10

European Biometric Surveillance, Concrete Rules, and Uniform Enforcement

Beyond Regulatory Abstraction and Local Enforcement

Paul De Hert and Georgios Bouchagiar

10.1 INTRODUCTION

In the era of biometric mass surveillance, novel technological implementations have led to an unprecedented monitoring of sensitive data. Among other purposes, this data has been used to discriminate based on certain characteristics (from sex to ethnic or social origin), contrary to multiple protective declarations, or draw insights into people's emotions. Such applications call for concrete regulatory intervention that is expressly targeted at practices that may interfere with fundamental human rights, including the right to privacy and personal data protection.

Despite promising initiatives, such as the European Citizens' Initiative's 'Civil society initiative for a ban on biometric mass surveillance practices', which was registered by the European Commission in 2021,[1] regulators have failed to readily intervene (before the materialisation of the harm) with a view to banning, halting, or sanctioning certain intrusive practices. Although this failure might to some extent be justified by lengthy law-making procedures, there is an acute social need to protect people's facial and other biometric data from constant watching by public or private actors, including for-profit firms, whose exercise of surveillance activities appears unregulated or under-regulated.

After discussing new challenging trends in the technological arena, this chapter emphasises the need for concrete rules surrounding specific technological uses and their possible harms. Technological uses (and misuses) can have a global reach,

[1] The procedure of collecting signatures for the 'Civil society initiative for a ban on biometric mass surveillance practices' (initiated at the beginning of 2021) is ongoing. See: Commission Implementing Decision (EU) 2021/360 of 19 February 2021 on the extension of the periods for the collection of statements of support for certain European citizens' initiatives pursuant to Regulation (EU) 2020/1042 of the European Parliament and of the Council (notified under document C(2021) 1121) (2021) OJ L69/9; Commission Implementing Decision (EU) 2021/944 of 3 June 2021 on the extension of the periods for the collection of statements of support for certain European citizens' initiatives pursuant to Regulation (EU) 2020/1042 of the European Parliament and of the Council (notified under document C(2021) 3879).

https://doi.org/10.1017/9781009321211.013 Published online by Cambridge University Press

meaning they pose a global risk, with a potential for global harm that may affect numerous citizens simultaneously. Hence, there is a need for precise law-making *and* uniform enforcement – via joint-intervention and collaboration between regulatory entities around the globe – with a view to halting, banning, and sanctioning targeted practices interfering with fundamental human rights.

Section 10.2 discusses trends such as remote biometric surveillance, biometric monitoring targeted at classifying people on legally protected grounds, biometric processing drawing inferences on emotions or intentions, and traditional practices, such as closed-circuit television (CCTV) surveillance, whose regulation appears to require updating. It then makes the argument that these four trends must become a warning for regulators, because they have resulted in the emergence of new needs of the citizens.

Section 10.3 summarises findings of our comparative study of US initiatives that regulate facial recognition or biometric data processing. Relying on these initiatives, we highlight three regulatory building blocks for the EU. First, concreteness and precision of the law: US legal texts appear clear and expressly targeted at technological uses, vulnerable groups, or coercive state powers. Second, bright-line bans: the US prohibition-agenda includes moratoria and other techniques that may, in some instances, reach the level of unconditionality. Third, practical organisation of remedies: it is not only the civil/administrative route that citizens can follow; rather, many areas, from competition and market to criminal law, are combined to enhance effectiveness of protection.

Since the surveillance-effect appears ubiquitous and the technological reach seems transnational, the solution may lie not only in concrete law-making, but also in uniform or global enforcement. Section 10.4 discusses the 2021 Clearview-case to demonstrate that in this targeted case, joint scrutiny by different national entities and joint regulatory intervention (via rigorous investigations), had a positive effect and led to a considerable degree of enhanced protection for those affected by the firm's mass surveillance practices. Section 10.5 summarises, comments, and makes more concrete recommendations.

10.2 BIOMETRIC SURVEILLANCE: FOUR CRITICAL TRENDS

New technological implementations have allowed for an unprecedented regime of observation, rendering the people and their biometric data particularly vulnerable to unregulated or under-regulated state and business practices.

