis see: Bert-Jaap Koops, 'The Concept of Function Creep' (2021) 13(1) Law, Innovation and Technology (forthcoming).
6 Avi Marciano, 'Reframing- Biometric Surveillance: From a Means of Inspection to a Form of Control' (2019) 21 Ethics and Information Technology 127, 130ff.
7 This can be the case with centralised databases that are designed for visa- or asylum-related purposes (involving identification), yet that may be directed toward the fight against terrorism (entailing both control and identification). To Tzanou, this is the 'competence creep'; Maria Tzanou, 'The EU as an Emerging 'Surveillance Society': The Function Creep Case Study and Challenges to Privacy and Data Protection' (2010) 4(3) Vienna Journal on International Constitutional Law 407, 415. For function creep and other risks in the context of forensic DNA databases, see: Forensic Genetics Policy Initiative, ***Establishing Best Practice for Forensic DNA Databases*** (Forensic Genetics Policy Initiative, September 2017) <http://dnapolicyinitiative.org/wp-content/uploads/2017/08/BestPractice-Report-plus-cover-final.pdf> accessed 6 September 2021.
8 See for instance: Jim Nash, 'New Apple Patent May Mean OLED Fingerprint Biometrics for iPhones, Laptops' (*Biometric Update*, 25 January 2020) <https://www.biometricupdate.com/202001/new-apple-patent-may-mean-oled-fingerprint-biometrics-for-iphones-laptops> accessed 6 September 2021.
9 Madhumita Murgia, 'Microsoft Quietly Deletes Largest Public Face Recognition Data Set' (*Financial Times*, 6 June 2019) <https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2> accessed 6 September 2021.
10 Byron Mühlberg, 'Clearview AI Data Breach Exposes Facial Recognition Firm's Client List' (*CPO Magazine*, 11 March 2020) <https://www.cpomagazine.com/cyber-security/clearview-ai-data-breach-exposes-facial-recognition-firms-client-list/> accessed 6 September 2021.

The processing of behavioural data (data about the way one texts, talks, walks, coughs or sleeps) can make surveillance remote. Distance can then obfuscate sample-taking that requires neither awareness nor participation from the part of the watched.[11]

These developments transform the ***what*** and the ***who*** of our culture of control.[12] A new culture of control develops in the sense that what is expressed (eg, texted or acted upon), -including ***anything*** from temperature and heartbeat to coughing-, is now worthy and capable of being recorded. The result is a culture of banalised monitoring, where the processing of such ***anything*** is routinised because of everyone's (state, the private actors' and the people) engagement in surveillance.[13] Moreover, there is a new 'who'. Those under surveillance are not (only) criminals; any citizen, any individual can be asked to undergo banalised surveillance, for it is for her own, as well as everyone's own, good.[14]

Focusing on the protection of personal data, the European legislator has opted for a broad regime to protect facial, visual and biometric data,[15] and to frame biometric and visual surveillance. The 2016 EU General Data Protection Regulation (the 'GDPR') is an ***omnibus*** act with general principles and characterised by technological neutrality. It mainly speaks of data in general and hardly goes into the details of visual and biometric data or surveillance. This law defines biometric data as '***personal data*** resulting from ***specific technical processing*** relating to the ***physical, physiological or behavioural characteristics*** of a natural person, which ***allow or confirm the unique identification*** of that natural person' (own emphasis).[16]

11 Lucas Introna and Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues* (The Center for Catastrophe Preparedness & Response 2009) 10 <https://nissenbaum.tech.cornell.edu/papers/facial_recognition_report.pdf> accessed 6 September 2021.

12 David Lyon, 'Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity' (2017) 11 International Journal of Communication 824, 827 citing David Garland, ***The Culture of Control: Crime and Social Order in Contemporary Society*** (University of Chicago Press 2001).

13 For a discussion on people's familiarisation with surveillance practices, see: William Webster, 'Surveillance as Xray: Understanding the Surveillance State' in William Webster and others (eds), ***Living in Surveillance Societies: The State of Surveillance*** (University of Stirling 2013) 14, 22. For the recent ban by the Federal Trade Commission on 'SpyFone', a technology enabling allegedly illegal surveillance of the people and by the people, see: Hunton Andrews Kurth, 'FTC Bans Stalkerware App Company from the Surveillance Business and Orders Company to Delete Any Illegally Collected Information' (Hunton Privacy Blog, 8 September 2021) <https://www.huntonprivacyblog.com/2021/09/08/ftc-bans-stalkerware-app-company-from-the-surveillance-business-and-orders-company-to-delete-any-illegally-collected-information/#more-20732> accessed 9 September 2021.

14 These new forms of banalised surveillance have been exemplified by the coronavirus-outbreak. In an influential article discussing surveillance practices that have (or could have) followed (or may follow) the coronavirus-pandemonium, Harari warns about the wide array of biological patterns that are now processable and, hence, subjectable to various forms of exploitation. Yuval Noah Harari, 'Yuval Noah Harari: The World After Coronavirus' (***Financial Times***, 20 March 2020) <https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75> accessed 6 September 2021 ('(…) It is crucial to remember that anger, joy, boredom and love are biological phenomena just like fever and a cough. The same technology that identifies coughs could also identify laughs. If corporations and governments start harvesting our biometric data en masse, they can get to know us far better than we know ourselves, and they can then not just predict our feelings but also manipulate our feelings and sell us anything they want — be it a product or a politician'). Harari argues that risks of spreading of the disease presented citizens of the world with major dilemmas: 'totalitarian surveillance' versus 'citizen empowerment'; and 'nationalist isolation' versus 'global solidarity'. Yuval Noah Harari, 'Yuval Noah Harari: The World After Coronavirus' (n 14). Advocating for protection of both collective and individual rights (public health and privacy), the author recommends, among others, that states grant citizens powers (eg, offer instruments to report events of disease-outbreaks), coordinate their strategies (instead of isolating themselves) or communicate effective measures (instead of individually trying to reinvent the wheel). Exceptional circumstances, such as the pandemic, can indeed threaten public health in unprecedented ways and may, for this reason, justify temporary measures resulting in proportionate limitations to non-absolute rights, such as the right to privacy or the protection of personal dataIt is, however, worth reminding the saying 'ουδέν μονιμότερον του προσωρινού' meaning 'nothing is more permanent than the temporary' and referring to temporary situations that are extended (due to inaction or negligence or) intentionally to serve concrete interests. Potential perpetuation of exceptional measures and extreme forms of surveillance can raise many questions. And it seems that Europe has not yet come close to guaranteeing that, if/when public health is no longer threatened to the corona-degree and at its global level, surveillance-databases will stop devouring 'anything', all data making them ever-growing and even more opaque, more like black holes than black boxes.

15 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.

16 GDPR, art 4(14).

In this context, biometric data are, first of all, ***personal data*** (ie, 'information relating to an identified or identifiable natural person'),[17] but also ***sensitive data***. This second denominator implies a more strictly regulated regime within the GDPR: processing of such information, aimed at unique identification, is in principle prohibited.[18] This might sound firm, but then follows in the GDPR a long list of (ten) exceptions that weakens this prohibition,[19] including ***explicit*** consent and ***data that have already been manifestly made public by the data subject***.[20] Furthermore, the data subject, in general, enjoys the right: to information;[21] to access her/his data;[22] to rectification (regarding inaccurate data);[23] to erasure of her/his data;[24] to restrict processing;[25] to data portability;[26] to object to processing;[27] or not to be subjected to automated decision-making.[28] Several duties, including the obligation to conduct impact assessments, are imposed on the 'data controller' (he or she who processes –in the sense of deciding upon the means and the purposes of the processing of– personal data of others) to safeguard compliance with these principles.[29]

17 GDPR, art 4(1). Then, there are three cumulative prerequisites for personal data to become biometric: first, ***specific technical processing*** (ie, in a specific manner resulting in unique identification); second, processing relating to the ***physical, physiological or behavioural characteristics*** (such as face images or sleeping patterns); and, third, such data must ***allow or confirm the unique identification.***

18 GDPR, art 9(1) ('(…) the processing of (…) biometric data for the purpose of uniquely identifying a natural person (…) shall be prohibited(…)').

19 GDPR, art 9(2) ('(…) (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; (e) processing relates to personal data which are manifestly made public by the data subject; (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; (g) 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; (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on 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').

20 Do we manifestly make our facial data public when walking on the street or posting images on Facebook? On the exceptions-list legitimising the (otherwise unlawful) processing, it is noted that the GDPR allows national legislators to introduce further exceptional conditions. GDPR, art 9(4) ('(…) Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health').

21 GDPR, arts 13-14.

22 GDPR, art 15.

23 GDPR, art 16.

24 GDPR, art 17.

25 GDPR, art 18.

26 GDPR, art 20.

27 GDPR, art 21.

28 GDPR, art 22.

29 Moreover, data controllers must comply with general principles of data processing; namely, the principle of 'lawfulness, fairness and transparency', 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation', 'integrity and confidentiality' and 'accountability. GDPR, art 5.

Aside from the GDPR, there is the 2016 Law Enforcement Directive (the 'LED') applicable to the processing of personal data by competent authorities working in the area of police and criminal justice.[30] This Directive, like the GDPR, says nothing particular about visual data (so it can be processed by the police) and is a bit more strict for the processing of biometric data: the police can process this data 'where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only: (a) where authorised by Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; or (c) where such processing relates to data which are manifestly made public by the data subject'.[31] These permissive terms explain the rise of CCTV in the public spaces of Europe and the flirtation by local police forces all over Europe to implement facial recognition systems.

To sum up, the EU legal framework appears well organised and structured, addressing both private and public actors. However, its general provisions and its technological neutrality do not always allow for the effective regulation of specific technologies and a clear 'no' against facial recognition is not included.

This working paper discusses the United States (US) regulatory approaches to visual data and/or biometrics (including facial recognition), with a view to observing certain elements and submitting some ideas that could inspire Europeans. As the analysis will demonstrate, the EU could draw inspiration from concreteness, clarity and precision of certain US legal provisions, as well as banning-techniques and practical remedy-structure.

We took stock of the following US-initiatives:[32]

- at federal level, the proposed 2019 ***Commercial Facial Recognition Privacy Act*** (the '2019 CFRP Act'),[33] the proposed 2020 ***Facial Recognition and Biometric Technology Moratorium Act*** (the 'FRBT Moratorium Act'),[34] the proposed 2020 ***National Biometric Information Privacy Act*** (the 'NBIPA')[35] and the proposed Data Protection Act of 2021;[36]

30 In general, the LED uses a GDPR-terminology; it applies to the processing for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; and it appears police-friendly. For instance, the principle of transparency is absent, although it may be desirable even in a LED context. The use of secret technologies by the police may be justified to effectively fight against crime. No one would want 'would-be lawbreakers' to be able to evade law enforcement. Yet, secrecy impairs several equally desirable goals: people need know that the police are watching; and the police must be subject to democratic oversight and laws that are public, as well as enjoy the benefit of outside feedback and expert criticism. See Johnathan Manes, 'Secrecy & Evasion in Police Surveillance Technology' (2019) 34 Berkeley Technology Law Journal 503, 544 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3265072> accessed 6 September 2021.

31 LED, art 10.

32 This contribution only discusses US texts that were available to the authors. Literature has reported a number of face recognition-bans at town- or city-level in the US. However, the official text of these local laws was, at the time of writing, inaccessible. For an overview, see Jameson Spivack and Clare Garvie, 'A Taxonomy of Legislative Approaches to Face Recognition in the United States' in Amba Kak (ed), *Regulating Biometrics: Global Approaches and Urgent Questions* (AI NOW 2020) 86, 89-90 (referring to, among others, cities and towns in California and Massachusetts) <https://ainowinstitute.org/regulatingbiometrics.pdf> accessed 6 September 2021.

33 116th Congress, 1st Session, S 847 'To prohibit certain entities from using facial recognition technology to identify or track an end user without obtaining the affirmative consent of the end user, and for other purposes' ('Commercial Facial Recognition Privacy Act of 2019') <https://www.congress.gov/bill/116th-congress/senate-bill/847/text> accessed 6 September 2021.

34 116th Congress, 2nd session, S 4084 'To prohibit biometric surveillance by the Federal Government without explicit statutory authorization and to withhold certain Federal public safety grants from State and local governments that engage in biometric surveillance'('Facial Recognition and Biometric Technology Moratorium Act of 2020') <https://www.congress.gov/116/bills/s4084/BILLS-116s4084is.pdf> accessed 6 September 2021. See also 116th Congress, 2nd Session, H R 7356 'To prohibit biometric surveillance by the Federal Government without explicit statutory authorization and to withhold certain Federal public safety grants from State and local governments that engage in biometric surveillance'<https://www.congress.gov/116/bills/hr7356/BILLS-116hr7356ih.pdf> accessed 6 September 2021.

35 116th Congress, 2nd Session, 'To regulate the collection, retention, disclosure, and destruction of biometric information, and for other purposes'('National Biometric Information Privacy Act of 2020') <https://www.merkley.senate.gov/imo/media/doc/20.08.04%20National%20Biometric%20Information%20Privacy%20Act.pdf> accessed 6 September 2021.

36 Data Protection Act of 2021, 117th Congress 1st Session <https://www.gillibrand.senate.gov/imo/media/doc/DPA%20Bill%20Text.pdf> accessed 6 September 2021.

- at state level, the 2008 ***Illinois Biometric Information Privacy Act*** (the 'IBIPA'),[37] Texas Business and Commerce Code Sec 503.001 'Capture or Use of Biometric Identifier' (2009),[38] California's Assembly Bill No 1215 (2019),[39] its proposed 2020 ***Genetic Information Privacy Act*** (the 'GIPA')[40] and California Privacy Rights Act of 2020 ('CPRA'),[41] Washington's Engrossed Substitute Senate Bill 6280 (2020),[42] Indiana's House Bill 1238 (2020),[43] New Jersey's Assembly Bill 989 (2020),[44] New York's Assembly Bill A6787D (2020)[45] and Virginia's proposed Senate Bill 1392 (2021);[46] and,
- at city level, Portland's two separate ordinances on the prohibition of face recognition technologies[47] and Baltimore's ordinance banning the use of face recognition by private actors, as well as by the city of Baltimore.[48]

In what follows, we will sketch the US approach to visual data and/or biometrics at federal, state and city level (sections 2 to 5). We will then identify certain elements, namely concreteness/clarity/precision of certain US legal regulations/initiatives, banning-techniques and practical remedy-organisation (sections 6 to 10). Finally, we will conclude with some insights that could be drawn from the US regime (section 11), with additional critical remarks on the recent Proposal of the European Commission for a Regulation on Artificial Intelligence (section 12).

2. Privacy and data protection in the US: piece-meal, multilevel and technology-specific

General

Before proceeding to the analysis, two remarks need be made regarding the US legal regime: one referring to the US Privacy Act that is primarily aimed at the government (and saying nothing for private parties); and another one on the Fair Information Practice Principles (the 'FIPP'), ie soft law that has long been influencing data protection-related regulations.

37 740 Ill Comp Stat Ann 14/ <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57> accessed 6 September 2021.
38 Texas Business and Commerce Code, Sec 503.001 'Capture or Use of Biometric Identifier'<https://texas.public.law/statutes/tex._bus._and_com._code_section_503.001> accessed 6 September 2021.
39 Assembly Bill No 1215, Chapter 579, 'An act to add and repeal Section 832.19 of the Penal Code, relating to law enforcement' (2019) <https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1215> accessed 6 September 2021.
40 Senate Bill 980, 'Privacy: genetic testing companies'<https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200SB980> accessed 6 September 2021.
41 The California Privacy Rights Act of 2020 <https://vig.cdn.sos.ca.gov/2020/general/pdf/topl-prop24.pdf> accessed 6 September 2021.
42 WA Engrossed Subst SB 6280 (2020) <http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf> accessed 6 September 2021.
43 IN HB 1238 (2020) <http://iga.in.gov/legislative/2020/bills/house/1238> accessed 6 September 2021.
44 NJ AB 989 (2020) <https://www.njleg.state.nj.us/2020/Bills/A1000/989_I1.PDF> accessed 6 September 2021.
45 New York's Assembly Bill A6787D <https://legislation.nysenate.gov/pdf/bills/2019/a6787d> accessed 6 September 2021.
46 Virginia's Senate Bill No 1392 <https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+SB1392H1> accessed 6 September 2021.
47 Portland's Ordinance 'Prohibit the use of Face Recognition Technologies by Private Entities in Places of Public Accommodation in the City (Ordinance; add Title 34)'('Portland's first Ordinance') <https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2020/09/Portland-Ordinance-Private-Entities-1.pdf> accessed 6 September 2021; and Portland's Ordinance 'Prohibit the Acquisition and Use of Face Recognition Technologies by the City of Portland Bureaus (Ordinance)'('Portland's second Ordinance') <https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2020/09/Portland-Ordinance-Government-Agency-2.pdf> accessed 6 September 2021.
48 Ordinance 'Surveillance Technology in Baltimore'.

Firstly, the US have long been following a piecemeal approach to data regulation, with laws such as the Fair Credit Reporting Act; the Electronic Communications Privacy Act; the Cable Communications Policy Act, the Video Privacy Act and the US Privacy Act.[49] The latter contains a code of fair information practices that governs the collection, maintenance, use and dissemination of information about individuals that is maintained in systems of records by federal agencies. The Act prohibits the disclosure of a record about an individual, unless the disclosure is pursuant to one of the statutory exceptions; provides individuals with some data subject rights; and sets forth various agency record-keeping requirements. The US Privacy Act, with its focus on 'records', rather than on data, is far beyond the GDPR in terms of scope and precision and does not say much on law enforcement processing, a situation that partly explains why firms, like Clearview AI, have been able to build up an impressive facial recognition market in the States.

Secondly, there are the Fair Information Practice Principles (the 'FIPP').[50] These principles that are at the heart of the US Privacy Act of 1974 were reflected in many state laws.[51] In the nineteen-nineties, the US Federal Trade Commission (the 'FTC') issued its own FIPP-version to protect privacy in online contexts. These principles refer to notice/awareness, choice/consent, access/participation, integrity/security and enforcement/redress.[52] It is worth noting that the FIPP have been subjected to critique due to, among others, their limited (or not precisely defined) scope,[53] their failure to cope with technological developments[54] or their lack of clarity (for example, how the consent-model can apply to health contexts where sensitive data can be shared with third parties).[55] Nevertheless, the FIPP can be mirrored in recent recommendations, regarding commercial or aviation-related implementations of face recognition technology, published by consumer-protection organisations and other entities.[56] To some commentators, such recommendations are insufficient; a specific federal law is needed to render soft laws and proposals enforceable in practice.[57]

All of the above developments may have contributed to the introduction of the US federal initiatives analysed below. Before discussing these, let us point at the recent proposal for a Data Protection Act.

49 Fair Credit Reporting Act, 15 USC § 1681; Electronic Communications Privacy Act, 18 USC § 2510; Cable Communications Policy Act, 47 USC § 551; Video Privacy Act, 18 USC § 2710. For further examples and a detailed discussion on US privacy-related laws, see Gabriela Zanfir-Fortuna, 'America's 'Privacy Renaissance': What to Expect under a New Presidency and Congress: A Deep Dive into US Privacy Legislation and Implications for US-EU-UK Relations' (Ada Lovelace Institute, 17 December 2020) <https://www.adalovelaceinstitute.org/blog/americas-privacy-renaissance/> accessed 6 September 2021.

50 See in more detail Orla Lynskey, ***The Foundations of EU Data Protection Law*** (Oxford University Press 2015) 17; Gabriela Zanfir-Fortuna, 'America's 'Privacy Renaissance': What to Expect under a New Presidency and Congress' (n 49).

51 US Department of Homeland Security, 'Privacy Policy Guidance Memorandum' (29 December 2008) <https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf> accessed 6 September 2021.

52 FTC, ***Privacy Online: A Report to Congress*** (Federal Trade Commission, June 1998) 7ff <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf> accessed 6 September 2021. See also the 2000 version as modified in 2007: FTC, 'Fair Information Practice Principles' <https://web.archive.org/web/20090205180646/http://ftc.gov/reports/privacy3/fairinfo.shtm> accessed 6 September 2021.

53 For instance, other FIPP-versions have included more principles, like transparency and data quality. See among others US Department of Homeland Security, 'Privacy Policy Guidance Memorandum' (n 51).

54 See for instance David Annecharico, 'Online Transactions: Squaring the Gramm-Leach-Bliley Act Privacy Provisions with FTC Fair Information Practice Principles' (2002) 6 North Carolina Banking Institute 637.

55 Herman Tavani and Maria Bottis, 'The Consent Process in Medical Research Involving DNA Databanks: Some Ethical Implications and Challenges' (2010) 40(2) ACM SIGCAS Computers and Society 11.

56 'Privacy Best Practice Recommendations for Commercial Facial Recognition Use'<https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf> accessed 6 September 2021.

57 For a discussion, see Letícia Silveira Tavares, 'Regulating the Imbalance of Power Created by Facial Recognition'(2020) 163 Privacy Laws & Business International Report 27: 'In the US, consumer advocates have issued, in conjunction with the national Telecommunication and Information Administration (nTIA), facial recognition technology best practice recommendations (…) for the private sector. However, it has been argued that without a federal law, "the guidelines remain simply unenforceable suggestions." Following on from the guidelines, another move towards a better use of FRT was made by the US Privacy and Civil Liberties Oversight Board. It has approved a review of the use of facial recognition and other biometric technologies in aviation security. The board outlined that it would particularly examine how facial recognition and other biometric technologies are used to verify individuals' identity in situations such as flight booking and baggage claiming'.

The proposed Data Protection Act of 2021

Initially introduced in 2020 (as Data Protection Act of 2020),[58] this Act aims at establishing an independent federal agency –the Data Protection Agency– with a view to addressing high risk data practices, as well as the 'collection, processing, or sharing of personal data'.[59]

This Act refers to personal data in general. Biometrics are included in this concept; that is all too familiar to European ears. The proposal defines biometric data as 'information regarding the physiological or biological characteristics of an individual that may be used, singly or in combination with each other or with other identifying data, to establish the identity of an individual'.[60] Moreover, it treats biometric data as a protected class and the processing of biometric data as a high risk data practice.[61]

The key novelty of the Act appears to be the establishment of the above federal Data Protection Agency that would (among others): enact and enforce data protection provisions, investigate complaints or initiate civil actions to guarantee control of individuals over their personal data; promote fair competition; advise public actors on contemporary issues regarding technologies and personal data; supervise data aggregators (meaning persons processing significant amounts of data primarily for commercial purposes);[62] make publicly available a list of data aggregators, who process 'personal data of more than 10,000 persons or households';[63] or report to the Federal Trade Commission on privacy and data protection implications of any merger entailing certain data risks.[64] Importantly, the Act would in principle prohibit data aggregators and service providers from (among others) committing 'unlawful, unfair, deceptive, abusive, or discriminatory acts or practices', denying access to records or failing to keep records or to report to

58 Data Protection Act of 2020, 116th Congress, 2d Session <https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/02/Data-Protection-Act-2020.pdf> accessed 6 September 2021.

59 Data Protection Act of 2021, 117th Congress 1st Session <https://www.gillibrand.senate.gov/imo/media/doc/DPA%20Bill%20Text.pdf> accessed 6 September 2021.

60 Data Protection Act of 2021, section 2(4) ('(…) (B) includes— (i) genetic data; (ii) imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted; (iii) keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information; and (iv) any mathematical code, profile, or algorithmic model derived from information regarding the physiological or biological characteristics of an individual. (C) does not include information captured from a patient in a health care setting for a medical purpose or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996 (…) (D) does not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening').

61 Data Protection Act of 2021, section 2(21) ('(…) The term ''protected class'' means the actual or perceived race, color, ethnicity, national origin, religion, sex, gender, gender identity or expression, sexual orientation, familial status, biometric information, genetic information, or disability of an individual or a group of individuals'); section 2(11) ('(…) The term ''high-risk data practice'' means an action by a data aggregator that involves (…) (G) any processing of biometric information for the purpose of uniquely identifying an individual, with the exception of one-to-one biometric authentication').

62 Data Protection Act of 2021, section 2(6) ('(…) The term ''data aggregator'' (…) (A) means any person that collects, uses, or shares, in or affecting interstate commerce, an amount of personal data that is not de minimis, as well as entities related to that person by common ownership or corporate control; and (B) does not include an individual who collects, uses, or shares personal data solely for non-commercial reasons').

63 Data Protection Act of 2021, section 11(c) ('(…) The Agency shall maintain a publicly accessible list of data aggregators that collect, process, or share personal data of more than 10,000 persons or households, and the permissible purposes for which the data aggregators purport to collect personal data').

64 Data Protection Act of 2021, section 11(d) ('(…) The Agency shall conduct a review and submit to the Federal Trade Commission and Department of Justice a report on the privacy and data protection implications of (1) any merger involving a data aggregator described in subsection (a); or (2) any merger that proposes the transfer of personal data of 50,000 or more individuals').

the Agency, as well as re-identifying or trying to re-identify 'an individual, household, or device from anonymized data'.[65]

3. Biometric and visual surveillance laws at US federal level

The proposed 2019 Commercial Facial Recognition Privacy Act

The proposed Commercial Facial Recognition Privacy Act (the 'CFRPA' or '2019 CFRP Act') was introduced in March 2019 to avoid abuse by (primarily) private operators of facial recognition technology[66] to identify individual users without their consent.[67] Governmental actors (federal, state or local) and law enforcement, national security and intelligence agencies are exempted.[68]

The Act in principle prohibits the use by the 'controller' of facial recognition technology for the purpose of collecting facial recognition data, unless there is an opt-in (affirmative consent) and (where possible) a notice providing intelligible information about the involvement of the technology.[69] Furthermore, it prohibits the controller from using such technologies for discrimination purposes and for purposes other than those of the initial processing, as well as from sharing facial recognition data with third parties without affirmative consent.[70] The Act also requires that controllers engage in 'meaningful human review' before

65 Data Protection Act of 2021, section 12 ('(…) It shall be unlawful for— (1) any data aggregator or service provider to commit any act or omission in violation of this Act, Federal privacy law, or any rule or order issued by the Agency under this Act; (2) any data aggregator or service provider to commit any unlawful, unfair, deceptive, abusive, or discriminatory acts or practices in connection with the collection, processing, or sharing of personal data; (3) any data aggregator or service provider to fail or refuse as required by this Act or Federal privacy law, or any rule or order issued by the Agency thereunder— (A) to permit access to or copying of records; (B) to establish or maintain records; or (C) to make reports or provide information to the Agency; (4) any person to knowingly or recklessly provide substantial assistance to a data aggregator or service provider in violation of this Act or Federal privacy law, or any rule or order issued thereunder, and notwithstanding any provision of this Act, the provider of such substantial assistance shall be deemed to be in violation of this Act or Federal privacy law to the same extent as the person to whom substantial assistance is provided; or (5) any person, data aggregator, or service provider to re-identify, or attempt to re-identify, an individual, household, or device from anonymized data, unless such person, data aggregator, or service provider is conducting authorized testing to prove personal data has been anonymized').

66 CFRPA, section 2(5): '*facial recognition technology* means 'technology that analyzes facial features in still or video images; and (…) is used to assign a unique, persistent identifier; or (…) for the unique personal identification of a specific individual'.

67 CFRPA, section 2(6): '*facial recognition data* means any unique attribute or feature of the face of an end user that is used by facial recognition technology to assign a unique, persistent identifier or for the unique personal identification of a specific individual.

68 CFRPA, section 2(3).

69 This Act requires consent to data processing be of an affirmative nature and involve an individual, voluntary and explicit agreement (CFRPA, section 2(1)); and it treats the controller as the person determining the purposes and means of 'facial recognition data' processing (CFRPA, section 2(2)). See also CFRPA, section 3(a)(1): 'Except as provided in subsection (e), it shall be unlawful for a controller to knowingly (1) use facial recognition technology to collect facial recognition data, unless the controller (A) obtains from an end user affirmative consent in accordance with subsection (b); and (B) to the extent possible, if facial recognition technology is present, provides to the end user (i) a concise notice that facial recognition technology is present, and, if contextually appropriate, where the end user can find more information about the use of facial recognition technology by the controller; and (ii) documentation that includes general information that explains the capabilities and limitations of the facial recognition technology in terms that end users are able to understand'. Section 3(e) of the CFRPA provides for exceptions related to, among others, personal file management (if not aimed at uniquely identifying individuals), identification of public figures (in journalistic contexts serving the public interest or in copyrighted material for theatrical purposes) or cases of emergency involving serious danger.

70 CFRPA, section 3(a)(2-4): 'Except as provided in subsection (e), it shall be unlawful for a controller to knowingly (2) use the facial recognition technology to discriminate against an end user in violation of applicable Federal or State law; (3) repurpose facial recognition data for a purpose that is different from those presented to the end user under paragraph (1)(A); or (4) share the facial recognition data with an unaffiliated third party without affirmative consent that is separate from the affirmative consent required under paragraph (1)(A)'.

taking decisions that can significantly affect an individual.[71] It, moreover, demands audits by independent parties, who must be enabled to check for bias and inaccuracies of facial recognition technologies that are provided as online services.[72]

Any breach of the provisions related to prohibited conducts is classified as unfair or deceptive act or practice of the Federal Trade Commission Act.[73] Hence, the CFRPA offers a civil remedy-route.[74]

The proposed 2020 Facial Recognition and Biometric Technology Moratorium Act

The proposed Facial Recognition and Biometric Technology Moratorium Act (the 'FRBT Moratorium Act') of 2020 can be seen as a prime example of so-called 'directive moratoria', halting the use of a technology while guiding the legislator to take concrete steps.[75] It was introduced in June 2020 with a view to prohibiting the use by the federal government of face recognition or other biometric technology until the law expressly allows such a use.

This Act addresses federal actors. It prohibits any biometric surveillance by the federal government,[76] save where the law explicitly authorises it, provided such a law is sufficiently precise (for instance, as to authorised actors, rules on data processing, accuracy assessments or safeguards for due process, privacy and free speech).[77]

The FRBT Moratorium Act also provides for remedies protecting persons aggrieved from biometric surveillance by the federal government. More concretely, it grants to any individual aggrieved the right to

71 CFRPA, section 3(c): 'A controller, and the processor if applicable, shall employ meaningful human review prior to making any final decision based on the output of facial recognition technology if the final decision (1) may result in a reasonably foreseeable and material physical or financial harm to an end user; or (2) may be unexpected or highly offensive to a reasonable end user'.

72 CFRPA, section 3(d): 'A covered entity that makes a facial recognition technology available as an online service shall make available an application programming interface to enable at least 1 third party that is legitimately engaged in independent testing to conduct reasonable tests of the facial recognition technology for accuracy and bias'.

73 CFRPA, section 4(a): 'A violation of section 3 shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B))'.

74 Even though unfair or deceptive acts or practices could result in violation of a criminal provision and despite the fact that some states have introduced criminal remedies for such acts/practices (for extreme violations), the Federal Trade Commission Act as well as most state laws on unfair or deceptive acts or practices primarily protect the consumer by enabling enforcement via civil courts. See in more detail Carolyn Carter, *A 50-State Report on Unfair and Deceptive Acts and Practices Statutes* (National Consumer Law Center Inc, February 2009) 6.

75 A similar technique used by the US is the 'time-bound moratorium' that stops the use of a technology for a certain amount of time. Such techniques have been reported by literature devoted to face recognition. For an overview, see Jameson Spivack and Clare Garvie, 'A Taxonomy of Legislative Approaches to Face Recognition in the United States' (n 32) 89-92.

76 FRBT Moratorium Act, section 3(a): 'it shall be unlawful for any Federal agency or Federal official, in an official capacity, to acquire, possess, access, or use in the United States (1) any biometric surveillance system; or (2) information derived from a biometric surveillance system operated by another entity'. Under section 2 of the above Act: '(1) '*biometric surveillance system* means any computer software that performs facial recognition or other remote biometric recognition in real time or on a recording or photograph (3) *facial recognition* means an automated or semi-automated process that (…) assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating surveillance information about an individual based on the physical characteristics of the individual's face; or (…) logs characteristics of an individual's face, head, or body to infer emotion, associations, activities, or the location of an individual (4) *Federal official* means any officer, employee, agent, contractor, or subcontractor of the Federal Government '.

77 FRBT Moratorium Act, section 3(b): '(t)he prohibition set forth in subsection (a) does not apply to activities explicitly authorized by an Act of Congress that describes, with particularity (1) the entities permitted to use the biometric surveillance system, the specific type of biometric authorized, the purposes for such use, and any prohibited uses; (2) standards for use and management of information derived from the biometric surveillance system, including data retention, sharing, access, and audit trails; (3) auditing requirements to ensure the accuracy of biometric surveillance system technologies, standards for minimum accuracy rates, and accuracy rates by gender, skin color, and age; (4) rigorous protections for due process, privacy, free speech and association, and racial, gender, and religious equity; and (5) mechanisms to ensure compliance with the provisions of the Act'.

bring her/his case against the federal government; and it authorises state officers to initiate civil proceedings on behalf of the people, where their interests are reasonably believed to have been or be at risk or prejudiced.[78]

The proposed 2020 National Biometric Information Privacy Act

The proposed National Biometric Information Privacy Act (the 'NBIPA' or 'NBIP Act') was introduced in August 2020 with a view to tackling biometric data exploitation by private entities.[79] It covers ***biometric information***,[80] as well as ***biometric identifiers*** ('uniquely identifying information', such as retina, iris scan or voice/face/finger/palm-prints).[81]

The addressees of the NBIP Act are private entities.[82] In general, these entities are bound by the duty to make publicly available their written policy on retention and destruction of biometric information and biometric identifiers.[83] Moreover, they are prohibited from obtaining such biometric data, unless they do so in the course of offering a service or (the obtaining) serves concrete business-purposes included in the above policy; but this exception requires that the individual concerned has already been informed and has consented.[84] Furthermore, the Act forbids these entities to exploit for profit biometric information and biometric identifiers;[85] and to (re)disseminate such information and identifiers, save where the individual at issue has consented or where the (re)disclosure serves the completion of a transaction requested/

78 See FRBT Moratorium Act, section 3(c)(2): '(A) A violation of this section constitutes an injury to any individual aggrieved by a violation of this Act (B) An individual described in subparagraph (A) may institute proceedings against the Federal Government whose official is alleged to have violated this section for the relief described in subparagraph (D) in any court of competent jurisdiction (C) (t)he chief law enforcement officer of a State, or any other State officer authorized by law to bring actions on behalf of the residents of a State, may bring a civil action, as parens patriae, on behalf of the residents of that State in an appropriate district court of the United States to enforce this Act, whenever the chief law enforcement officer or other State officer has reason to believe that the interests of the residents of the State have been or are being threatened or adversely affected by a violation of this Act'. Furthermore, the Act treats information gathered in violation of its provisions as inadmissible in any type of investigation or proceeding. See FRBT Moratorium Act, section 3(c). And it prohibits federal funding regarding biometric surveillance systems, except where relevant state or local governments have implemented laws 'substantially' equivalent to those suggested by the Act. See FRBT Moratorium Act, section 3(e).

79 For an overview, see Hunton Andrews Kurth, 'Senate Bill Limits Corporate Use of Facial Recognition' (Hunton Privacy Blog, 6 August 2020) <https://www.huntonprivacyblog.com/2020/08/06/senate-bill-limits-corporate-use-of-facial-recognition/> accessed 6 September 2021.

80 The term 'biometric information' (the subject matter of this Act, according to its title) is not defined in the text of that Act. Moreover, in this Act, biometric information is distinguished from 'biometric identifiers'. See for example NBIPA, section 3(a)(1): 'any private entity in possession of *biometric identifiers or biometric information* concerning an individual') (own emphasis); section 3(b)(1): 'A private entity may not (…) obtain a person's or a customer's *biometric identifier or biometric information')* (own emphasis).

81 NBIPA, section 2(1): 'biometric identifier includes (…) a retina or iris scan (…) a voiceprint (…) a faceprint (…) fingerprints or palm prints (…) any other uniquely identifying information based on the characteristics of an individual's gait or other immutable characteristic of an individual'.

82 NBIPA, section 2(3): 'The term private entity means any individual, partnership, corporation, limited liability company, association, or other group, however organized; and (…) does not include any Federal, State, or local government agency or academic institution'.

83 NBIPA, section 3(a)(1): 'any private entity in possession of biometric identifiers or biometric information concerning an individual shall develop and make available to the public a written policy establishing a retention schedule and guidelines for permanently destroying such biometric identifiers and biometric information'.

84 NBIPA, section 3(b)(1): 'A private entity may not collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information unless (…) the entity requires the identifier or information (…) to provide a service for the person or customer; or (…) for another valid business purpose specified in the written policy published pursuant to section 3; and (…) the entity first (…) informs the person or customer, or his or her legally authorized representative, in writing (…) that such biometric identifier or biometric information is being collected or stored; and (…) of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (…) receives a written release executed by the subject of the biometric identifier or biometric information or by the subject's legally authorized representative'. See also section 2(4): 'The term *written release* means specific, discrete, freely given, unambiguous, and informed written consent given by an individual who is not under any duress or undue influence of an entity or third party at the time such consent is given; or (…) in the context of employment, a release executed by an employee as a condition of employment'.

85 NBIPA, section 3(c): 'A private entity in possession of a biometric identifier or biometric information may not sell, lease, trade, use for advertising purposes, or otherwise profit from a person's or a customer's biometric identifier or biometric information'.

permitted by the individual concerned or where the (re)disclosure is demanded by the law or a court.[86]

Moreover, private entities need 'store, transmit, and protect' biometric information/identifiers with 'reasonable care' (meeting the relevant industry's standards); and in a way equivalent to (or more shielding than) that in which the private actor treats 'personal information that can be used to uniquely identify an individual or an individual's account or property' (that is, 'confidential and sensitive information').[87] The individuals concerned have the right to request (and the private entities have the duty to provide for free of charge) information relevant to the processing.[88]

In case of violation of the aforementioned provisions, civil proceedings can be initiated by the person affected or the state.[89]

Remarkably, though proposed by different actors,[90] the 2020 NBIP Act and the 2019 CFRP Act seem to have in common two key elements. First comes the definition of private/covered entities and the exclusion of public actors;[91] and, second, there is a general prohibition, not applicable to cases where the individual concerned has been informed and has consented.[92] Furthermore, though addressing the conduct of different actors, the 2020 NBIP Act (regulating private entities) and the FRBT Moratorium Act of 2020 (addressing federal actors) use identical phrasing when referring to remedies and, in particular, actions brought by the state.[93]

Before proceeding to state-level, it should be added that the effectiveness of the US federal initiatives, which have not yet turned into laws, could hardly be assessed at this point of time. However, and in light of our preliminary remarks on the FIPP and the US piecemeal approach to data, there seems to be a growing interest in enhancing the protection of the people against the use of contemporary intrusive technologies

86 NBIPA, section 3(d): 'A private entity in possession of a biometric identifier or the biometric information of a person, including a consumer, job applicant, employee, former employee, or contractor, may not disclose, redisclose, sell, lease, trade, use for advertising purposes, otherwise disseminate, or profit from such biometric identifier or biometric information unless (…) the subject of the biometric identifier or biometric information, or the subject's legally authorized representative, provides a written release to such specified action immediately prior to such disclosure or redisclosure (…) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative; or (…) the disclosure or redisclosure (…) is required by Federal, State, or municipal law (…) or is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction'.