First, remote biometric surveillance may be aimed at matching citizens to reference datasets without their knowledge.[2] In the absence of concrete laws targeted

[2] European Parliamentary Research Service, 'Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence' (16 December 2021), European Union, p. I, refers to 'remote biometric identification' as 'AI systems used for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI

at such practices, states can hardly guarantee their citizens that firms – whose for-profit activities may be exercised around the globe and operate without enhanced checks and balances (known from public law) – will not collect this data unnoticed. Neither can it be guaranteed that firms will not share collected biometric data with law enforcement, who may subsequently exploit such data and inferences in the name of national security or the need to effectively fight against crime. In the Clearview case (discussed in Section 10.4), citizens became explicitly exposed to a giant firm's mass processing and excessive sharing of sensitive data with law enforcement agencies around the world.

Second, biometric monitoring can be targeted at classifying people based on specific attributes, ranging from gender and age to political views.[3] With no specific regulation, citizens are unaware of how they may be protected against these unfairly discriminative practices – as discrimination on such bases is expressly prohibited under the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights (ECHR).[4] Such protections are particularly important in an era when sensitive data is processed in an uncontrollable data-tsunami-fashion that becomes sharable with various state entities, and given that the European Court of Human Rights has held the view (and emphasised) for more than a decade that mere retention/collection of personal data may raise serious privacy-concerns.[5]

Third, biometric watching can today be directed to processing with the further objective of drawing inferences on emotions or even intents.[6] Orwellian fears become relevant if citizens could suffer any detriment or mistreatment on the basis

system whether the person will be present and can be identified', www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)697191.

[3] European Parliamentary Research Service, 'Person identification', p. I, defines 'biometric categorisation' as 'AI systems used for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data'.

[4] Charter of Fundamental Rights of the European Union (2012) OJ C326/391, Art. 21. '1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited. 2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited […].' European Convention on Human Rights (as amended by Protocols Nos 11, 14 and 15 supplemented by Protocols Nos 1, 4, 6, 7, 12, 13 and 16), Art. 14. 'The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status […].'

[5] *S and Marper* v. *the United Kingdom*, Application Nos 30562/04 and 30566/04 (ECtHR, 4 December 2008) 121. 'The Court […] reiterates that the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private life interest of an individual concerned, irrespective of whether subsequent use is made of the data […].'

[6] European Parliamentary Research Service, 'Person identification, human rights and ethical principles' , p. I, sees 'emotion recognition' as 'AI systems used for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data'.

of ideas, feelings, or thoughts that, as regulators would agree, must stay untouched by any law or practice.

Fourth, old-school surveillance, for instance via CCTV systems, is no more old-school. With new applications and improvements of old technologies, citizens have come to realise that legal regimes, introduced to regulate old technological implementations, have failed to evolve and are apparently lagging behind rapidly developing tech-trends.[7] Gone are the days of a simple CCTV camera announced by an information notice that a location is under surveillance. These notices are hardly effective against powerful cameras capable of capturing detailed images from miles away.

These developments, leading to ubiquitous monitoring of all earth-citizens, must become a three-prong warning for regulators. *First*, although surveillance practices are very well targeted at citizens and their sensitive data, laws are not. Especially at the EU level, laws have remained untargeted, general, abstract, and neutral. Technologies such as cameras or drones are unmentioned in the 2016 General Data Protection Regulation (GDPR) or the 2016 Law Enforcement Directive (LED).[8] Much criticism has also surrounded recent efforts in the proposed AI Act to address more expressly certain emerging or materialised harms,[9] (potentially) caused by biometric and other un(der)regulated technologies.[10] *Second*, regulatory responses and checks, such as proportionality assessments performed by courts, must focus on and properly balance what is actually at stake, without fearing that they might look

[7] On old (CCTV) modes of surveillance that keep being subjected to new soft law, in light of technological developments and further implementations, see: ICO, 'Video surveillance (including guidance for organisations using CCTV)' (n.d.): 'Traditional closed circuit television (CCTV) also continues to evolve into more complex artificial intelligence (AI) based surveillance systems. These can process more sensitive categories of personal data […] The ways in which the technology is used also continue to develop. This includes connected databases utilising Automatic Number Plate Recognition (ANPR) or the use of Facial Recognition Technology (FRT) in public spaces […]', https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/.

[8] Paul De Hert and Georgios Bouchagiar, 'Visual and biometric surveillance in the EU. Saying "no" to mass surveillance practices?' (2022) 27(2) *Information Polity* 193.

[9] See, among many others, European Parliamentary Research Service, 'Person identification, human rights and ethical principles', 53ff, finding regulatory failures and gaps and suggesting, among others, more specific and targeted regulation and bans on certain uses.