87 NBIPA, section 3(e): 'A private entity in possession of a biometric identifier or biometric information shall store, transmit, and protect from disclosure all biometric identifiers and biometric information (…) using the reasonable standard of care within the private entity's industry; and (…) in a manner that is the same as, or more protective than, the manner in which the private entity stores, transmits, and protects other confidential and sensitive information'. See also section 2(2): 'The term confidential and sensitive information means personal information that can be used to uniquely identify an individual or an individual's account or property'.

88 NBIPA, section 3(f): 'Any business that collects, uses, shares, or sells biometric identifiers or biometric information, upon the request of an individual, shall disclose, free of charge, any such information relating to such individual collected during the preceding 12-month period, including (…) the categories of personal information; (…) specific pieces of personal information; (…) the categories of sources from which the business collected personal information; (…) the purposes for which the business uses the personal information; (…) the categories of third parties with whom the business shares the personal information; and (…) the categories of information that the business sells or discloses to third parties'.

89 NBIPA, section 4: '(a) Any individual aggrieved by a violation of section 3 may bring a civil action in a court of competent jurisdiction against a private entity that allegedly committed such violation. Any such violation constitutes an injury-in-fact and a harm to any affected individual (c) An individual described in subsection (a) may institute legal proceedings against a private entity alleged to have violated section 3 for the relief described in subsection (e) in any court of competent jurisdiction (d) any (…) State officer authorized by law to bring actions on behalf of the residents of a State, may bring a civil action, as parens patriae, on behalf of the residents of such State in an appropriate district court of the United States to enforce this Act if the chief law enforcement officer or other State officer has reason to believe that the interests of the residents of the State have been or are being threatened or adversely affected by a violation of section 3'.

90 The 2020 NBIP Act was introduced by Mr Merkley and Mr Sanders, whereas the 2019 CFRP Act was proposed by Mr Blunt and Mr Schatz.

91 Even though the definitions do not share same terminology, the focus remains on private actors. Compare NBIPA, section 2(3) with CFRPA, section 2(3).

92 On the 2020 NBIP Act, see sections 3(b)(1), 2(4) and 3(d). On the CFRPA, see section 3(a)(1-4).

93 Compare NBIPA, section 4 (d) with FRBT Moratorium Act, section 3(c).

by both private and public actors. Particularly interesting is the moratorium-technique, telling federal actors an explicit 'no' and placing the burden on the shoulders of the legislator, who must introduce concrete rules for technologies to be legitimately implemented.

4. Biometric and visual surveillance laws at US state level

The 2008 Illinois Biometric Information Privacy Act

The *Illinois Biometric Information Privacy Act* (the 'IBIPA') was the first US state law on biometrics.[94] It was enacted in 2008 to regulate the processing ('collection, use, safeguarding, handling, storage, retention, and destruction')[95] of 'biometric identifiers' ('retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry')[96] and 'biometric information'[97] by private entities.[98]

Its key features include: the requirement that private actors inform the public about their retention/erasure policy;[99] the prohibition of several processing operations (primarily, obtaining, profiting and disseminating), which is often conditional upon consent;[100] the duty (applicable to storing, communicating and

94 For a discussion, see Woodrow Hartzog, 'BIPA: The Most Important Biometric Privacy Law in the US?' in Amba Kak (ed), *Regulating Biometrics* (n 32) 96.

95 IBIPA, section 5(g).

96 IBIPA, section 10: '*Biometric identifie*r means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening'.

97 IBIPA, section 10: 'Biometric information means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers'.

98 IBIPA, section 10: 'Private entity means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency (….)'.

99 This Act demands that firms prepare, in written form, a retention- and destruction-policy that must be made publicly accessible. IBIPA, section 15(a): 'A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines'.

100 Consent is or can be one of the legitimate grounds for obtaining and disseminating biometric-related data. More precisely, the Act prohibits private entities from obtaining biometric identifiers and biometric information, save where the person concerned has been sufficiently informed and has given consent ('written release'); and from disseminating such information, except where disclosure is based on consent or is needed to finalise a transaction or is demanded by the law or a court. A contrario, the profiting-prohibition is not conditional upon consent. On obtaining, see IBIPA, section 15(b): 'No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first: (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) (…) informs (…) in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release'. See also IBIPA, section 10: '*Written release* means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment'. On disseminating, see IBIPA, section 15(d): 'No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction'. On profiting, see IBIPA, section 15(c): 'No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information'.

securing) to adhere to a standard of care, in the sense of treating biometrics in a way similar to or more shielding than that in which 'confidential and sensitive information' is protected;[101] and the establishment of a private cause of action, meaning that anyone aggrieved may initiate legal proceedings against the private entity that, intentionally or negligently, breaches the Act.[102]

Having been introduced as early as 2008, the IBIPA must have been an important source of inspiration for biometric regulation at federal level. This is especially true for the above-analysed 2020 NBIP Act, which, addressing private actors, adopts a similar approach to: the definition of biometric information/identifiers; the making available of the retention/destruction policy; the obtaining- and disseminating-prohibition that is conditional upon consent; the profiting-prohibition; the requirement of adherence to a standard of care; and the opportunity to initiate civil proceedings (Illinois' influencing on the above particular aspects appears to be equally true regarding regulation at state level, such as the 2009 Texas Business and Commerce Code Sec 503.001 discussed ***below***). _

The IBIPA's introduction of a private cause of action has been addressed by literature as one of its most crucial novelties.[103] The importance of this provision was demonstrated when (recently) Facebook settled to pay USD 550,000,000 after a class-action based upon privacy breach caused by the firm's tagging service.[104] Via its Tag Suggestions-service, Facebook had allegedly violated sections 15(a) and (b) of the IBIPA on notice and consent: it gathered face-related data of users' images, without having obtained consent and without having informed users about relevant retention-periods.[105] The court order, granting preliminary approval of the class action settlement, set the deadline for individual claims end of November 2020 and the final approval hearing on the 7th of January 2021.[106] It is noted that the same service, involving face recognition technology that was, in many cases, turned on by default,[107] had also caught

101 IBIPA, section 15(e): 'A private entity in possession of a biometric identifier or biometric information shall: (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information'. See also IBIPA, section 10: 'Confidential and sensitive information means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number'.

102 IBIPA, section 20: 'Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation: (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater; (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater; (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and (4) other relief, including an injunction, as the State or federal court may deem appropriate'.

103 For a critical discussion, see Woodrow Hartzog, 'BIPA: The Most Important Biometric Privacy Law in the US?' (n 94) 97 (the author provides for an excellent comparative analysis (Illinois vis-à-vis other state laws) and concludes that Illinois' Act can only work as a guide due to its inability to foresee and capture in a sustainable manner future biometrics-implementations).

104 See among others Letícia Silveira Tavares, 'Regulating the Imbalance of Power Created by Facial Recognition' (n 57) 27 (see also at page 20: 'Facebook to Pay $550 Million to Settle Facial Recognition Case').

105 Natasha Singer and Mike Isaac, 'Facebook to Pay $550 Million to Settle Facial Recognition Suit' (*The New York Times*, 29 January 2020) <https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html?mkt_tok=eyJpIjoiWVdReFl6aG1PRFptWTJJeCIsInQiOiJZeUxUNW1XcEl2M0FoSlBNKzZMWmNtTDFoQzBOVEFtK2pEa1cyU0tcL2hVYkdaa2NuTmdwd0JnSDBhd3NaMWkrZndSTERDZ1YxVk1hUDkzM0xsQ056RWt2V1FLeGJZdTBSNWl1NzNXVTlGd29OeGpUZEQ0cXpPemNGQmhWZVloSVMifQ%3D%3D> accessed 6 September 2021.

106 In Re Facebook Biometric Information Privacy Litigation (Case No 15-cv-03747-JD) Order Granting Preliminary Approval of Class Action Settlement <http://www.facebookbipaclassaction.com/media/2963197/fb_preliminary_approval_order.pdf> accessed 6 September 2021.

107 Since May 2019, social media have been providing instructions on how to stop being subjected to Facebook's facial recognition technology, which was often turned on by default. TJ McCue, 'Just Say No to Facebook Facial Recognition: Here's How to Turn It Off' (*Forbes*, 23 May 2019) <https://www.forbes.com/sites/tjmccue/2019/05/23/just-say-no-to-facebook-facial-recognition-heres-how-to-turn-it-off/#68b6462a366b> accessed 6 September 2021.

the attention of the FTC. The FTC imposed on Facebook a USD 5,000,000,000 penalty, the (at least then) biggest penalty ever imposed on a tech firm. More concretely, Facebook's technology could process user-generated images, extract patterns from these images, match facial data –involved in photographs users uploaded– to templates and suggest tags or identify users; such capabilities, turned on by default, were among the many reasons why Facebook was fined.[108] To the FTC, by requiring users to opt-out instead of obtaining affirmative consent, Facebook misrepresented the extent to which users could gain and exercise control over their data.[109]

Whether the payment by tech-giants of such large sums can truly compensate for biometric abuse can be doubted: first, these large sums (that may not be that large compared with a tech-giant's income) may correspond to tiny compensation-amounts per individual user;[110] and, second, though 'a good headline', these sums are just civil, negotiated penalties that may fail to address crucial privacy issues emerging from potential misleading practices.[111] Nonetheless, it would be fair to argue that the Illinois Act's private cause of action constitutes a useful tool in the hands of the people; this, especially where intrusiveness is embedded by-design or by-default by tech-giants. Pending cases, such as the recent class-action brought against Apple for (alleged) exploitation of facial data without consent and through the firm's preinstalled and unremovable 'Photo app'-feature,[112] may demonstrate in the future whether the civil route, entailing the imposition of penalties, can effectively protect biometrics and truly compensate the injured parties.

The 2009 Texas Business and Commerce Code (Sec 503.001)

Obviously influenced by the above 2008 Illinois Act, the 2009 ***Texas Business and Commerce Code Sec 503.001*** (the 'TBCC') addresses the capture and use of 'biometric identifiers' –that is 'retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry'.[113]

108 Makena Kelly, 'FTC Hits Facebook with $5 Billion Fine and New Privacy Checks' (*The Verge*, 24 July 2019) <https://www.theverge.com/2019/7/24/20707013/ftc-facebook-settlement-data-cambridge-analytica-penalty-privacy-punishment-5-billion> accessed 6 September 2021.

109 Federal Trade Commission, 'Statement of Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson' (*FTC*, 24 July 2019) 1 <https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf> accessed 6 September 2021; 'Complaint for Civil Penalties, Injunction, and Other Relief'(Case No 19-cv-2184) paras 14, 154, 183-186 <https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf> accessed 6 September 2021. In a similar case, Paravision processed images via its face recognition technology without the permission of users; here, the settlement before the FTC included, not only deletion of data that had been inappropriately gathered but also, the novel remedy of deleting the very machine learning algorithms that had been trained on users' images; see Tom Simonite, 'A Startup Will Nix Algorithms Built on Ill-Gotten Facial Data' (*Wired*, 12 January 2021) <https://www.wired.com/story/startup-nix-algorithms-ill-gotten-facial-data/> accessed 6 September 2021; Kim Lyons, 'FTC Settles with Photo Storage App that Pivoted to Facial Recognition' (*The Verge*, 11 January 2021) <https://www.theverge.com/2021/1/11/22225171/ftc-facial-recognition-ever-settled-paravision-privacy-photos> accessed 6 September 2021. The complaint is available on FTC, 'EVERALBUM complaint' <https://www.ftc.gov/system/files/documents/cases/everalbum_complaint.pdf> accessed 6 September 2021.

110 In this regard, see Gilardi & Co LLC, 'Facebook Biometric Information Privacy Litigation' (mentioning a possible individual claim of around USD 300) <http://www.facebookbipaclassaction.com/> accessed 6 September 2021. See also Edelson, 'Facebook Biometric Privacy Settlement' <https://edelson.com/facebook-settlement> accessed 6 September 2021; Natasha Singer and Mike Isaac, 'Facebook to Pay $550 Million to Settle Facial Recognition Suit' (n 105).

111 This was stressed by dissenting Commissioners in the FTC-case. See Federal Trade Commission, 'Dissenting Statement of Commissioner Rohit Chopra' (FTC, 24 July 2019) 4 <https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf> accessed 6 September 2021; 'Dissenting Statement of Commissioner Rebecca Kelly Slaughter' (FTC, 24 July 2019) 1-2 <https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf> accessed 6 September 2021.

112 Illinois residents claimed violation of the IBIPA by Apple's technology that processed facial characteristics via images stored on Apple's devices ('Photo app') without consent. It was further argued that users had been denied the opportunity to delete the preinstalled technology. This case, to be adjudicated now at federal level, may result in the imposition of another large penalty (as was the case with Facebook-FTC). See in more detail: Hunton Andrews Kurth, 'BIPA Lawsuit Proceeds Against Apple in Federal Court' (Hunton Privacy Blog, 18 November 2020) <https://www.huntonprivacyblog.com/2020/11/18/bipa-lawsuit-proceeds-against-apple-in-federal-court/> accessed 6 September 2021.

113 Texas Business and Commerce Code (Sec 503.001), point (a).

It prohibits the capturing of such identifiers in commercial contexts, save where the individual at issue has been informed or has given her/his consent.[114] Moreover, it forbids those holding biometric identifiers to disclose or to commercially exploit that information, except where disclosure is grounded on consent, serves the goal of finalising a transaction that the owner of the identifier permitted, is demanded by the law or is linked to law enforcement.[115] Furthermore, there is a duty to demonstrate 'reasonable care', when securing (eg, storing or sharing) biometric identifiers that must, in addition, be protected in a way identical to or more shielding than that in which confidential data are treated.[116] The Texas Code also provides for retention rules.[117]

In case of violation of the above provisions, civil penalties can be sought for by the attorney general.[118]

The 2019 California Assembly Bill No 1215

Passed in 2019, California's ***Assembly Bill No 1215*** (California Assembly Bill No 1215) adds a new section (832.19) to California's Criminal Code.[119] It has a limited scope covering officer-worn cameras,[120] which it sees as transparency- and accountability-enhancing technologies, rather than 'roving surveillance systems'.[121] The Bill is aimed at prohibiting law enforcement actors from engaging in biometric surveillance via their cameras or information collected by these devices.[122] Moreover, it gives individuals the opportunity to initiate legal proceedings ('action for equitable or declaratory relief') against law enforcement actors,

114 Texas Business and Commerce Code (Sec 503.001), point (b).
115 Texas Business and Commerce Code (Sec 503.001), point (c).
116 Texas Business and Commerce Code (Sec 503.001), point (c).
117 Texas Business and Commerce Code (Sec 503.001), points (c), (c-1) and (c-2): 'A person who possesses a biometric identifier of an individual that is captured for a commercial purpose (…) shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except as provided by Subsection (c-1): 'If a biometric identifier of an individual captured for a commercial purpose is used in connection with an instrument or document that is required by another law to be maintained for a period longer than the period prescribed by Subsection (c)(3), the person who possesses the biometric identifier shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the instrument or document is no longer required to be maintained by law'.
118 Texas Business and Commerce Code (Sec 503.001), point (d).
119 The Bill recognises various risks posed by biometric surveillance technologies, including face recognition, to privacy and other constitutional rights. According to the Bill, these risks can range from involuntary tracking and the construction of huge databases to misidentification of particular groups (such as females or the coloured). See Assembly Bill No 1215, section 1.
120 Dashcams are the predecessors of such officer-worn cameras. For a discussion, see Darius Štitilis and Marius Laurinaitis, 'Legal Regulation of the Use of Dashboard Cameras: Aspects of privacy protection' (2016) 32(2) Computer Law & Security Review 316, 317-318.
121 California Assembly Bill No 1215, section 1(e).
122 This prohibition does not affect the use of remote fingerprinting technologies for identification purposes, provided that such a use is in accordance with the law and does not lead to the retention of biometric/surveillance information. California Assembly Bill No 1215, section 2(b): 'A law enforcement agency or law enforcement officer shall not install, activate, or use any biometric surveillance system in connection with an officer camera or data collected by an officer camera'. Under section 2(a)(2) of the California Assembly Bill No 1215: 'Biometric surveillance system means any computer software or application that performs facial recognition or other biometric surveillance'. See also California Assembly Bill No 1215, section 2(a)(3), defining facial recognition or other biometric surveillance' as an 'automated or semiautomated process that captures or analyzes biometric data of an individual to identify or assist in identifying an individual' and/or an 'automated or semiautomated process that generates, or assists in generating, surveillance information about an individual based on biometric data'. See also California Assembly Bill No 1215, section 2(d): 'This section does not preclude a law enforcement agency or law enforcement officer from using a mobile fingerprint scanning device during a lawful detention to identify a person who does not have proof of identification if this use is lawful and does not generate or result in the retention of any biometric data or surveillance information'); California Assembly Bill No 1215, section 2(a)(1), defining 'biometric data' as 'a physiological, biological, or behavioral characteristic that can be used, singly or in combination with each other or with other information, to establish individual identity'; and section 2(a)(8), defining 'surveillance information' as '(a)ny information about a known or unknown individual, including, but not limited to, a person's name, date of birth, gender, or criminal background' and/or '(a)ny information derived from biometric data, including, but not limited to, assessments about an individual's sentiment, state of mind, or level of dangerousness'.

who have acted in violation of its provisions.[123] The Bill is subjected to time-limit: relevant provisions are to be repealed in 2023.[124]

The 2020 California Genetic Information Privacy Act

The proposed ***Genetic Information Privacy Act*** (the 'GIPA'), expected to become part of the state's Civil Code, promises a more rigorous protection of genetic privacy.[125] Introduced in February 2020, the GIPA (as Chapter 2.6) will form part of the Civil Code's Part 2.6 'confidentiality of medical information' and follow existing chapter 2.5. The latter chapter already provides for important safeguards, but only with regard to disclosure of the result of a genetic test ***by a health care service plan***.[126] With GIPA, private firms engaging in genetic testing could also be covered.

The GIPA protects consumers' 'genetic data', meaning 'any data, regardless of its format, that results from the analysis of a biological sample from a consumer, or from another element enabling equivalent information to be obtained, and concerns genetic material'.[127] It addresses private actors (direct-to-consumer genetic testing companies,[128] but also other firms gathering, using, storing or disseminating genetic data coming from direct-to-consumer genetic testing product/service or given by the consumer).[129]

These private entities are bound by the duty to make their policy on genetic data processing ('collection, use, maintenance, and disclosure') available to the consumer.[130] Moreover, they need obtain the express (and, where applicable, separate) consent of the consumer for the 'collection, use, and disclosure' of rele-

123 California Assembly Bill No 1215, section 2(c): 'In addition to any other sanctions, penalties, or remedies provided by law, a person may bring an action for equitable or declaratory relief in a court of competent jurisdiction against a law enforcement agency or law enforcement officer that violates this section'.

124 California Assembly Bill No 1215, section 2(e).

125 For a discussion, see John Verdi, 'California's SB 980 Would Codify Strong Protections for Genetic Data' (Future of Privacy Forum, 3 September 2020) <https://fpf.org/2020/09/03/californias-sb-980-would-codify-strong-protections-for-genetic-data/> accessed 6 September 2021.

126 Civil Code, division 1, part 2.6. 'confidentiality of medical information' <http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=56.17> accessed 6 September 2021.

127 Genetic data do not include, among others, information that has been de-identified or information that is processed (by an authorised actor) for scientific purposes. GIPA, section 56.18(b)(7).

128 GIPA, section 56.18(b)(5): 'Direct-to-consumer genetic testing company means an entity that does either of the following: (s) ells, markets, interprets, or otherwise offers consumer-initiated genetic testing products or services directly to consumers (a) nalyzes genetic data obtained from a consumer, except to the extent that the analysis is performed by a person licensed in the healing arts for diagnosis or treatment of a medical condition'.

129 See for example GIPA, section 56.181(a).

130 GIPA, section 56.181(a)(1): 'To safeguard the privacy, confidentiality, security, and integrity of a consumer's genetic data, a direct-to-consumer genetic testing company, or any other company that collects, uses, maintains, or discloses genetic data collected or derived from a direct-to-consumer genetic testing product or service or directly provided by a consumer, shall (1) Provide clear and complete information regarding the company's policies and procedures for the collection, use, maintenance, and disclosure, as applicable, of genetic data by making available to a consumer both of the following: (…) A summary of its privacy practices, written in plain language, that includes information about the company's collection, use, maintenance, and disclosure, as applicable, of genetic data (…) A prominent and easily accessible privacy notice that includes, at a minimum, complete information about the company's data collection, consent, use, access, disclosure, maintenance, transfer, security, and retention and deletion practices, and information that clearly describes how to file a complaint alleging a violation of this chapter, pursuant to subdivision (c) of Section 56.182 A notice that the consumer's deidentified genetic or phenotypic information may be shared with or disclosed to third parties for research purposes in accordance with Part 46 (commencing with Section 46.101) of Title 45 of the Code of Federal Regulations'.

vant data,[131] as well as provide for effective mechanisms enabling consumers to revoke consent.[132] Furthermore, they must provide for necessary security mechanisms, but also enable consumers to access their data and exercise their right to delete them.[133] There is also a duty not to discriminate against consumers binding both private and public actors.[134] Last, private entities are, in principle, prohibited from disclosing genetic data.[135]

It is added that California's Genetic Information Privacy Act provides for civil remedies.[136]

131 GIPA, section 56.181(a)(2): 'a direct-to-consumer genetic testing company, or any other company that collects, uses, maintains, or discloses genetic data collected or derived from a direct-to-consumer genetic testing product or service or directly provided by a consumer, shall (2) Obtain a consumer's express consent for collection, use, and disclosure of the consumer's genetic data, including, at a minimum, separate and express consent for each of the following: (A) The use of the genetic data collected through the genetic testing product or service offered to the consumer (…) (B) The storage of a consumer's biological sample (…) (C) Each use of genetic data or the biological sample beyond the primary purpose of the genetic testing or service and inherent contextual uses (D) Each transfer or disclosure of the consumer's genetic data or biological sample to a third party (…) (E) The marketing or facilitation of marketing to a consumer based on the consumer's genetic data or the marketing or facilitation of marketing by a third party based upon the consumer having ordered, purchased, received or used a genetic testing product or service'.

132 GIPA, section 56.181(b) and (c): '(b) A company that is subject to the requirements described in paragraph (2) of subdivision (a) shall provide effective mechanisms, without any unnecessary steps, for a consumer to revoke their consent after it is given, at least one of which utilizes the primary medium through which the company communicates with consumers. (c) If a consumer revokes the consent that they provided pursuant to subdivision (2) of subdivision (a), the company shall honor the consumer's consent revocation as soon as practicable, but not later than 30 days after the individual revokes consent, in accordance with both of the following: (1) Revocation of consent under this section shall comply with Part 46 of Title 45 of the Code of Federal Regulations. (2) The company shall destroy a consumer's biological sample within 30 days of receipt of revocation of consent to store the sample'.

133 GIPA, section 56.181(d): 'The direct-to-consumer genetic testing company, or any other company that collects, uses, maintains, or discloses genetic data collected or derived from a direct-to-consumer genetic testing product or service, or provided directly by a consumer, shall (1) Implement and maintain reasonable security procedures and practices to protect a consumer's genetic data against unauthorized access, destruction, use, modification, or disclosure (2) Develop procedures and practices to enable a consumer to easily (a)ccess the consumer's genetic data (d)elete the consumer's account and genetic data, except for genetic data that is required to be retained by the company to comply with applicable legal and regulatory requirements'.

134 This provision forbids discriminatory activities, such as the offering of services of different quality or the establishing of suspicion on the ground of the consumer exercising her rights. GIPA, section 56.181(e): '(e) A person or public entity shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this chapter by (1) Denying goods, services, or benefits to the customer (2) Charging different prices or rates for goods or services (3) Providing a different level or quality of goods, services, or benefits to the consumer (4) Suggesting that the consumer will receive a different price or rate for goods, services, or benefits, or a different level or quality of goods, services, or benefits (5) Considering the consumer's exercise of rights under this chapter as a basis for suspicion of criminal wrongdoing or unlawful conduct'.

135 This prohibition may not apply under certain circumstances and where the recipients are entities, whose primary activity is not related to, among others, health or insurance. GIPA, section 56.181(f): '(1) shall not disclose a consumer's genetic data to any entity that is responsible for administering or making decisions regarding health insurance, life insurance, long-term care insurance, disability insurance, or employment or to any entity that provides advice to an entity that is responsible for performing those functions (2) (…) may disclose a consumer's genetic data or biological sample to an entity described in paragraph (1) if all of the following are true: (A) The entity is not primarily engaged in administering health insurance, life insurance, or long-term care insurance, disability insurance, or employment (…) (B) The consumer's genetic data or biological sample is not disclosed to the entity in that entity's capacity as a party that is responsible for administering, advising, or making decisions regarding health insurance, life insurance, long-term care insurance, disability insurance, or employment (…) (C) Any agent or division of the entity that is involved in administering, advising, or making decisions regarding health insurance, life insurance, long-term care insurance, disability insurance, or employment is prohibited from accessing the consumer's genetic data or biological sample'.

136 The remedy mechanism is not applicable to the processing of certain medical/health information, particular health care providers and entities, scientific activities performed by authorised institutions and the state's 'newborn screening program'. GIPA, section 56.182: '(a) Any person who negligently violates this chapter shall be assessed a civil penalty (b) Any person who willfully violates this chapter shall be assessed a civil penalty (c) Actions for relief pursuant to this chapter shall be prosecuted exclusively in a court of competent jurisdiction by the Attorney General or a district attorney or by a county counsel authorized by agreement with the district attorney or by a city attorney (d) Court costs recovered pursuant to this section shall be paid to the party or parties that prosecuted the violation. Penalties recovered pursuant to this section shall be paid to the individual to whom the genetic data at issue pertains. (e) Any provision of a contract or agreement between a consumer and a person governed by this chapter that has, or would have, the effect of delaying or limiting access to a legal remedy for a violation of this chapter shall not apply to the exercise of rights or enforcement pursuant to this chapter. (f) Each violation of this chapter is a separate and actionable violation'. See also GIPA, section 56.182: '(b) This chapter shall not apply to (1) Medical information governed by the Confidentiality of Medical Information Act (…) or to protected health information that is collected, maintained, used, or disclosed by a covered entity or business associate governed by the privacy, security, and breach notification rules (…) (2) A provider of health care governed by the Confidentiality of Medical Information Act (…) or a covered entity governed by the privacy, security, and breach notification rules (…) (3) A business associate of a covered entity governed by the privacy, security, and data breach notification rules (…) (4) Scientific research or educational activities conducted by a public or private nonprofit postsecondary educational institution (…) (5) The California newborn screening program'.

California Privacy Rights Act of 2020: an EU-like instrument

The CPRA, created by Proposition 24 with a view to amending California Consumer Privacy Act, is targeted at businesses and aims to better protect consumers.[137] This Act introduces a new category of 'sensitive personal information', including biometric data, which is subject to novel (EU-like) disclosure and purpose limitation requirements; and it grants consumers new rights.

More concretely, the CPRA defines biometric data ('biometric information') in a way similar to the GDPR. However, it offers more examples in the text,[138] as well as clarifications; for instance, biometrics that are gathered by businesses without awareness of a given consumer do not constitute 'publicly available' information (the latter is in turn ***not*** considered as personal data).[139] Moreover, the Act grants consumers various GDPR-like rights, including: the right to correction of inaccurate personal data, the right to opt out of automated decision making, the right to access data about automated decision making and the right to restrict collection, use and disclosure of personal data (including sensitive data, like biometrics).[140] Furthermore, same as the GDPR, the CPRA imposes on businesses duties to conduct audits, as well as risk assessments, where the processing entails high risk to consumers.[141] Notably, principles known from the EU-regime, namely data minimisation, purpose limitation and storage limitation, are also present in this initiative.[142] Another element bringing this Act close to the EU regime is 'consent' that is defined in a GDPR-way and is required for various processing operations (including selling/sharing of data after an opt-out, secondary use/disclosure of sensitive data after an opt-out or financial incentive programs).[143]

137 CPRA, section 3 'Purpose and Intent'.

138 CPRA, section 14 ('(…) "Biometric information" means an individual's physiological, biological or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that (…) is used or is intended to be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information (…)').

139 CPRA, section 14 ('(…) "Personal information" does not include publicly available information (…) "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge (…)').

140 CPRA, section 3 ('(…) Consumers should be able to control the use of their personal information, including limiting the use of their sensitive personal information, the unauthorized use or disclosure of which creates a heightened risk of harm to the consumer, and they should have meaningful options over how it is collected, used, and disclosed (…)').

141 CPRA, section 20 ('(…) Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to: (A) Perform a cybersecurity audit on an annual basis (…) (B) Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information (…)').

142 CPRA, section 4 ('(…) (a) A business that controls the collection of collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the of the following (…) The categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section (…) If the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section (…) The length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose (…) A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes (…)').

143 CPRA, section 14 ('(…) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent (…)').

The CPRA becomes fully enforceable on the 1st of July 2023; and the California Privacy Protection Agency (established by the CPRA) has recently issued an 'Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020'.[144]

The 2020 Washington Engrossed Substitute Senate Bill 6280

Washington's Engrossed Substitute Senate Bill 6280, passed in March 2020, regulates the use of ***facial recognition services***[145] by state or local authorities.

More concretely, these authorities need to submit a 'notice of intent', regarding the use of a facial recognition service and its concrete purpose, and then prepare an 'accountability report' that must be clear and comprehensive as to certain minimums[146] (such as the concrete purpose the technology pursues or data management policies).[147] This report must be subjected to public review and consultation (prior to its finalisation), as well as regular updates.[148] Furthermore, where the face recognition system is aimed at making decisions that 'produce legal effects concerning individuals or similarly significant effects concerning individuals', such decisions need be subjected to 'meaningful human review'.[149]

Other requirements include the duty to implement suitable interfaces allowing for independent checks or accuracy assessments (especially, to avoid discrimination),[150] regular training duties[151] or the duty to offer information about the use of the technology to the criminal defendant before her/him being tried.[152] The Bill further provides for the creation of a 'facial recognition task force' that must offer recommendations on possible risks, evaluate sufficiency of existing legislation or assess 'quality, accuracy, and efficacy' of the technology.[153] Under the Bill, the use of facial recognition services by state or local actors for surveillance-, identification- or tracking-purposes is prohibited, save where there is a warrant or court order or under exceptional circumstances.[154] Other restrictions refer to, among others, the application of the technology to persons on concrete discriminatory grounds protected by the law (like religion, race or gender),[155] reliance upon the facial recognition service as the only basis for establishing 'probable cause'

144 Hunton Andrews Kurth, 'California Privacy Protection Agency Invites Comments on Proposed CPRA Rulemaking' (Hunton Privacy Blog, 24 September 2021) <https://www.huntonprivacyblog.com/2021/09/24/california-privacy-protection-agency-invites-comments-on-proposed-cpra-rulemaking/#more-20793> accessed 28 September 2021.

145 Under section 2(3) of the Engrossed Substitute Senate Bill 6280, facial recognition service means 'technology that analyzes facial features and is used by a state or local government agency for the identification, verification, or persistent tracking of individuals in still or video images'; under the same provision, this technology 'does not include: (i) The analysis of facial features to grant or deny access to an electronic device; or (ii) the use of an automated or semiautomated process for the purpose of redacting a recording for release or disclosure outside the law enforcement agency to protect the privacy of a subject depicted in the recording, if the process does not generate or result in the retention of any biometric data or surveillance information'.

146 Engrossed Substitute Senate Bill 6280, section 3(1) and (2).

147 Engrossed Substitute Senate Bill 6280, section 3(2).

148 Engrossed Substitute Senate Bill 6280, section 3(3) and (4). Prior to the use of the service, the report must be made publicly available; and, where the initial purpose of the use of the service (as stated in the report) is to be altered, there need be prior review and consultation and, then, update of the initial report. See Engrossed Substitute Senate Bill 6280, sections 3(5) and 3(7).

149 Engrossed Substitute Senate Bill 6280, section 4, clarifying that '(d)ecisions that produce legal effects concerning individuals or similarly significant effects concerning individuals means decisions that result in the provision or denial of financial and lending services, housing, insurance, education enrolment, criminal justice, employment opportunities, health care services, or access to basic necessities such as food and water, or that impact civil rights of individuals'. See also Engrossed Substitute Senate Bill 6280, section 2(7), defining meaningful human review as 'review or oversight by one or more individuals who are trained (…) and who have the authority to alter the decision under review'. In such cases, public agencies must, prior to using the technology, test its functionality and 'take reasonable steps to ensure best quality results' (Engrossed Substitute Senate Bill 6280, section 5).

150 Engrossed Substitute Senate Bill 6280, section 6.

151 Engrossed Substitute Senate Bill 6280, section 7.

152 Engrossed Substitute Senate Bill 6280, section 8.

153 Engrossed Substitute Senate Bill 6280, section 10.

154 Engrossed Substitute Senate Bill 6280, section 11(1).

155 Engrossed Substitute Senate Bill 6280, section 11(2).

in criminal contexts[156] or image-tampering in face recognition contexts.[157] It need be pointed out that nothing identical, similar or even close to the above restrictions on 'probable cause' and image-manipulation exists in the LED. Even though these issues could be addressed by national laws in the EU, the US concrete provisions can demonstrate supremacy of piecemeal regulation.

The 2020 Indiana House Bill 1238

The Indiana's House Bill 1238 was introduced in 2020. The requirements set out in this Bill (as made publicly available by Indiana General Assembly) are rather simple and brief. State or local law enforcement actors, deploying surveillance technologies, must conduct a 'surveillance technology impact and use policy', make that policy available on their webpage, and update it prior to altering the technology's function or purpose.[158]

The 2020 New Jersey Assembly Bill 989

The New Jersey's Assembly Bill 989 was proposed in 2020 to subject facial recognition technologies to independent accuracy- and bias-checking. More precisely, the attorney general must 'arrange for independent, third party testing and auditing of the accuracy of the five most commonly available facial recognition systems by market share, under operational conditions', as well as report to the Legislature.[159]

The 2020 New York Assembly Bill A6787D

New York's Assembly Bill A6787D was signed in December 2020 with a view to protecting children's privacy, safety and security.[160] It suspends the implementation of biometric technologies,[161] including face

156 Engrossed Substitute Senate Bill 6280, section 11(5): 'A state or local law enforcement agency may not use the results of a facial recognition service as the sole basis to establish probable cause in a criminal investigation. The results of a facial recognition service may be used in conjunction with other information and evidence lawfully obtained by a law enforcement officer to establish probable cause in a criminal investigation'.

157 Engrossed Substitute Senate Bill 6280, section 11(7): 'A state or local law enforcement agency may not substantively manipulate an image for use in a facial recognition service in a manner not consistent with the facial recognition service provider's intended use and training'.

158 House Bill 1238: 'Requires a state or local law enforcement agency (agency) that uses surveillance technology to prepare a surveillance technology impact and use policy (policy) and post the policy on the agency's Internet web site. Specifies the information that must be included in the policy. Provides that surveillance technology includes a system, equipment, or software used for collecting, processing, sharing or analyzing audio, video, location data, thermal data, license plate data, facial recognition, or other biometric surveillance to produce information about a person's identity. Requires an agency to establish and post a policy with regard to surveillance technology that is in use by the agency on June 30, 2020, not later than January 1, 2021. Requires an agency to post an amended policy before implementing any enhancements to surveillance technology or using the technology in a purpose or manner not previously disclosed through the existing policy '.

159 Assembly Bill 989: 'The testing and auditing is required to determine whether there is a statistically significant variation in the accuracy of the facial recognition systems on the basis of race, skin tone, ethnicity, gender, or age of the individuals portrayed in the images, whether or not those categories are applied individually or in combination. Under the bill, the Attorney General is required to submit a report to the Legislature containing the results of the testing required by the bill. The report is to be submitted within 30 days after the completion of the testing'.

160 See in more detail: Hunton Andrews Kurth, 'New York Temporarily Bans Facial Recognition Technology in Schools' (Hunton Privacy Blog, 29 December 2020) <https://www.huntonprivacyblog.com/2020/12/29/new-york-temporarily-bans-facial-recognition-technology-in-schools/> accessed 6 September 2021; Governor's Press Office, 'Legislation (A6787-D/S5140-B) Directs the Study of Whether Facial Recognition and Other Kinds of Biometric Technology Should be Used in Schools; Suspends Their Use Until Properly Reviewed' (Governor's Press Office, 22 December 2020) <https://www.governor.ny.gov/news/governor-cuomo-signs-legislation-suspending-use-and-directing-study-facial-recognition> accessed 6 September 2021.

161 'Biometric identifying technology' is defined as 'any tool using an automated or semi-automated process that assists in verifying a person's identity based on a person's biometric information' (section 1 § 2-e, a). See also section 1 § 2-e, b referring to 'biometric information' as 'any measurable physical, physiological or behavioral characteristics that are attributable to a person, including but not limited to facial characteristics, fingerprint characteristics, hand characteristics, eye characteristics, vocal characteristics, and any other characteristics that can be used to identify a person including, but are not limited to: fingerprints; handprints; retina and iris patterns; DNA sequence; voice; gait; and facial geometry'.

recognition tools,[162] in public and private schools. More concretely, it sets out a moratorium referring to purchases and uses of such technologies up until 1 July 2022 or until these technologies are proven safe and, therefore, their implementations are authorised by the State Education Commissioner (whichever takes place later).[163] It further provides for consultations to be conducted with public authorities, experts and relevant stakeholders, in order to identify the conditions for suitability of the use of biometric technologies in schools, as well as the constraints that should be in place to safeguard privacy and other rights and interests.[164]

The 2021 Virginia Senate Bill No 1392

Virginia's Senate Bill 1392 was proposed in February 2021 under the title 'Consumer Data Protection Act'. Under this Bill, biometric data are treated as sensitive data;[165] and they are defined as 'data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual'.[166] Virginia's initiative is focused on private, for profit, entities that process significant amounts of personal data.[167]

It grants concrete rights to consumers and imposes particular duties on controllers.[168] Upon request of the consumer, the controller must: confirm whether or not it is processing personal data and grant access to such data;[169] correct inaccuracies;[170] erase data;[171] enable the consumer to transmit personal data to another controller;[172] opt out of the processing, when the goal is related to 'targeted advertising',[173] the

162 New York's Assembly Bill sees 'facial recognition' as 'any tool using an automated or semi-automated process that assists in uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's face' (section 1 § 2-e, c).

163 'Public and nonpublic elementary and secondary schools, including charter schools, shall be prohibited from purchasing or utilizing biometric identifying technology for any purpose, including school security, until July first, two thousand twenty-two or until the commissioner authorizes such purchase or utilization (…) whichever occurs later' (New York's Assembly Bill, subdivision 2).

164 'The commissioner shall not authorize the purchase or utilization of biometric identifying technology, including but not limited to facial recognition technology, without first issuing a report prepared in consultation with the department's chief privacy officer, making recommendations as to the circumstances in which the utilization of such technology is appropriate in public and nonpublic elementary and secondary schools, including charter schools, and what restrictions and guidelines should be enacted to protect individual privacy, civil rights, and civil liberty interests (…) The commissioner shall, via scheduled public hearings and other outreach methods, seek feedback from teachers, school administrators, parents, individuals with expertise in school safety and security, and individuals with expertise in data privacy issues and student privacy issues, and individuals with expertise in civil rights and civil liberties prior to making such recommendations' (New York's Assembly Bill, subdivisions 3 and 4).