[10] Although some of these efforts and AI-proposals appear promising, it remains to be seen whether they will be effectively realised. See Maximilian Gahntz, Mark Surman, and Mozilla Insights, 'How to make sure the EU's AI Act delivers on its promise' (25 April 2022), Mozilla Foundation, https://foundation.mozilla.org/en/blog/how-to-make-sure-the-eu-ai-act-delivers-on-its-promise/#:~:text=The%20draft%20AI%20Act%20includes,before%20they%20can%20be%20deployed. In our view, these efforts need to be taken seriously. Regulators simply *must* provide the citizen a response to materialised, detected, or emerging risks and harms. At least those states that see themselves as pioneers in a tech-field should make themselves analogously responsibilised towards those affected by their technological expertise and uses. Compare Els Kindt, 'Biometric data processing: Is the legislator keeping up or just keeping up appearances?' in Gloria González, Rosamunde Van Brakel and Paul De Hert (eds.), *Research Handbook on Privacy and Data Protection Law* (Edward Elgar, 2022), pp. 375, 396: '[T]he responsibility of the States to regulate the automated use of unique and other human characteristics cannot be underestimated: Any State claiming a pioneer role in the development of new technologies bears special responsibility for "striking the right balance" […].'

political or too activist.[11] This risk is only heightened when a regulatory framework is lacking or too vague. *Third*, fundamental human rights demand priority and enforcement – an argument closely linked to the second point. While the risk-based, cost/benefit rationale already underlying many fields, from environment to data protection,[12] could entertain utilitarianism-advocates, it cannot and should not replace the logic of the 'fundamental'. There are certain sensitive areas where financial interests and security must not be over-prioritised; where fundamental human rights cannot be outweighed by being attributed numerical values in a mathematical fashion.[13]

These technological trends and regulatory challenges must catch the eye of the regulator; for the watching of anyone anywhere, their sorting into whatever classes on whatever bases and for whatever purposes, the foreseeing of people's thoughts and feelings, and the rebirth of old-school technologies escaping old-school laws have given birth to new citizens' needs.

10.3 REGULATORY STRATEGY: FOCUS ON CONCRETE TECHNOLOGICAL USES AND THEIR POSSIBLE HARM

The need for bright-line rules directed to concrete technological uses and possible harms has long been identified and stressed in privacy-related contexts;[14] and, in recent publications, we have resorted to the US legal regime and its piecemeal approach to make concrete recommendations that might be useful for EU audiences.[15] More concretely, we have digested about fifteen US-initiatives at federal,

[11] See, on the refusal of the judges in *Bridges* to test the proportionality of facial recognition systems, Nóra Ni Loideain, Chapter 11 in this volume. See also De Hert and Bouchagiar, 'Visual and biometric surveillance in the EU'.

[12] See, among others, Gabe Maldoff, 'White Paper – The risk-based approach in the GDPR: Interpretation and implications' (March 2016), IAPP, https://iapp.org/resources/article/the-risk-based-approach-in-the-gdpr-interpretation-and-implications/; Gianclaudio Malgieri, 'Malgieri & Ienca on European Law Blog: "The EU regulates AI but forgets to protect our mind"' (7 July 2021), Gianclaudio Malgieri, European Law Blog, www.gianclaudiomalgieri.eu/2021/07/07/malgieri-ienca-on-european-law-blog-the-eu-regulates-ai-but-forgets-to-protect-our-mind/; European Commission, 'Environmental risks' (n.d.), https://ec.europa.eu/environment/risks/index_en.htm.

[13] Compare with Orla Lynskeyon the possible role of law in this area: either shaping proportionate surveillance or banning facial recognition since it affects the core of individual and collective rights and interests. Orla Lynskey, 'Keynote address in facial recognition in the modern state' (15 September 2022), *UNSW Allens Hub*, https://allenshub.unsw.edu.au/events/facial-recognition-modern-state.

[14] See, among others, McKay Cunningham, 'Next generation privacy: The internet of things, data exhaust, and reforming regulation by risk of harm' (2014) 2(2) *Groningen Journal of International Law* 115, 142, 144. 'Privacy laws should focus on data use, not collection. Privacy laws should identify and address the specific harm or risk associated with the use of sensitive data in particular contexts […]'; Paul De Hert, 'The future of privacy – Addressing singularities to identify bright-line rules that speak to us' (2016) 2(4) *European Data Protection Law Review* 461.