165 Senate Bill 1392, section 59.1-571: '"Sensitive data" means a category of personal data that includes: (…) The processing of genetic or biometric data for the purpose of uniquely identifying a natural person'.

166 Senate Bill 1392, section 59.1-571, further mentioning that biometric data do not include 'a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA'.

167 Senate Bill 1392, section 59.1-572: 'This chapter applies to persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data'.

168 Under the Senate Bill 1392, section 59.1-571, a consumer is 'a natural person who is a resident of the Commonwealth acting only in an individual or household context (…) (i)t does not include a natural person acting in a commercial or employment context'; and a controller is defined as 'the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data'.

169 Senate Bill 1392, section 59.1-573, subsection A.

170 Senate Bill 1392, section 59.1-573, subsection A ('correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data').

171 Senate Bill 1392, section 59.1-573, subsection A.

172 Senate Bill 1392, section 59.1-573, subsection A ('obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means').

173 Senate Bill 1392, section 59.1-571: '"Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests'.

'sale of personal data'[174] or profiling[175] 'in furtherance of decisions that produce legal or similarly significant effects concerning the consumer'.[176] Moreover, the controller must, upon request of the consumer, respond to or inform the consumer in due time;[177] provide the consumer with relevant information free of charge (save where it can demonstrate the consumer's request is 'manifestly unfounded, excessive, or repetitive');[178] and create an appeal-mechanism for the consumer.[179] Importantly, the rights of consumers to request from controllers to comply with the aforementioned duties cannot be waived or limited by agreement.[180]

Furthermore, Virginia's Senate Bill imposes concrete transparency-related duties: the controller must limit its processing activities to 'what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer';[181] not process data for goals not 'reasonably necessary to' and not 'compatible with' the initial goals of the processing 'as disclosed to the consumer' (save where the controller obtains consent);[182] implement security practices with a view to safeguarding 'confidentiality, integrity, and accessibility of personal data';[183] not engage in processing that leads to unlawful discrimination against consumers;[184] not process sensitive data, including biometric data, without the consent[185] of the consumer (or, in case of a child, without complying with the Children's Online Privacy Protection Act).[186] In addition, the controller must: provide consumers 'with a reasonably accessible, clear, and meaningful privacy notice';[187] in case of sale or processing for targeted advertising,

174 Senate Bill 1392, section 59.1-571: '"Sale of personal data" means the exchange of personal data for monetary consideration by the controller to a third party'.
175 Senate Bill 1392, section 59.1-571: '"Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements'.
176 Senate Bill 1392, section 59.1-573, subsection A.
177 Senate Bill 1392, section 59.1-573, subsection B ('A controller shall respond to the consumer without undue delay, but in all cases within 45 days of receipt of the request submitted pursuant to the methods described in § 59.1-573 A (…) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but in all cases and at the latest within 45 days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision pursuant to subsection C').
178 Senate Bill 1392, section 59.1-573, subsection B ('Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request').
179 Senate Bill 1392, section 59.1-573, subsection C.
180 Senate Bill 1392, section 59.1-574, subsection B.
181 Senate Bill 1392, section 59.1-574, subsection A.
182 Senate Bill 1392, section 59.1-574, subsection A.
183 Senate Bill 1392, section 59.1-574, subsection A ('Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue').
184 Senate Bill 1392, section 59.1-574, subsection A ('Not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this subdivision shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his right to opt out pursuant to § 59.1-573 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program').
185 Senate Bill 1392, section 59.1-571: '"Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action'.
186 Senate Bill 1392, section 59.1-574, subsection A.
187 Senate Bill 1392, section 59.1-574, subsection C ('Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes: 1. The categories of personal data processed by the controller; 2. The purpose for processing personal data; 3. How consumers may exercise their consumer rights pursuant § 59.1-573, including how a consumer may appeal a controller's decision with regard to the consumer's request; 4. The categories of personal data that the controller shares with third parties, if any; and 5. The categories of third parties, if any, with whom the controller shares personal data').

'clearly and conspicuously disclose such processing';[188] and enable the consumer to exercise its rights.[189] Virginia's Senate Bill further imposes on the controller the duty to conduct personal data assessments, where the processing: is aimed at targeted advertising, sale of personal data or profiling; involves sensitive data (including biometric data); or entails a significant risk of harm.[190] Notably, the processor[191] is required to assist the controller in complying with its obligations.[192]

Certain exemptions are provided for, where the processing concerns de-identified data; yet, the controller must guarantee that such data cannot be linked to an individual, as well as ensure that it will not intend to re-identify relevant information.[193] Moreover, the rights of the consumers may be limited in some cases, such as where the controller must comply with the law, cooperate with law enforcement or conduct scientific research in the public interest.[194]

In case of violation of the above provisions, the Attorney General is authorised to initiate an action seeking for injunction to restrain the breach and civil penalties (maximum of USD 7,500 for each breach).[195]

To sum up, although the Virginia's Senate Bill is not specifically targeted at biometric data, it offers clear rules that, on the one hand, protect biometric data as sensitive personal data (whose processing is, in principle, prohibited) and, on the other hand, impose concrete duties on controllers.

5. Biometric and visual surveillance laws at US city-level

Portland's ban of face recognition technology

With its 2020 Ordinance (effective since January 2021),[196] Portland bans the application of face recognition to public spaces and by private entities. The main grounds for banning are the following: several risks, ranging from threats to anonymity, individual and collective privacy or equality to marginalisation or discrimination;[197] lack of an adequate mechanism to assess allegedly 'unacceptable gender and racial

188 Senate Bill 1392, section 59.1-574, subsection D.

189 Senate Bill 1392, section 59.1-574, subsection E ('A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights pursuant to § 59.1-573 but may require a consumer to use an existing account').

190 Senate Bill 1392, section 59.1-576.

191 Senate Bill 1392, section 59.1-571: '"Processor" means a natural or legal entity that processes personal data on behalf of a controller'.

192 Senate Bill 1392, section 59.1-575.

193 Senate Bill 1392, section 59.1-577. See also section 59.1-571: '"De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person'.

194 Senate Bill 1392, section 59.1-578.

195 Senate Bill 1392, section 59.1-580.

196 For an overview, see Hunton Andrews Kurth, 'Portland, Oregon First to Ban Private-Sector Use of Facial Recognition Technology' (Hunton Privacy Blog, 10 September 2020) <https://www.huntonprivacyblog.com/2020/09/10/portland-oregon-becomes-first-jurisdiction-in-u-s-to-ban-the-commercial-use-of-facial-recognition-technology/> accessed 6 September 2021.

197 Portland's first Ordinance, section 1, points 1, 3 and 8. Portland, emphasising due process, transparency and oversight, further stresses the risk of misuse and misidentification. See Portland's first Ordinance, section 1, point 14: 'While uses of Face Recognition Technologies may have benefits, the risk for misidentification and misuse is always present. Safe use of these technologies requires adequate due process, transparency, and oversight measures to be trusted. Implementing this infrastructure needs investment in development of rules and structures that allow appropriate uses of Face Recognition Technologies'.

bias';[198] the consideration of banning as the suitable precautionary measure;[199] and the need that 'surveillance technologies'[200] become 'transparent, accountable, and designed in ways that protect personal and collective privacy'.[201]

More concretely, Portland is committed to develop a plan on public awareness of relevant risks;[202] and it intends to ban the use of face recognition[203] technologies[204] in 'Places of Public Accommodation'[205] by 'Private Entities',[206] save where these entities must engage in the use of these technologies to comply with the law or where the user need be verified for access-purposes (in personal or employment contexts) or where face recognition takes place automatically in social media contexts.[207] On remedies, Portland provides for the opportunity to bring legal proceedings against the private entity.[208]

Furthermore, with its second ordinance, Portland bans the use of the above technologies and of information related to these technologies by the city's public actors ('bureaus').[209] The ban is subject to exceptions

198 Portland's first Ordinance, section 1, points 9 and 10.
199 Portland's first Ordinance, section 1, points 9, 13.
200 Portland's first Ordinance (section 1, point 11) defines 'Surveillance Technologies' as 'any software, electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group'.
201 Portland's first Ordinance, section 1, point 12: 'Surveillance Technologies, including Face Recognition, must be transparent, accountable, and designed in ways that protect personal and collective privacy, particularly information from children and vulnerable and marginalized groups'.
202 Portland's first Ordinance, section 1, points b and c.
203 'Face Recognition' is defined as 'the automated searching for a reference image in an image repository by comparing the facial features of a probe image with the features of images contained in an image repository (one-to-many search)'. Portland's first Ordinance, Exhibit A, 'TITLE 34 DIGITAL JUSTICE', 'Chapter 34.10, Prohibit the use of Face Recognition Technologies by Private Entities in Places of Public Accommodation in the City of Portland', 34.10.020.
204 The term 'Face Recognition Technologies' is defined as 'automated or semi-automated processes using Face Recognition that assist in identifying, verifying, detecting, or characterizing facial features of an individual or capturing information about an individual based on an individual's face'. Portland's first Ordinance, Exhibit A, 'TITLE 34 DIGITAL JUSTICE', 'Chapter 34.10, Prohibit the use of Face Recognition Technologies by Private Entities in Places of Public Accommodation in the City of Portland', 34.10.020.
205 Portland's first Ordinance, 34.10.020: 'Places of Public Accommodation means any place or service offering to the public accommodations, advantages, facilities, or privileges whether in the nature of goods, services, lodgings, amusements, transportation or otherwise (…) does not include: An institution, bona fide club, private residence, or place of accommodation that is in its nature distinctly private'.
206 Portland's first Ordinance, 34.10.020: 'Private Entity means any individual, sole proprietorship, partnership, corporation, limited liability company, association, or any other legal entity, however organized. A Private Entity does not include a Government Agency'.
207 Portland's first Ordinance, 34.10.040: 'The prohibition in this Chapter does not apply to use of Face Recognition Technologies: A. To the extent necessary for a Private Entity to comply with federal, state, or local laws; B. For user verification purposes by an individual to access the individual's own personal or employer issued communication and electronic devices; or C. In automatic face detection services in social media applications'.
208 Portland's first Ordinance, 34.10.050: 'A. Any person injured by a material violation of this Chapter by a Private Entity has a cause of action against the Private Entity in any court of competent jurisdiction for damages sustained as a result of the violation or $1,000 per day for each day of violation, whichever is greater and such other remedies as may be appropriate B. In an action brought to enforce this Chapter, a court may award to the plaintiff (…) a reasonable amount to be fixed by the court as attorney fees'.
209 Portland's second Ordinance, points b-e: 'Bureaus shall not acquire, evaluate or use Face Recognition Technologies, except as expressly provided in Section (f). This prohibition applies to Face Recognition Technologies that are procured by any means with or without the exchange of monies or other consideration. For purposes of clarity, this means bureaus shall not purchase, lease or accept a donation or gift of Face Recognition Technologies c. Bureaus shall not knowingly acquire, request, use, access or retain any information (unless required by public record retention rules) derived from Face Recognition Technologies or intentionally collect information to be used for Face Recognition Technologies, except as expressly provided in Section (f) d. Bureaus shall not direct a non-City entity to acquire or use Face Recognition Technologies on the City's behalf unless such acquisition or use would be otherwise allowed for bureaus under this ordinance e. Bureaus shall not knowingly allow a non-City entity to use Face Recognition Technologies on City owned property unless such use would be otherwise allowed for bureaus under this ordinance'.

mainly related to own staff's activities (such as verification or social media applications).[210] Moreover, according to the second ordinance, bureaus, assisted by temporary entities, are obliged to detect any use of face recognition technologies in the public realm.[211] Remedies protecting individuals injured against the city of Portland are also provided for.[212]

Baltimore's ban on face recognition

On 8 September 2021, Baltimore banned the use of face recognition by private actors, as well as by the city of Baltimore.[213] First, the 2021 ordinance[214] prohibits the city of Baltimore from obtaining a face recognition system and contracting other entities with a view to using such systems; some biometric security systems are exempted.[215] Second, it prohibits private actors from obtaining, retaining, accessing or using a face recognition system or information gathered from such a system; some biometric security systems, as well as Maryland's Image Repository System are exempted.[216]

210 Portland's second Ordinance point f: 'Bureaus may only use Face Recognition Technologies for the following purposes: 1. For verification purposes for bureau staff to access their own personal or City issued personal communication and electronic devices. For example, bureau staff may use Face Recognition Technologies to unlock their own or assigned mobile phones or tablets; 2. In automatic face detection services in social media applications. Bureau staff activity in social media is regulated by the policy HRAR 4.08A; and 3. In detecting faces for the sole purpose of redacting a recording for release or disclosure outside the City to protect the privacy of a subject depicted in the recording'. See also point g addressing unintentional use of face recognition-related information.

211 Portland's second Ordinance, points a, h-j: 'a. Each bureau director shall require bureau staff to review and assess whether bureau staff are using Face Recognition Technologies. Each bureau will complete this assessment and provide it to the Bureau of Planning and Sustainability's Smart City PDX Open Data Coordinator within 90 business days after the effective date of this ordinance. This report will be made publicly accessible h. The Bureau of Planning and Sustainability's Smart City PDX Open Data Coordinator will convene a temporary group to serve as a resource to all bureaus to assess whether a technology constitutes Face Recognition Technologies and explore whether any changes are necessary to other existing City policies or administrative rules i. (…) the Bureau of Planning and Sustainability is directed to explore the adoption of a comprehensive Data Governance and Privacy and Information Protection framework that addresses the appropriate use or prohibition of Surveillance Technologies (…) j. The Bureau of Planning and Sustainability and the Office of Equity and Human Rights shall address public use of Face Recognition Technologies'.

212 Portland's second Ordinance point l: '1. A person injured by a material violation of this ordinance may institute proceedings against the City in a court of competent jurisdiction for injunctive relief, declaratory relief, or writ of mandate to enforce this ordinance. 2. Prior to the initiation of any legal proceeding under subsection (1), the City must be given written notice via the City Attorney's Office of the violation(s), and the bureau who is alleged to have violated the ordinance will have 30 days from receipt of the notice to correct such violation(s). 3. If the alleged violation(s) is substantiated and subsequently corrected, a notice shall be posted in a conspicuous space on the City's website that describes the corrective measure(s) taken to address the violation(s)'.

213 Hunton Andrews Kurth, 'UPDATE: Baltimore Bans Private-Sector Use of Facial Recognition Technology' (Hunton Privacy Blog, 7 September 2021) <https://www.huntonprivacyblog.com/2021/09/07/update-baltimore-bans-private-sector-use-of-facial-recognition-technology/> accessed 9 September 2021. See also Hunton Andrews Kurth, 'Baltimore Passes Bill Banning Private-Sector Use of Facial Recognition Technology' (Hunton Privacy Blog, 16 June 2021) <https://www.huntonprivacyblog.com/2021/06/16/baltimore-passes-bill-banning-private-sector-use-of-facial-recognition-technology/> accessed 9 September 2021.

214 Ordinance 'Surveillance Technology in Baltimore' <https://baltimore.legistar.com/LegislationDetail.aspx?ID=4749282&GUID=3605654F-5629-41A1-BD96-89946A2C32FB&Options=&Search=&FullText=1> accessed 9 September 2021.

215 Ordinance 'Surveillance Technology in Baltimore' § 41-4 'Face surveillance technology' ('(…) (b) (2) "Face surveillance" means an automated or semi-automated process that assists in identifying or verifying an individual based on the physical characteristics of the individual's face (3) "Face surveillance system" means any computer software or application that performs face surveillance (…) "Face surveillance system" does not include a biometric security system designed specifically to protect against unauthorized access to a particular location or an electronic device (…) (c) Purchase prohibited. The City of Baltimore may not purchase or otherwise obtain a face surveillance system or face surveillance systems. (d) Contractor use prohibited. The City of Baltimore may not contract with another entity or individual, either directly or as a subcontract, for the use of face surveillance in the City').

216 Ordinance 'Surveillance Technology in Baltimore', 'Article 19. Police Ordinances', 'Subtitle 18. Surveillance' ('(…) § 18-1. Definitions (b) "Face surveillance" means an automated or semi-automated process that assists in identifying or verifying an individual based on the physical characteristics of an individual's face (…) (c) Face surveillance system (…) (1) (…) "Face surveillance system" means any computer software or application that performs face surveillance (…) (2) Exclusions (…) "Face surveillance system" does not include: (i) a biometric security system designed specifically to protect against unauthorized access to a particular location or an electronic device; or (ii) the Maryland Image Repository System (…) (e) (…) "Person" means: (1) an individual; (2) a partnership, firm, association, corporation, or other entity of any kind; (3) a receiver, trustee, guardian, personal representative, fiduciary, or representative of any kind; or (4) (…) the Mayor and City Council of Baltimore or an instrumentality or unit of the Mayor and City Council of Baltimore (…) § 18-2. Use of face surveillance technology prohibited A person may not obtain, retain, access, or use in Baltimore City: (1) any face surveillance system; or (2) any information obtained from a face surveillance system ').

Notably, in case of violation of the provisions on the ban related to private actors, the ordinance provides, not only for civil, but also for criminal remedies.[217] Last, both the city- and private actors-bans are expected to end in December 2022, unless research shows they need remain effective.[218]

6. Concreteness of the US initiatives: technology-specific regulation

In the following sections, we highlight five salient facts about the US initiatives that could inspire European audiences.

Firstly, there is unambiguous clarity about their precise scope, since they are explicitly targeted at certain technologies. Whereas in Europe visual/biometric data and facial recognition are covered by generic rules and principles on the ***processing*** of ***personal data*** (often of a ***sensitive*** nature, where they aim to ***uniquely identify*** an individual),[219] we see in the US tech-focused initiatives that do not always rely upon the potential to uniquely identify a natural person.[220]

On the one hand, it can be argued that the EU's broad and neutral approach can cover any emerging technology, as long as it involves processing of personal data. This is something positive: it reduces workload

217 Ordinance 'Surveillance Technology in Baltimore', 'Article 19. Police Ordinances', 'Subtitle 18. Surveillance' (' § 18-3. Penalties. (a) In general. Any person who violates any provision of this subtitle is guilty of a misdemeanor and, on conviction, is subject to a fine of not more than $1,000 or imprisonment for not more than 12 months or both fine and imprisonment. (b) Each day a separate offense. Each day that a violation continues is a separate offense ').

218 Ordinance 'Surveillance Technology in Baltimore' § 41-4 'Face surveillance technology' (' (e) (…) This section automatically expires on December 31, 2022, unless the City Council, after causing an appropriate study to be undertaken, conducting public hearings, and hearing testimonial evidence, finds that the prohibitions set forth in this section remain in the public interest, in which case this section may be extended for 5 more years '); Ordinance 'Surveillance Technology in Baltimore', 'Article 19. Police Ordinances', 'Subtitle 18. Surveillance' (' § 18-6. Termination of subtitle. This subtitle automatically expires on December 31, 2022, unless the City Council, after causing an appropriate study to be undertaken, conducting public hearings, and hearing testimonial evidence, finds that the prohibitions and requirements set forth in this subtitle remain in the public interest, in which case this section may be extended for 5 more years ').