[15] Paul De Hert and Georgios Bouchagiar, 'Facial recognition, visual and biometric data in the US. Recent, promising developments to regulate intrusive technologies' (2021) 7(29) *Brussels Privacy Hub* https://brusselsprivacyhub.eu/publications/wp729; De Hert and Bouchagiar, 'Visual and biometric surveillance in the EU'.

state, and local level. These initiatives refer either to biometrics or to face recognition.[16] On biometrics there is the federal 2020 National Biometric Information Privacy Act, which aims to tackle biometric data exploitation by private entities. What caught our attention was the setting out of concrete bans on specific manners of obtaining, exploiting, and sharing biometric data:

> 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 […] 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 […] may not disclose, redisclose, sell, lease, trade, use for advertising purposes, otherwise disseminate, or profit from such biometric identifier or biometric information […].[17]

In the same vein, the 2008 Illinois Biometric Information Privacy Act sets out a number of targeted prohibitions on the processing (again, mainly obtaining, profiting, and disseminating) of biometrics by private entities (prohibitions that will play a crucial bright-line-rule role in the Clearview case discussed in Section 10.4).[18] We also appreciated the imposition of a standard of care (regarding storing, communicating, and securing) that ensures biometrics are treated in a similar way to, or are more shielded than, other confidential and sensitive information in that industry:

> 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 […] No private entity […] may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information […] No private entity […] may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information […] A private entity […] 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 […] 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 […].[19]

Similar is the 2009 Texas Business and Commerce Code Sec 503.001 'Capture or Use of Biometric Identifier' (obviously influenced by the Illinois Act), which forbids the capturing, disclosing, or exploiting of biometrics in commercial contexts, save

[16] For full reference of these initiatives, see: De Hert and Bouchagiar, 'Facial recognition, visual and biometric data in the US'; De Hert and Bouchagiar, 'Visual and biometric surveillance in the EU'.

[17] Federal 2020 National Biometric Information Privacy Act, section 3(b)–(d).

[18] For a list of lawsuits, based on Illinois Biometric Information Privacy Act and revealing that some actors are becoming nervous and uneasy in light of risks connected with FRTs and machine learning-implementations, see Debra Bernard, Susan Fahringer, and Nicola Menaldo, 'New biometrics lawsuits signal potential legal risks in AI' (2 April 2020), Perkins Coie, www.perkinscoie.com/en/news-insights/new-biometrics-lawsuits-signal-potential-legal-risks-in-AI.html.

[19] 2008 Illinois Biometric Information Privacy Act, section 15(b)–(e).

for exceptional circumstances. It further requires that when securing biometrics, 'reasonable care' must be shown and that any measures taken must have the same level of protection (or be more shielding) than the measures taken to store their own confidential data.

The 2019 California's Assembly Bill No. 1215 is expressly aimed at forbidding biometric surveillance by law enforcement through cameras. There is not much to say about such a clear-cut provision targeted at avoiding abuse of law enforcement powers: '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 [….].'[20]

The 2020 California Privacy Rights Act is an EU-like tool targeted at businesses and the protection of consumers. Not only does it use GDPR-like terminology, but it also grants consumers various GDPR-like rights (including the right to correct inaccurate data or opt out of automated decision making), imposes on businesses GDPR-like obligations (such as the duty to conduct audits or risk assessments), and includes GDPR-like principles (such as data minimisation, purpose limitation, and storage limitation).

The 2020 Indiana House Bill 1238 imposes on law enforcement actors a duty to conduct a 'surveillance technology impact and use policy', make that policy available to the public, and update it prior to altering the technology's function or purpose. Interestingly, these duties are set out using brief and simple phrasing:

> Requires a state or local law enforcement agency […] that uses surveillance technology to prepare a surveillance technology impact and use policy […] and post the policy on the agency's Internet web site […] Specifies the information that must be included in the policy […] 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 […].[21]

The 2020 New York's Assembly Bill A6787D aims to protect children by suspending the use of biometric technologies (including face recognition) in public and private schools. It does so through a moratorium on purchases and uses of technologies for a concrete period of time or until these technologies are proven safe: 'Public and nonpublic elementary and secondary 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 […].'[22]

The 2021 proposed Virginia's Senate Bill 1392 focusses on private for-profit entities that process significant amounts of personal data, including biometrics. This