219 GDPR, art 9(1); LED, art 10.

220 More concretely, at federal level, the 2019 CFRPA (section 2(5)) addresses 'facial recognition technology', which *may* have the capacity to uniquely identify a person. The FRBT Moratorium Act (section 3(a)) is targeted at both technology and data: biometric surveillance systems and information derived from such systems; here, the focus seems to be on surveillance information, rather than data allowing for the unique identification (see section 2). The 2020 NBIP Act expressly addresses biometric information that is not defined in the text and 'biometric identifiers' that do constitute 'uniquely identifying information' (see section 2(1)). The Data Protection Act of 2021 is primarily aimed at tackling high risk data practices via the creation of an independent agency. At state level, Illinois and Texas, like the above National Biometric Information Privacy Act (2020), address biometric identifiers; yet, unlike that federal initiative, these two state proposed regimes miss the 'unique'- (identification) element (see IBIPA, section 10 and Texas Business and Commerce Code (Sec 503.001), point (a)). Moreover, California, Washington and Indiana are close to the surveillance approach adopted by the aforementioned federal FRBT Moratorium Act. Indeed, California focuses more on surveillance technology (cameras) and related information (not necessarily leading to identification) (see California Assembly Bill No 1215, sections 2(b), 2(a)(2) and 2(a)(3)). Washington seems to be concerned with a concrete technology (facial recognition service) that can allow for surveillance practices (such as persistent tracking) (see Engrossed Substitute Senate Bill 6280, section 2(3)); and Indiana calls for conducting a particular policy regarding the use and impact of surveillance technology (even though the law mentions 'identity', no reference is made to 'unique' identification) (see House Bill 1238). Other state initiatives appear to be aimed at addressing concrete technologies/information and risks. New Jersey, for example, aims to subject facial recognition technologies to independent accuracy- and bias-assessments (see Assembly Bill 989); and California's GIPA tackles the processing of genetic data that are used for genetic testing purposes (it is reminded that 'genetic data' refer to 'any data, regardless of its format, that results from the analysis of a biological sample from a consumer, or from another element enabling equivalent information to be obtained, and concerns genetic material'; under the EU regime, genetic data are distinguished from biometric data; still, the former do give unique information about particular aspects (like health) of a natural person; see GDPR, art 4(13)). Furthermore, New York's Assembly Bill A6787D specifically addresses risks of biometric identifying technologies-implementations for children. In addition, Virginia's Senate Bill 1392 (though not specifically directed to biometric data) treats biometric data as 'data generated by automatic measurements of an individual's biological characteristics (…) that is used to identify a specific individual', whose processing is, in principle, prohibited (Senate Bill 1392, section 59.1-571). Last, at city level, Portland seems to be primarily concerned with surveillance aspects of face recognition technologies (like detection of facial traits) (see Portland's first Ordinance, Exhibit A, 'TITLE 34 DIGITAL JUSTICE', 'Chapter 34.10, Prohibit the use of Face Recognition Technologies by Private Entities in Places of Public Accommodation in the City of Portland', 34.10.020).

of regulators, who need not draft new laws for technologies already covered; it avoids having many laws at the risk of lagging behind the many technologies;[221] it is focused on long-term objectives and strategies, rather than near-term goals (whose achievement would tackle, perhaps, merely practical issues); and it takes into due account the fact that technologies are developing rapidly, as well as the fact that specific rules on concrete technologies, as a straightforward response, might fail to address such rapid changes.[222] Moreover, as Murphy has rightly pointed out, tech-neutral laws are not restricted on the grounds of (perhaps arbitrary) technological classifications and can better address behaviours, the impact of the technology (whereas tech-specific regulations may fail to regulate what occurs, by focusing on how it occurs).[223] Furthermore, a broad approach may be preferable, since specific laws and their (possibly narrow) interpretation by courts could exclude certain technologies and, thus, leave individuals exposed to unregulated technological implementations.[224] Moreover, considering certain biometric processing as extra-risky is an additional positive feature. Indeed, national experience has proved the protective value of art. 9 GDPR.[225]

On the other hand, the EU's abstract approach, sometimes accompanied by lack of clarity, can create legal uncertainty: how should the EU legal provisions be applied to concrete contexts and technologies?[226] Are technologies that may not directly pursue identification-goals covered by the biometric-provisions of

221 For the metaphor, where the law is seen as the tortoise that lags behind the hare (the technology), see Lyria Bennett Moses, 'Agents of Change: How the Law 'Copes' with Technological Change' (2011) 20(4) Griffith Law Review 763.

222 For interesting arguments for a broader approach to technological implementations, see: Hin-Yan Liu and others, 'Artificial Intelligence and Legal Disruption: A New Model for Analysis' (2020) 12(2) Law, Innovation and Technology 205.

223 Maria Helen Murphy, *Surveillance and the Law* (Routledge 2019) 77-79. Besides, it can be argued that tech-specific regulations can be more effective and ensure legal certainty, *only if* there is clear consensus on the definition of a certain technology *and* the law reproduces such definition.

224 This was the case with *Duguid*, where the US Supreme Court, opting for a rather narrow interpretation of the ATDS (automatic telephone dialing systems), found that Facebook's equipment (login notification system) did not constitute an ATDS and was, hence, not subject to specific legal provisions, namely the Telephone Consumer Protection Act of 1991. See *Facebook, Inc v Duguid et al*, No 19-511 (1 April 2021); Hunton Andrews Kurth, 'Supreme Court Adopts Narrow Interpretation of ATDS' (Hunton Privacy Blog, 1 April 2021) <https://www.huntonprivacyblog.com/2021/04/01/supreme-court-adopts-narrow-interpretation-of-atds/> accessed 6 September 2021.

225 For example, in the Netherlands, the Data Protection Authority has recently found that the processing by the employer firm of its employees' biometrics (fingerprints) for authentication and/or security purposes was disproportionate: consent cannot be regarded as a valid processing-basis, given imbalance of the employer-employee relationship; and biometric data processing for authentication/security goals can only be allowed, where there is no other less intrusive means available. See Hunton Andrews Kurth, 'Dutch DPA Fines Company 750,000 Euros for Unlawful Employee Fingerprint Processing' (Hunton Privacy Blog, 12 May 2020) <https://www.huntonprivacyblog.com/2020/05/12/dutch-dpa-fines-company-750000-euros-for-unlawful-employee-fingerprint-processing/> accessed 6 September 2021.

226 Such questions have recently been the subject of discussion of the Council of the European Union. See Council of the European Union, 'Council position and findings on the application of the General Data Protection Regulation (GDPR)' (Council of the European Union, 19 December 2019) paras 14-15: '(14) At the same time, the Council notes that new phenomena, particularly emerging technologies, also provide new challenges for the protection of personal data as well as for the protection of other fundamental rights such as the prohibition of discrimination. Those challenges relate to topics such as the use of big data, artificial intelligence and algorithms, as well as the internet of things and block-chain technology. The same applies for the use of technologies such as facial recognition (…) In order to keep up with emerging technologies, the Council deems it necessary to monitor and assess the relationship between technological development and the GDPR at EU level on a continuing basis (…) (15) The Council underlines that the GDPR was drafted to be technologically neutral and that its provisions already address these new challenges. The Council finds it essential to consider that the GDPR, and more generally the EU's legal framework for the protection of personal data, is a prerequisite for the development of future digital policy initiatives. However, in light of the above, the Council deems that it is necessary to clarify as soon as possible how the GDPR applies to the aforementioned new technologies' <data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/en/pdf%20at%207> accessed 6 September 2021. Remarkably, in other areas, namely health data processing, the EU seems to accept the need for concrete rules. In this regard, see DG Health and Food Safety, 'Assessment of the EU Member States' rules on health data in the light of GDPR' (Specific Contract No SC 2019 70 02 in the context of the Single Framework Contract Chafea/2018/Health/03, European Commission 2021) <https://ec.europa.eu/health/sites/health/files/ehealth/docs/ms_rules_health-data_en.pdf> accessed 6 September 2021.

the GDPR? Such uncertainties could leave data subjects exposed to unregulated technologies or halt the introduction of new models to the market.[227]

As technologies are getting more and more precise, their implementations can become more intrusive. The example of face recognition, compared to traditional biometric applications (like fingerprinting), can support this claim. Face recognition models can gather facial traits through the capturing of a mere image; and this, without the target knowing such a capturing/gathering, without her/him consenting to it and/or without her/him participating in it.[228] Then, the US piece meal approach to such precise technologies may be preferable. Designers of face recognition technology or biometric surveillance models may better foresee how the 2019 CFRP Act or the 2020 FRBT Moratorium Act could apply to their case and, accordingly, decide whether and how to enter the market; similarly, individuals potentially subjectable to these technologies can be more certain about the way in which they may be protected against possible violation of the provisions of the above proposed legal instruments.

Still, on the negative side, such instruments may fail to capture technologies that do not fall under the 'face recognition umbrella'; regulation of these non-face-recognition tools would require the introduction of new instruments –after the often lengthy law-making procedure. In our view, this risk does not materialise in the US regulation reviewed here.[229] On the contrary, with extremely risky uses of technologies, like face recognition-implementations, there is a need to reverse the traditional innovation-friendly logic. A policy, like 'no facial recognition unless there is an explicit legal basis', as warranted by the 2020 FRBT Moratorium Act, seems to be the justified starting point; one that can also be found in the LED (and to a lesser extent in art. 9 GDPR).

227 For a discussion, see Letícia Silveira Tavares, 'Regulating the Imbalance of Power Created by Facial Recognition' (n 57) 27: 'Some argue that the EU data protection laws provide the right model to regulate FRT, since it has a principles driven approach that allows for innovation and limits intrusive or excessive uses. However, it is important to note that the rise of specific regulation for the use of FRT is still necessary, if not essential. Due to the General Data Protection Regulation (GDPR)'s technological neutrality, the regulation fails to address facial recognition technology, leaving individuals – and companies – at risk (…) While the GDPR's scope is limited to the use of biometrics for identification purposes, several questions remain unanswered and become a challenge for the private sector when choosing their applicable lawful basis for the use of FRT, as well as in appropriately applying the principles of data minimization and proportionality. Some argue that the GDPR has actually been affecting FRT market practices for lack of clarity, for example, the deletion of Microsoft's facial recognition technology database'.

228 For a discussion on silent versus salient technologies and the problem of inaccessibility/opacity rendering inspection hard, see Lucas Introna and David Wood, 'Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems'(2004) 2(2-3) Surveillance and Society 177, 183. Remarkably, the European Court of Human Rights has recently addressed the way in which face recognition-implementations may alter the degree of interference (for example, through correlations of data stored on databases); see *Gaughran v the United Kingdom* Application no 45245/15 (ECtHR, 13 February 2020), paras 67-70.

229 However, experience from other contexts, such as the recent *Duguid*-case of the US Supreme Court (see above n 206), has demonstrated that the above risk can in fact be materialised and let users exposed to technological uses that are not covered by the law.

7. US clarity on the scope: who is protected?

The EU legal regime captures both private and public entities; the primary duty-bearer is the controller.[230] The US initiatives are targeted at public and/or private actors.[231] Furthermore, the EU legal regime protects the 'data subject', a natural person, irrespective of her/his commercial aspects or her/his residence (or, in some cases, her/his location).[232] The US initiatives appear to be aimed at protecting the subjects of the information at hand and/or certain (vulnerable) aspects of the individuals concerned.[233]

One could argue that certain US proposals, being context- or technology-specific, are narrower that the EU's scope that covers any natural person. However, in many cases, such a claim may be unfair. For example, ***end-users*** protected under the 2019 CFRP Act could in fact be anyone. The same can be true with the FRBT Moratorium Act of 2020 that covers anyone potentially subjectable to face recognition surveillance; or with the 2020 NBIP Act concerned with the subject of biometric information or identifiers. Hence, not only the individuals protected can be anyone, any natural person (as is the case with the EU scheme); but also the person protected can, under the US scheme, be better aware of the 'why' and the 'how' she/he is protected: eg, as an ***end-user*** of the technology at hand or as an individual subjectable to biometric surveillance. Such considerations, taken together with the above-analysed clarity of the US-guaranteed protection (of both individuals and developers of technologies), could support the argument that the US proposals are more shielding than the EU legal framework.

230 That is, 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'. It is reminded that the GDPR binds the controller that can be a 'natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data' (GDPR, art 4(7)); and the LED applies to public authorities, as well as private entities performing public functions (LED, art 3(7)).

231 More precisely, at federal level, the CFRPA, adopting a GDPR-approach when defining the 'controller' as the person determining the purposes and means of (facial recognition) data processing, explicitly excludes governments (federal, state or local) and law enforcement, national security and intelligence agencies (see section 2(2) and (3)). Similar is the case with the 2020 NBIP Act (section 2(3)). On the other hand, the FRBT Moratorium Act (section 3(a)) is expressly directed to federal actors. Last, the key addressees of the Data Protection Act are data aggregators processing significant amounts of data for commercial purposes. At state level, Illinois and Texas aim to bind private entities (IBIPA, section 10; Texas Business and Commerce Code Sec 503.001, referring to commercial contexts); whereas Washington and Indiana focus on state and local authorities (Engrossed Substitute Senate Bill 6280, section 3; Indiana House Bill 1238 (2020), referring to state or local law enforcement actors). California, aiming to regulate in both civil and criminal areas, addresses, on one hand, law enforcement (California Assembly Bill No 1215, section 2(b)) and, on the other hand, genetic-related firms (GIPA, section 56.18(b)(5)). New Jersey's Assembly Bill 989 (2020) has a precise target: the attorney general who must guarantee accuracy via the arrangement of independent audits and tests and report to the Legislature; New York's Assembly Bill A6787D refers to concrete biometric implementations in public and private schools; and Virginia's Senate Bill 1392 addresses private entities as controllers (determining the purposes and the means of the processing) (section 59.1-571). At city level, Portland focuses on both private and public actors (Portland's first and second ordinances).

232 On the territorial scope, see GDPR, art 3.

233 This can be demonstrated at federal level: CFRPA (section 3(a)(1)) protects end users; the FRBT Moratorium Act (section 2) seems to be concerned with anyone potentially subjectable to surveillance via face recognition; and the 2020 NBIP Act(section 2(1)) protects the subject of biometric information or identifiers. At state level, Illinois, like the 2020 NBIP Act, focuses on the subject of biometric information and identifiers (IBIPA, section 10); whereas Texas and California (in its civil initiative) look at particular commercial/consumer aspects of natural persons (Texas Business and Commerce Code (Sec 503.001); Genetic Information Privacy Act, referring to consumers). Other states, aimed at regulating state actors, protect anyone who may be subject to the restricted/prohibited practice at hand. Namely, California, with its criminal initiative, aims to protect those subjectable to law enforcement-surveillance (California Assembly Bill No 1215, section 2(b)); Washington looks at those who may be affected by face recognition practices exercised by state or local authorities (Engrossed Substitute Senate Bill 6280, section 2(3)); in Indiana, protection aims to cover those potentially subjected to surveillance by law enforcement (House Bill 1238); New Jersey's initiative captures any individual, who may be affected by biased or inaccurate facial recognition technologies (Assembly Bill 989); New York's Assembly Bill A6787D is aimed at the protection of vulnerable persons, namely children; and Virginia is expressly concerned with consumers (Senate Bill 1392, section 59.1-571). At city level, Portland focuses on the protection of the residents and visitors of the city (therefore, location seems to play a role in determining the protective scope) (see for example, Portland's first Ordinance, section 1, point 1).

8. US precision on consent, information duties, function creep and other requirements

The focus of the US initiatives often leads to more elaboration and ***finesse*** of the data protection requirements and duties imposed. ***Below***, we make seven points, which may be particularly inspirational for EU audiences.

Consent

The US regime appears more demanding regarding the duty to obtain consent.[234] As analysed above, in some instances, the US regulator goes beyond requirements known from the EU law (such as the need for 'specific' or 'informed' consent) and focuses on the independent will of the data subject; attention is paid to the genuine will of the person concerned, who must be free from outside control.

Consent

Even though the US and the EU provisions on consent share in common several elements,[235] there are some important differences demonstrating supremacy of certain US proposals. A prime example is the NBIPA, which requires that consent be 'specific, discrete, freely given, unambiguous, and informed written consent' (elements identical to the GDPR's demands), but, moreover, without subjection to force or influence[236] (elements perhaps implied by, albeit, absent in the text of the EU legal instruments).[237]

Duty to inform

In the US, the duty to inform is, in some instances, accompanied by stringent requirements, such as the obligation to conduct accountability reports.

234 CFRPA, section 2(1) (demanding consent to data processing be of an affirmative nature and involve an individual, voluntary and explicit agreement); NBIPA, sections 3(b)(1) and 2(4) (prohibiting the obtaining of biometric data, save from where, among others, the individual has already provided for her 'specific, discrete, freely given, unambiguous, and informed written consent', without having being subjected to force or influence); Illinois IBIPA, section 15(b) and (d) (prohibiting private entities from obtaining and disseminating biometric identifiers and biometric information, save where, among others, the person concerned haas given consent in the form of a 'written release'); Texas Business and Commerce Code (Sec 503.001), points (b) and (c) (prohibiting the capturing, disclosing or exploiting of biometric identifiers, except where, among others, the individual has given her consent); GIPA, section 56.181(a)(2) (mentioning the requirement of obtaining the express and, where applicable, separate consent of the consumer for the collection, use, and disclosure of relevant data); Virginia Senate Bill 1392, section 59.1-571, defining consent as 'a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer'; section 59.1-574, prohibiting the processing of biometric data, save where consent is obtained.

235 Compare GDPR, arts 9(2)(a) (referring to *explicit* consent) and 4(11) (defining consent as 'any *freely given*, *specific*, *informed* and *unambiguous* indication of the data subject's wishes by which he or she, by a statement or by a *clear affirmative action*, signifies *agreement* to the processing of personal data relating to him or her' (own emphasis)) with CFRPA, section 2(1): '*affirmative consent* means the consent of an end user that involves an *individual*, *voluntary*, and *explicit agreement* to the collection and data use policies of a controller' (own emphasis); NBIPA, section 2(4): '*written release* means (A) *specific*, discrete, *freely given*, *unambiguous*, and *informed* written consent given by an individual who is not under any duress or undue influence of an entity or third party at the time such consent is given' (own emphasis); GIPA, section 56.18(b)(6): '*Express consent* means a consumer's *affirmative* authorization in response to a clear, meaningful, and prominent notice regarding the collection, use, maintenance, or disclosure of genetic data for a specific purpose. The nature of the data collection, use, maintenance, or disclosure shall be conveyed in clear and prominent terms in such a manner that an ordinary consumer would notice and understand it. Express consent *cannot be inferred from inaction*. Agreement obtained through use of dark patterns does not constitute consent' (own emphasis); Virginia Senate Bill 1392, section 59.1-571 treating consent as 'a clear affirmative act signifying a consumer's *freely given*, *specific, informed, and unambiguous* agreement to process personal data relating to the consumer' (own emphasis).

236 NBIPA, sections 3(b)(1) and 2(4).

237 Although there seems to be no guidance on how this concept should be interpreted in practice, one can see elements known from other (for instance, judicial) fields that can promote independence of the person concerned (eg, judges need remain free from influence, when adjudicating a case).

Duty to inform

The EU legal regime provides for an information-requirement (right to information);[238] and, as is the case with the US, the right to information can be limited, under the LED, by domestic law.[239] In the US laws under review, we can see the duty to inform coming in many shapes and sizes. For example, there are requirements referring to the making of the processing policy available to the public or the individual concerned.[240] Even though this duty may, under some US initiatives, be conditional upon the particular circumstances and context of the processing,[241] there are instances where the US appear more demanding. In this regard, Washington, in addition to its 'notice of intent', requires that there be a detailed 'accountability report' explicitly referring to numerous minimums; from technology-related information (like the name/version/vendor of the service or the foreseeable possibilities beyond those covered by the intended use) to the types of data analysed, the potential benefits, information management policies and protocols, data integrity strategies, testing as well as error rates and their possible effect or channels for scrutiny and feedback.[242] Although Washington does not expressly demand external audit of the accountability report by independent parties, its requirements of, first, communication of the report to the public (for consultation and commenting) and, second, submission of the report to a legislative authority appear to provide for enhanced safeguards (eg, compared to the EU's data protection impact assessments that are required only in certain contexts).

Function creep

The US approach seems to be more protective in some situations, where it requires that the purpose of the processing be explicit ***and*** presented to the end-user ***and*** remain unaltered.

Function creep

Repurposing of the processing is expressly prohibited, under the 2019 CFRP Act,[243] and conditioned upon prior review and consultation, under Washington's Engrossed Substitute Senate Bill 6280.[244] Although a function creep-prohibition can be found in the purpose limitation-related obligations, set out

238 GDPR, arts 13-14; LED, art 13.

239 LED, art 13(3): 'Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to: (a) avoid obstructing official or legal inquiries, investigations or procedures; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; (e) protect the rights and freedoms of others'.

240 CFRPA, section 3(a)(1) (prohibiting the use by the controller of facial recognition technology for the purpose of facial recognition data collection, unless there is an opt-in and, if possible, a notice providing intelligible information on the technology); NBIPA, sections 3(a)(1) (imposing the duty to make publicly available a written policy on retention and destruction of biometric information and biometric identifiers) and 3(f): 'Any business that collects, uses, shares, or sells biometric identifiers or biometric information, upon the request of an individual, shall disclose, free of charge, any such information relating to such individual collected during the preceding 12-month period'); Illinois IBIPA, section 15(b) (prohibiting private entities from obtaining biometric identifiers and biometric information, save where, among others, the person concerned has been sufficiently informed); Texas Business and Commerce Code (Sec 503.001), point (b) (prohibiting the capturing of biometric identifiers in commercial contexts, except where, among others, the individual at issue has been informed); Washington Engrossed Substitute Senate Bill 6280, section 3(1) and (2) (demanding that authorities submit a 'notice of intent', regarding the use of a facial recognition service and its concrete purpose, and then prepare an 'accountability report' that must be clear and comprehensive as to certain minimums), as well as section 3(5) (requiring that the 'accountability report' be made publicly available); GIPA, section 56.181(a)(1) (referring to the duty to make the policy on the 'collection, use, maintenance, and disclosure' of genetic data available to the consumer); Indiana House Bill 1238 (demanding that state or local law enforcement actors conduct a 'surveillance technology impact and use policy' that need be made available to the public through their webpage).

241 See for example CFRPA, section 3(a)(1): 'it shall be unlawful for a controller to knowingly use facial recognition technology to collect facial recognition data, unless the controller *to the extent possible*, if facial recognition technology is present, provides to the end user (…) a concise notice that facial recognition technology is present, and, *if contextually appropriate*, where the end user can find more information about the use of facial recognition technology by the controller' (own emphasis).

242 Engrossed Substitute Senate Bill 6280, section 3(1) and (2).

243 CFRPA, section 3(a)(3): 'repurpose facial recognition data for a purpose that is different from those presented to the end user'.

244 Engrossed Substitute Senate Bill 6280, section 3(7).

in the GDPR,[245] it can be claimed that the above US initiatives appear more explicit, for example, by demanding no alteration of the explicit objective, as this objective has been presented to the end-user, of facial recognition information.[246]

Exceptional disclosure on the basis of a more rigorous consent-model

The US approach appears more user-friendly, when exceptionally allowing for disclosure of relevant data upon obtaining consent of the individual who is ***not*** 'under any duress or undue influence of an entity or third party'.

Exceptional disclosure on the basis of a more rigorous consent-model

The majority of the above-discussed US initiatives provide for the duty not to share/disclose/disseminate protected information (such as biometric identifiers, biometric information or face recognition data).[247] This duty can be conditional upon certain circumstances.[248] Under the EU regime, general rules apply with regard to this issue: disclosure and dissemination are among the operations constituting 'processing' and can benefit from the Article 9 GDPR-exceptions.[249] In biometric contexts, this processing (though in principle prohibited) can therefore be exceptionally permitted (under the GDPR).[250] Remarkably, in the LED, such a processing of biometric data is permitted by default, where 'strictly necessary',

245 GDPR, art 5(1)(b): 'Personal data shall be (…) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (…)') in combination with art 6(4): 'Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation'.

246 CFRPA, section 3(a)(3): 'repurpose facial recognition data for a purpose that is different from those presented to the end user'. See also Virginia Senate Bill 1392, section 59.1-574, establishing the duty not to 'process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent'.

247 CFRPA, section 3(a)(4); NBIPA, section 3(d); IBIPA, section 15(d) ; Texas Business and Commerce Code (Sec 503.001), point (c); GIPA, section 56.181(f).

248 NBIPA, section 3(d), using the term 'may' instead of 'shall': 'A private entity in possession of a biometric identifier or the biometric information (…) *may not* disclose ' (own emphasis); IBIPA, section 15(d): 'No private entity (…) *may* disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information *unless*: (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction' (own emphasis); Texas Business and Commerce Code (Sec 503.001), point (c) (allowing for exceptions, where disclosure of biometric identifiers is grounded on consent, serves the goal of finalising a transaction that the owner of the identifier permitted, is demanded by the law or is linked to law enforcement); GIPA, section 56.181(f), providing for exceptions: '(2) *may disclose* a consumer's genetic data or biological sample to an entity described in paragraph (1) if all of the following are true (A) The entity is not primarily engaged in administering health insurance, life insurance, or long-term care insurance, disability insurance, or employment (B) The consumer's genetic data or biological sample is not disclosed to the entity in that entity's capacity as a party that is responsible for administering, advising, or making decisions regarding health insurance, life insurance, long-term care insurance, disability insurance, or employment (C) Any agent or division of the entity that is involved in administering, advising, or making decisions regarding health insurance, life insurance, long-term care insurance, disability insurance, or employment is prohibited from accessing the consumer's genetic data or biological sample' (own emphasis).

249 GDPR, art 4(2): 'processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

250 GDPR, art 9(1) and (2).

'subject to appropriate safeguards for the rights and freedoms of the data subject' and under certain circumstances, exhaustively described in the LED.[251]

One can note that both (EU-US) approaches to exceptional disclosure or communication can share common features. A prime example is the demand for obtaining consent, which, as analysed above, is a legitimising factor in both systems. The consent-basis has been subjected to critique. How could data subjects become educated to give truly informed consent? Or how could consent work in public contexts (like state surveillance), where non-waivable human rights (such as to move and enter a public area) could be involved? Such questions refer to the very consent-model that is present in both frameworks; departing from such a model or seeing consent as the last resort might be preferable as placing the burden on the shoulders of controllers, instead of the (perhaps uneducated) user.[252] In any event, it is reminded that the US case-specific provisions (especially, the NBIPA requiring the person consenting be ***not*** 'under any duress or undue influence of an entity or third party')[253] allow for a more rigorous consent-model. This can in turn make the argument for enhanced user-friendliness of the US approach.

Duty to review and audit

The US regime requires human intervention that is meaningful ***and*** takes place prior to any decision-making that could affect the individual concerned; moreover, it demands specific auditing with a view to eliminating bias.

Duty to review and audit

The 2019 CFRP Act requires that controllers employ 'meaningful human review' before taking decisions capable of affecting an individual;[254] a similar or identical obligation can be found in Washington's Engrossed Substitute Senate Bill 6280.[255] Moreover, the federal 2019 CFRP Act demands audits of face recognition technologies (that are provided as online services) by independent parties, who must be en-

251 LED, art 10: 'shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only: (a) where authorised by Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; or (c) where such processing relates to data which are manifestly made public by the data subject'.

252 See in more detail: Letícia Silveira Tavares, 'Regulating the Imbalance of Power Created by Facial Recognition'(n 57) 27-28: 'Historically, the notice and choice focused approach of educating consumers about companies' data policies and practices has not been successful (…) It is notorious that placing the responsibility on consumers to educate themselves with privacy policies and notices, before making decisions regarding their privacy is not realistic (…) nor fair (…) The same logic would apply to a framework that would expect a data subject consent (…) to be enough for the processing of facial biometrics. It could be considered unreasonable in both private and public use of the technology. Furthermore, in the context of having facial biometrics collected, the consent model would make some of the advantages of the technology non-viable, for example, simplification of payment procedures, as it would take time for the notice to be read and understood by the consumer. Similarly, displaying a privacy notice of FRT when using public space surveillance is also arguably not feasible, since the non-acceptance would restrict our right to freely move in the public space. Therefore, the responsibility of a fair and transparent use of FRT, if any, must fall on the ones deploying the technology'.

253 NBIPA, section 2(4).

254 CFRPA, section 3(c): 'A controller (…) shall employ meaningful human review prior to making any final decision based on the output of facial recognition technology if the final decision (…) (1) may result in a reasonably foreseeable and material physical or financial harm to an end user; or (2) may be unexpected or highly offensive to a reasonable end user'.

255 Engrossed Substitute Senate Bill 6280, section 5, stipulating that, where a face recognition system is aimed at making decisions that 'produce legal effects concerning individuals or similarly significant effects concerning individuals', such decisions need be subjected to 'meaningful human review'. Such duties resemble the GDPR's demand that controllers provide for measures to guarantee human intervention (GDPR, art 22(3)). Yet, under the GDPR, this intervention is only allowed in concrete cases (where automated decisions are necessary for the entering/performance into/of a contract or rely upon the data subject's explicit consent; GDPR, art 22(2)(a) and (c)); and the textual interpretation of the intervention-provision (art 22 GDPR, mentioning the need to protect the data subject's right to challenge the decision made) suggests that such an intervention can come after (not prior to) the automated decision. See GDPR, art 22(1) and (3): ' The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision'.

abled to check for bias and inaccuracies.[256] Such precise rules on audits, in our view, go beyond general 'investigation' (audit-related) powers delegated to the European (independent) supervisory authorities;[257] this, even though it can be argued that, in light of the EU's accuracy-principle, regular and careful inspections/audits must be performed by the controller or other actors (for instance, through the intervention of the data protection officer).[258]

Consent revocation, security, access and retention/deletion

Although both the EU and the US impose obligations concerning consent revocation, security, access and retention or deletion of relevant data, the US provisions are more clear and detailed; for example, with strict deadlines for deletion.

Consent revocation, security, access and retention/deletion

Some obligations imposed by several US initiatives (in particular, California's concrete provisions/duties on consent revocation,[259] security, access to data and retention/deletion of data,[260] as well as Illinois' and Texas' deletion-related provisions)[261] have their EU-counterparts;[262] but these lack the clarity and detailedness of the US provisions that, for instance, impose strict deadlines for the deletion.

Prohibition of discrimination, duty not to profit, standards of care and confidentiality

Several US initiatives provide for obligations that are completely absent in the EU. These include: the prohibition on discrimination or profiting, the application of standards of care or the treatment of biometric data as particularly sensitive ***and*** confidential information.

256 CFRPA, section 3(d): 'A covered entity that makes a facial recognition technology available as an online service shall make available an application programming interface to enable at least 1 third party that is legitimately engaged in independent testing to conduct reasonable tests of the facial recognition technology for accuracy and bias'. It is added that New Jersey's Assembly Bill 989 also subjects facial recognition technologies to independent accuracy- and bias-checking.

257 GDPR, art 58(1)(b): 'Each supervisory authority shall have all of the following investigative powers: to carry out investigations in the form of data protection audits'.

258 GDPR, art 39(1)(b): 'The data protection officer shall have at least the following tasks: (…) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits'.

259 GIPA, section 56.181(b) and (c): 'A company (…) shall provide effective mechanisms (…) for a consumer to revoke their consent after it is given (…) If a consumer revokes the consent that they provided (…) the company shall honor the consumer's consent revocation as soon as practicable'.

260 GIPA, section 56.181(d): 'The direct-to-consumer genetic testing company, or any other company that collects, uses, maintains, or discloses genetic data collected or derived from a direct-to-consumer genetic testing product or service, or provided directly by a consumer, shall (1) Implement and maintain reasonable security procedures and practices to protect a consumer's genetic data against unauthorized access, destruction, use, modification, or disclosure (…) (2) Develop procedures and practices to enable a consumer to easily (…) access the consumer's genetic data (…) delete the consumer's account and genetic data, except for genetic data that is required to be retained by the company to comply with applicable legal and regulatory requirements'.

261 IBIPA, section 15(a): 'A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first'); Texas Business and Commerce Code (Sec 503.001), points (c), (c-1) and (c-2): 'A person who possesses a biometric identifier of an individual that is captured for a commercial purpose shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except as provided by Subsection (c-1)'.

262 GDPR, art 7(3) (on consent withdrawal); art 32 (on security); art 15 (on access to data); and art 17 (on deletion).

Prohibition of discrimination, duty not to profit, standards of care and confidentiality

Under some US initiatives, certain duties are aimed at prohibiting discrimination or profiting, applying standards of care or treating biometric data as particularly sensitive and confidential information. More precisely, at federal and state level, there is a duty of non-discrimination applicable to concrete contexts (such as face recognition-implementations).[263] Under the EU regime, discrimination-related concerns, though apparent in recitals of the GDPR (especially those concerning automated processing),[264] seem to lack specificity and, importantly, have not led to the imposition of concrete duties on the controller. Furthermore, the federal 2020 NBIP Act, as well as Illinois' and Texas' initiatives, provide for the duty not to profit from biometric information and biometric identifiers,[265] but also the duty to apply industry-standards ('reasonable standard of care') or treat biometric identifiers or biometric information in a way identical to or more shielding than that in which sensitive or confidential information is addressed.[266] Therefore, things in the US appear way more explicit.

9. Use of prohibitions on (aspects of) biometric and visual surveillance

A salient fact about the US initiatives is their 'big no' to certain processing operations that seems incomparable with the EU's 'no, but'.[267] Some examples:

California's Assembly Bill No 1215, in an absolute manner, prohibits law enforcement actors from engaging in biometric surveillance via their cameras or information collected by these devices:

'A law enforcement agency or law enforcement officer shall not install, activate, or use any biometric surveillance system in connection with an officer camera or data collected by an officer camera' (section 2(b)).

The 2020 FRBT Moratorium Act prohibits any exercise of biometric surveillance by the federal government until precise laws (and Congress authorisation) are in place:

263 CFRPA, section 3(a)(2): 'it shall be unlawful for a controller to knowingly (…) use the facial recognition technology to discriminate against an end user in violation of applicable Federal or State law'); GIPA, section 56.181(e): 'A person or public entity shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this chapter'. It is added that Virginia (regulating in commercial areas), as well as Washington and New Jersey (regulating in non-commercial contexts) also provide for non-discrimination-related obligations (Virginia Senate Bill 1392, section 59.1-574; Engrossed Substitute Senate Bill 6280, section 6; New Jersey's Assembly Bill 989); and that the risk of unjustifiable discrimination against minorities is among the main reasons why the city of Portland plans to ban face recognition technology (Portland's first Ordinance, section 1, points 3, 9).

264 See for example GDPR, recitals 71, 75, 85.

265 NBIPA, sections 3(c) and 3(d); IBIPA, section 15(c); Texas Business and Commerce Code (Sec 503.001), point (c).

266 NBIPA, section 3(e); IBIPA, section 15(e); Texas Business and Commerce Code (Sec 503.001), point (c).

267 Nowhere in the EU can we find these principled American prohibitions that can even be unconditional. We recall that art. 9 GDPR sees the prohibition of biometric data processing as the rule; albeit, it provides for a long list of exceptions, as well as for the opportunity for national laws to introduce further exceptional conditions (see art. 9(2) and (4) GDPR). The desired prohibition-as-a-rule can then be easily, legitimately circumvented. Moreover, the LED (art. 10) expressly allows for the processing of biometric data; this, as the principle. Although stringent conditions need be met, the safeguards for the data subject are admittedly limited.

'it shall be unlawful for any Federal agency or Federal official, in an official capacity, to acquire, possess, access, or use in the United States (1) any biometric surveillance system; or (2) information derived from a biometric surveillance system operated by another entity (…) the prohibition set forth in subsection (a) does not apply to activities explicitly authorized by an Act of Congress that describes, with particularity (1) the entities permitted to use the biometric surveillance system, the specific type of biometric authorized, the purposes for such use, and any prohibited uses; (2) standards for use and management of information derived from the biometric surveillance system, including data retention, sharing, access, and audit trails; (3) auditing requirements to ensure the accuracy of biometric surveillance system technologies, standards for minimum accuracy rates, and accuracy rates by gender, skin color, and age; (4) rigorous protections for due process, privacy, free speech and association, and racial, gender, and religious equity; and (5) mechanisms to ensure compliance with the provisions of the Act' (section 3(a) and (b)) .

The Data Protection Act of 2021 prohibits data aggregators and service providers from engaging in certain activities (such as committing 'unlawful, unfair, deceptive, abusive, or discriminatory acts or practices' or re-identifying 'an individual, household, or device from anonymized data'):

'It shall be unlawful for (…) (1) any data aggregator or service provider to commit any act or omission in violation of this Act, Federal privacy law, or any rule or order issued by the Agency under this Act; (2) any data aggregator or service provider to commit any unlawful, unfair, deceptive, abusive, or discriminatory acts or practices in connection with the collection, processing, or sharing of personal data; (3) any data aggregator or service provider to fail or refuse as required by this Act or Federal privacy law, or any rule or order issued by the Agency thereunder (…) (A) to permit access to or copying of records; (B) to establish or maintain records; or (C) to make reports or provide information to the Agency; (4) any person to knowingly or recklessly pro4 vide substantial assistance to a data aggregator or service provider in violation of this Act or Federal privacy law, or any rule or order issued thereunder, and notwithstanding any provision of this Act, the provider of such substantial assistance shall be deemed to be in violation of this Act or Federal privacy law to the same extent as the person to whom substantial assistance is provided; or (5) any person, data aggregator, or service provider to re-identify, or attempt to re-identify, an individual, household, or device from anonymized data, unless such person, data aggregator, or service provider is conducting authorized testing to prove personal data has been anonymized' (section 12) .

New York's Assembly Bill A6787D bans the implementation (that is, purchase and use) of biometric technologies in public and private schools until 1 July 2022 or until these technologies are proven safe and authorised by the State Education Commissioner:

'(…) Public and non-public elementary and secondary schools, including charter schools, shall be prohibited from purchasing or utilizing biometric identifying technology for any purpose, including school security, until July first, two thousand twenty-two or until the commissioner authorizes such purchase or utilization as provided in subdivision three of this section, whichever occurs later'.

Portland's Ordinance (34.10.030) bans face recognition:

> '(…) a Private Entity shall not use Face Recognition Technologies in Places of Public Accommodation within the boundaries of the City of Portland'.[268]

Baltimore's Ordinance prohibits certain face recognition uses by the city and private actors:

> '(c) (…) The City of Baltimore may not purchase or otherwise obtain a face surveillance system or face surveillance systems. (d) (…) The City of Baltimore may not contract with another entity or individual, either directly or as a subcontract, for the use of face surveillance in the City';[269]
> '(…) § 18-2 (…) A person may not obtain, retain, access, or use in Baltimore City: (1) any face surveillance system; or (2) any information obtained from a face surveillance system'.[270]

10. More practical organized remedies

Save from Washington, Indiana, New Jersey and New York,[271] the above-discussed US initiatives provide for civil remedies.[272] In certain cases, this provision may be connected with the focus on commercial dimensions of the protected persons (for instance, end users[273] or consumers);[274] put simply, such commercial contexts typically call for the application of civil (rather than criminal) law. A prime example is the 2019 CFRP Act –aimed at the protection of end users– that expressly classifies any breach of its provisions (on prohibited conducts) as unfair or deceptive act/practice[275] (and, therefore, makes competition-related laws applicable).[276] The Facebook-cases (analysed in the Illinois-section ***above***) can offer useful insights into the way in which and the degree to which civil (perhaps negotiated, settled) penalties may guarantee effective protection.

Furthermore, Portland provides for the opportunity to have 'a cause of action against the Private Entity in any court of competent jurisdiction for damages sustained as a result of the violation or $1,000 per day for each day of violation, whichever is greater and such other remedies as may be appropriate'.[277] A

268 It is reminded that Portland provides for an exception to that ban: 'The prohibition in this Chapter does not apply to use of Face Recognition Technologies: A. To the extent necessary for a Private Entity to comply with federal, state, or local laws; B. For user verification purposes by an individual to access the individual's own personal or employer issued communication and electronic devices; or C. In automatic face detection services in social media applications'. Portland's first Ordinance, 34.10.040.

269 Ordinance 'Surveillance Technology in Baltimore' § 41-4 'Face surveillance technology'.

270 Ordinance 'Surveillance Technology in Baltimore', 'Article 19. Police Ordinances', 'Subtitle 18. Surveillance'.

271 The absence of remedies-related provisions in these state initiatives could be due to the fact that the addressees duty-bearers (public authorities or schools) are already bound by concrete legal provisions, as well as the new duties introduced by these initiatives (like the obligation to prepare an 'accountability report' under Washington's Engrossed Substitute Senate Bill 6280).

272 See for example NBIPA, section 4; FRBT Moratorium Act, section 3(c); IBIPA, section 20; Texas Business and Commerce Code (Sec 503.001), point (d); California Assembly Bill No 1215, section 2(c); CPRA, section 24.14; GIPA, section 56.182; Virginia Senate Bill 1392, section 59.1-580; Portland's first Ordinance, 34.10.050.

273 CFRPA.

274 Genetic Information Privacy Act; Virginia Senate Bill 1392.

275 CFRPA, section 4(a).

276 It is worth noting that, in September 2021, the US House Committee on Energy and Commerce supported the establishment of a new FTC privacy bureau with a view to accomplishing tasks concerning unfair or deceptive acts/practices with regard to privacy, data security, identity theft, data abuses and related matters. See: Committee on Energy and Commerce, 'Budget Reconciliation Legislative Recommendations Relating to FTC Privacy Enforcement' <https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2021/09/BILLS-117pih-SubtitleO.pdf> accessed 23 September 2021; Hunton Andrews Kurth, 'U.S. House Committee Votes to Create New FTC Privacy Bureau and Appropriate $1 Billion to the Agency' (Hunton Privacy Blog, 16 September 2021) <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/> accessed 23 September 2021.

277 Portland's first Ordinance, 34.10.050.

similar private cause of action is present in Illinois, where anyone aggrieved may initiate legal proceedings against the private entity that, intentionally or negligently, breaches the Biometric Information Privacy Act.[278] Remarkably, Baltimore, going beyond civil sanctioning, also provides for criminal remedies.

Although the GDPR provides for civil/administrative sanctions,[279] we see no linkages to other legal fields (such as competition law) that could enhance effectiveness of remedies;[280] and sanctioning through criminal law is left at the discretion of national regulators.

11. Conclusion: five take homes for EU regulation

This working paper discussed various US initiatives with a view to highlighting what may be gained from a European perspective.

First, the US initiatives analysed ***above*** often create certainty and foreseeability as to the application of the law. Individuals can become better aware of the circumstances under which, as well as the way in which they may be protected; and firms, designers of technologies, can become more certain about if, when and how they may introduce their products into the market.

Second, the US initiatives, often targeted at private and/or public entities, pay special attention to certain dimensions of the individuals protected. This seems to enhance legal certainty. Anyone becomes better aware of when and how to seek for remedies; people know that in a specific situation, such as subjection to biometric surveillance or use of a technology, they are protected exactly because they are being subjected to surveillance practices or because they qualify as end-users of the technology at hand.

Third, the US approach to certain requirements revealed the desire to truly respect the people and effectively responsibilise relevant actors. We saw the US' focus on the independent will of the consenting individual; concrete reporting duties aimed at making information-obligations more rigorous and, thus, enhancing accountability; but also duties completely absent in the EU scheme, like the prohibition on discrimination and profiting or the application of standards of care.

Fourth, and most importantly, we witnessed the US' big 'no' to specific processing operations; this, in many shapes and sizes, from straightforward bans to moratorium techniques, that could be a useful source of inspiration for Europeans, who appear to say 'no, but'.

Fifth, we found a more practical organisation of remedies that are based, not only on data protection laws but also, on other legal fields (like competition law) making protection of individuals more effective and realistic.

278 Biometric Information Privacy Act, section 20.
279 See for instance: GDPR, arts 77-84.
280 It is expressly added that, even though there is no inextricable link between the EU data protection- and competition-law, an increasing amount of cross-fertilization between these fields is taking place. See, for example: Natasha Lomas, 'Competition challenge to Facebook's 'superprofiling' of users sparks referral to Europe's top court' (TechCrunch, 24 March 2021) <https://techcrunch.com/2021/03/24/competition-challenge-to-facebooks-superprofiling-of-users-sparks-referral-to-europes-top-court/> accessed 15 September 2021. See also: Inge Graef and Sean Van Berlo, 'Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility' (2020) European Journal of Risk Regulation 1.

12. Post-scriptum: effective prohibitions via the EU AI Act?

Although the EU seems to be moving towards the regulation of new technological implementations, relevant legislative steps appear to lack straightforwardness, bright-line rules and bans. A prime example of failure to truly prohibit certain uses of technologies is the recent Proposal of the European Commission for a Regulation on Artificial Intelligence ('Artificial Intelligence Act').[281] This Act seems to adopt a risk-based approach via, mainly, market regulation. It includes two key parts: prohibitions on certain AI-implementations (explained ***below***); and conditional use of certain high-risk AI-technologies.

With regard to prohibitions, the Act forbids:
-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;[282]
-the placing on the market, putting into service or use of certain AI-technologies by public actors;[283] and
-the use of certain biometric technologies in public areas for law enforcement goals (unless this is considered necessary, eg, to prevent crime).[284]

In our view, these prohibitions are not real prohibitions. Rather, it is a permissive approach allowing for various implementations, ranging from the selling of biometric technologies by European designers to non-EU countries (especially those supporting surveillance regimes) to the use of systems processing biometrics after-the-fact (not real-time) or for goals other than law enforcement, such as monitoring.[285]

281 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 (Brussels, 21 April 2021; COM(2021) 206 final; 2021/0106 (COD)) ('Artificial Intelligence Act').

282 Artificial Intelligence Act, art 5 (' 1. The following artificial intelligence practices shall be prohibited: (a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm; (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm ').

283 Artificial Intelligence Act, art 5 ('1. The following artificial intelligence practices shall be prohibited: (c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following: (i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected; (ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity ').

284 Artificial Intelligence Act, art 5 ('1. The following artificial intelligence practices shall be prohibited: (d) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives: (i) the targeted search for specific potential victims of crime, including missing children; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State 2. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements: a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system; (b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences. In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations ').

285 For a critical discussion, see: Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22(4) Computer Law Review International (forthcoming).

Furthermore, 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.[286] 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; same can be the case with financial harm that may not be related to a concrete ***individual.*** Moreover, the prohibition related to law enforcement is conditional upon many ***ifs*** and may not apply where the AI-practice is deemed necessary to achieve certain goals, like crime detection. Remarkably, although the Act provides for a detailed authorisation process (including an independent body), this rigorous process may not apply in certain cases of urgency;[287] and, in any event, Member States are granted discretion in permitting by law such AI-practices in the law enforcement context.[288] On the second issue of limited uses of some AI-systems, the Act demands, for the consideration of such a system as high-risk, the satisfaction of two cumulative conditions: first, the technology must be targeted for use as 'safety component of a product' or (must) be a product; and, second, the product must pass an evaluation conducted by a third-party to assess conformity for entering into the market.[289]

Notably, even though the Act sets out certain requirements and limitations, the overall approach and regulation of high-risk AI is mainly based on risk, rather than respect for fundamental rights.[290] Moreover, although certain duties are imposed on relevant stakeholders (like providers),[291] some obligations are rather vague, potentially ineffective, or appear police-friendly. For instance, there is, in principle, a duty of transparency, where people must be informed about the operation of the technology; however, there is no

286 Indeed, it may be particularly hard to detect the effects the use of AI has on a person, especially where AI, that by nature works with groups rather than individuals, is embedded within social processes. In this regard, see: Tetyana Krupiy, 'Why the proposed Artificial Intelligence Regulation does not deliver on the promise to protect individuals from harm' (European Law Blog, 23 July 2021) <https://europeanlawblog.eu/2021/07/23/why-the-proposed-artificial-intelligence-regulation-does-not-deliver-on-the-promise-to-protect-individuals-from-harm/> accessed 15 September 2021.

287 Artificial Intelligence Act, art 5 ('3. As regards paragraphs 1, point (d) and 2, each individual use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use. The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2 ').

288 Artificial Intelligence Act, art 5 ('4. A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement within the limits and under the conditions listed in paragraphs 1, point (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point (d), including which of the criminal offences referred to in point (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement ').

289 Artificial Intelligence Act, art 6 ('1. Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled: (a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II; (b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II. 2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk'). It is noted that para 2 (of the above art 6 of the Artificial Intelligence Act) does not require that the AI system be itself a product.

290 See for example: Artificial Intelligence Act, art 9 ('Risk management system'). For a discussion, see: Gianclaudio Malgieri, 'Regulating artificial intelligence: "The new model is increasingly based on the empowerment of companies"'(*Le Monde*, 13 May 2021) <https://www.lemonde.fr/idees/article/2021/05/13/reglementer-l-intelligence-artificielle-le-nouveau-modele-s-appuie-de-plus-en-plus-sur-la-responsabilisation-des-entreprises_6080117_3232.html> accessed 6 September 2021.

291 See for example: Artificial Intelligence Act, art 16 ('Obligations of providers of high-risk AI systems').

duty to scrutinise whether such an operation is lawful.[292] In addition, the transparency-duty, requiring the provision of information to the people about, among others, their interaction with the technology, does not apply in certain situations, such as where AI is used to prevent the commission of offences;[293] and, as some authors have put it, people may want to prevent criminal offenses everywhere in the public space.[294] Although the above Act can be considered as a good starting point to trigger discussions on effective AI-regulation, it misses: first, real, true prohibitions;[295] and, second, the imposition of concrete duties on relevant actors, as well as the granting of concrete rights to individuals.

By way of (counter-)example, and aside from all US initiatives discussed ***above***, one may refer to the recent Tenant Data Privacy Act (the 'TDPA') passed by the New York City Council. The TDPA aims to regulate the processing of tenant data by owners of 'smart access' buildings, meaning buildings where access is granted via keyless entry technology, like biometric identification.[296] This Act relies heavily on consent of the individual; preparation of privacy policy in simple language; implementation of security safeguards; and obligations to delete data. Importantly, its provisions appear particularly specific and clarifying.

292 In this regard, see: Nadia Benaissa, 'Het AI wetsvoorstel biedt nog onvoldoende bescherming' (Bitsoffreedom, 22 April 2021) (mentioning that users must be informed about possible errors and risks, but there is no possibility for intervention or objection, as well as no possibility to check whether a decision has been lawfully taken) <https://www.bitsoffreedom.nl/2021/04/22/het-ai-wetsvoorstel-biedt-nog-onvoldoende-bescherming/> accessed 6 September 2021.

293 Artificial Intelligence Act, art 52 ('1. Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence. 2. Users of an emotion recognition system or a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences. 3. Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated. However, the first subparagraph shall not apply where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and subject to appropriate safeguards for the rights and freedoms of third parties ').

294 In this regard, see: Nadia Benaissa, 'Het AI wetsvoorstel biedt nog onvoldoende bescherming (Bitsoffreedom, 22 April 2021) (mentioning that users must be informed about possible errors and risks, but there is no possibility for intervention or objection, as well as no possibility to check whether a decision has been lawfully taken) <https://www.bitsoffreedom.nl/2021/04/22/het-ai-wetsvoorstel-biedt-nog-onvoldoende-bescherming/> accessed 6 September 2021.

295 The lack of concrete prohibitions was recently stressed by both the EDPB and the EDPS in their 5/2021 Joint Opinion. EDPB and EDPS, EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (18 June 2021) 2 ('the EDPB and the EDPS call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces'), 3 ('(…) A ban is equally recommended on AI systems categorizing individuals from biometrics into clusters according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination under Article 21 of the Charter'), 11 ('(…) the EDPB and the EDPS call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals - in any context'), 12 ('(…) the EDPB and EDPS recommend a ban, for both public authorities and private entities, on AI systems categorizing individuals from biometrics (for instance, from face recognition) into clusters according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination prohibited under Article 21 of the Charter, or AI systems whose scientific validity is not proven or which are in direct conflict with essential values of the EU (e.g., polygraph, Annex III, 6. (b) and 7. (a)). Accordingly, "biometric categorization" should be prohibited under Article 5'). See also: EDPB and EDPS, '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' (21 June 2021) <https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en> accessed 6 September 2021.

296 For an overview, see: Hunton Andrews Kurth, 'New York City Council Passes Tenant Data Privacy Act' (Hunton Privacy Blog, 13 May 2021) <https://www.huntonprivacyblog.com/2021/05/13/new-york-city-council-passes-tenant-data-privacy-act/> accessed 6 September 2021. The text of the Act is available at <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4196254&GUID=29A4B0E2-4C1F-472B-AE88-AE10B5313AC1&Options=ID%7cText%7c&Search=> accessed 6 September 2021.

For instance, individual occupants or group of occupants of such buildings enjoy a private right of action in case of illegal sale of personal information.[297]

EU regulators should draw inspiration from these US approaches to establish a more effective legal regime on biometric and visual data. Perhaps, the EU could grab the opportunity now, with the recent registration (on the 7th of January 2021) of the European Citizens' Initiative (ECI) 'Civil society initiative for a ban on biometric mass surveillance practices'[298] that is aimed at strict regulation with a view to banning indiscriminate and arbitrarily targeted uses of biometric technologies.[299]

297 TDPA § 26-3006 (' Private right of action. a. A lawful occupant of a dwelling unit, or a group of such occupants, in a smart access building may bring an action alleging an unlawful sale of data in violation of paragraph one of subdivision a of section 26-3003 in any court of competent jurisdiction. If such court finds that a person is in violation of such paragraph for the unlawful sale of data, such court shall, in addition to any other relief such court determines to be appropriate: 1. Award to each such occupant per each unlawful sale of such occupant's data: (i) compensatory damages and, in such court's discretion, punitive damages, or (ii) at the election of each occupant, damages ranging from $200 to $1,000; and 2. Award to such occupants reasonable attorneys' fees and court costs. b. Nothing in this section shall relieve any such occupant or occupants from any obligation to pay rent or any other charge for which such occupant or occupants are otherwise liable to a person found to be in violation of this chapter. Nothing in this section shall affect any other right or responsibility of an occupant or owner afforded to such person pursuant to a lawful lease. c. This section does not limit or abrogate any claim or cause of action a person has under common law or by other law or rule. The provisions of this section are in addition to any other remedies that may be provided for under common law or by other law or rule').

298 Introduced by the Lisbon Treaty, the ECI is an 'agenda-setting' instrument for citizens. It is registered as admissible by the European Commission, when it does not manifestly fall outside the Commission's authority, it is not 'manifestly abusive, frivolous or vexatious' and it is 'not manifestly contrary to the values' of the European Union. After registration, one million citizens from at least one quarter of Member States can call the European Commission 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. Provided the organizers of the ECI manage to collect a sufficient number of supporting signatures (at least one million), the European Commission may, after explaining its reasoning, accept or reject the organizers' call. See European Commission, 'European Citizens' Initiative: Commission decides to register an initiative for 'a ban on biometric mass surveillance practices'' (Press Release, Brussels, 7 January 2021) <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_22> accessed 6 September 2021.

299 See in more detail ECI, 'Civil society initiative for a ban on biometric mass surveillance practices' (with further references) <https://europa.eu/citizens-initiative/initiatives/details/2021/000001_en> accessed 6 September 2021.

The Brussels Privacy Hub Working Papers series

N°1 "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area" (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection" (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 "Towards efficient cooperation between supervisory authorities in the area of data privacy law" (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "The data protection regime in China" (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 "The right to privacy and personal data protection in Brazil: time for internet privacy rights?" (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 "Permissions and Prohibitions in Data Protection Jurisdiction" (May 2016) by Mistale Taylor (25 pages)

N°7 "Structure and Enforcement of Data Privacy Law in South Korea" (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)

N°8 "The "Right to be Forgotten" and Search Engine Liability" (December 2016) by Hiroshi Miyashita (15 pages)

N°9 "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges" (March 2017) by Gianclaudio Malgieri and Paul De Hert (25 pages)

N°10 "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw" (July 2017) by Meg Leta Jones, JD, PhD (31 pages)

N°11 "The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies" (July 2018) by Paul De Hert and Johannes Thumfart (27 pages)

N°12 "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach" (August 2018) by Irene Kamara and Paul De Hert (35 pages)

N°13 "Big data analytics by telecommunications operators and the draft ePrivacy Regulation" (September 2018) by Vagelis Papakonstantinou and Paul de Hert (13 pages)

N°14 "Enforcement in Indonesia Data Privacy Laws: The 2018 Facebook-Cambridge Analytica scandal as a case study" (October 2018) by Anbar Jayadi (21 pages)

N°15 "Belgium, Courts, Privacy and Data Protection. An inventory of Belgian case law from the pre-GDPR regime (1995-2015)." (January 2019) by Paul De Hert (34 pages)

N°16 Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an *interim* period of no regulation at all) (June 2019) by Vagelis Papakonstantinou and Paul de Hert (25 pages)

N°17 Data Localisation: Deconstructing myths and suggesting a workable model for the future. The cases of China and the EU (September 2019) by Author: Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (31 pages)

N°18 Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination (January 2020) by Dr Monique Mann and Professor Tobias Matzner (18 pages)

N°19 Access to the Internet in the EU: a policy priority, a fundamental, a human right or a concern for eGovernment? (February 2020) by Lina Jasmontaite and Paul de Hert (23 pages)

N°20 The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? (March 2020) by Elena Gil González, Paul De Hert & Vagelis Papakonstantinou (31 pages)

N°21 Article 8 ECHR compliant and foreseeable surveillance: the ECtHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law (April 2020) by Paul De Hert & Gianclaudio Malgieri (42 pages)

N°22 The "Ethification" of Privacy and Data Protection Law in the European Union. The Case of Artificial Intelligence (May 2020) by Niels van Dijk and Simone Casiraghi (23 pages)

N°23 Logic and Key Points of China's Cybersecurity Review Measures (June 2020) by Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (9 pages)

N°24 Individuation: re-imagining data privacy laws to protect against digital harms (July 2020) by Anna Johnston (22 pages)

N°25 The Dark Side of the MOOC? The Rise of EdTech in Times of COVID-19: A Data Protection Challenge for Universities (August 2020) by Jonas Botta (16 pages)

N°26 European Law Enforcement and US Data Companies: A Decade of Cooperation Free from Law (September 2020) by Angela Aguinaldo and Paul De Hert (16 pages)

N°27 Fashion ID and Decisively Influencing Facebook Plugins: A Fair Approach to Single and Joint Controllership (June 2021) by Paul De Hert and Georgios Bouchagiar (24 pages)

N°28 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 (September 2021) by Paul De Hert and Georgios Bouchagiar (26 pages)

N°29 Facial recognition, visual and biometric data in the US. Recent, promising developments to regulate intrusive technologies (October 2021) by Paul De Hert and Georgios Bouchagiar (46 pages)

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Editorial Board: Paul De Hert and Christopher Kuner

Contact: info@brusselsprivacyhub.eu

VUB BRUSSELS PRIVACY HUB