[20] 2019 California's Assembly Bill No. 1215, section 2(b).
[21] House Bill 1238.
[22] New York's Assembly Bill, subdivision 2.

https://doi.org/10.1017/9781009321211.013 Published online by Cambridge University Press

Bill offers clear rules protecting biometric data as sensitive personal information, whose processing is in principle prohibited. What we found novel, compared with the GDPR-regime, is the prohibition on discrimination against consumers: 'A controller shall not discriminate against a consumer for exercising any of the consumer rights […] 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 […].'[23]

Moving on to the US initiatives on face recognition, the proposed federal 2019 Commercial Facial Recognition Privacy Act bans the use of face recognition technology (FRT) by private actors (save where there is consent and, where possible, notification) for the purposes of facial recognition data collection, discrimination, purposes other than those of initial processing, and the sharing of facial recognition data. Though conditional, the ban on discrimination is, again, a novelty, when compared with the EU regime: '[I]t 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 […].'[24]

The federal 2020 Facial Recognition and Biometric Technology Moratorium Act forbids the federal government from using face recognition or other biometric technology until expressly allowed by the law: '[I]t shall be unlawful for any Federal agency or Federal official […] 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 […] does not apply to activities explicitly authorized by an Act of Congress […].'[25]

Washington's Engrossed Substitute Senate Bill 6280 (2020) is targeted at state/local authorities using facial recognition services and imposes several concrete duties (such as conduct of accountability reports that are reviewable by the public), as well as restrictions (such as preventing the application of the technology to persons on concrete discriminatory grounds). What appeared interesting to us (in addition to the regulator's concern about discrimination) was the clear ban on reliance upon the facial recognition service as the only basis for establishing 'probable cause' in criminal contexts or image-tampering in face recognition contexts. Nothing similar or even close to this exists in the LED:

> 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 […] 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 […].[26]

[23] Senate Bill 1392, section 59.1-574, subsection A.
[24] Federal 2019 Commercial Facial Recognition Privacy Act, section 3(a)(2–4).
[25] Federal 2020 Facial Recognition and Biometric Technology Moratorium Act, section 3(a)–(b).
[26] Engrossed Substitute Senate Bill 6280, section 11(5), (7).

https://doi.org/10.1017/9781009321211.013 Published online by Cambridge University Press

The 2020 New Jersey's Assembly Bill 989 is targeted at subjecting facial recognition technologies to accuracy- and bias-checking; again, the focus is placed on avoiding discrimination on concrete grounds: '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 […].'[27]

Portland's ordinances (2020) ban the application of face recognition to public spaces and by private entities, as well as the use of FRTs by the city's public actors ('bureaus'). Portland clearly says 'no' to both state and private entities.

Baltimore's ordinance (2021) prohibits, first, 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) and, second, private actors from obtaining, retaining, accessing, or using a face recognition system or information gathered from such a system (certain biometric security systems and Maryland's Image Repository System are exempted). Remarkably, 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: '§ 18-3. Penalties […] 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 […] Each day that a violation continues is a separate offense […].'[28]

After analysing these US texts, we detected three key ideas that encapsulate the overall approach followed by the US regulators:[29]

Concreteness and precision: We appreciated the unambiguous clarity of the US initiatives, which appear to have clear objectives and target concrete and intrusive technological uses. Compared with the EU regime, US provisions are more demanding with respect to various requirements. *First*, although some bans are conditional upon consent, the latter goes beyond the EU model – demanding not only that consent be 'informed', 'specific', and so forth (terms also present in the GDPR), but also focussing on the independent, genuine will of the person concerned, who must be free from outside control. These demands make the US prohibition stronger and more honest than the EU's ban, which is accompanied by a long list of exceptions.[30] *Second*, some duties and prohibitions concretely set

[27] Assembly Bill 989.

[28] Ordinance 'Surveillance Technology in Baltimore', 'Article 19. Police Ordinances', 'Subtitle 18. Surveillance'.

[29] For full analysis of our conclusions, see: De Hert and Bouchagiar, 'Facial recognition, visual and biometric data in the US'; De Hert and Bouchagiar, 'Visual and biometric surveillance in the EU'.

[30] A good example of this can be found in Federal 2020 National Biometric Information Privacy Act, 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 […].'

out in the US texts are completely absent in the EU. These include the prohibition on discrimination, the prohibition on profiting, the application of standards of care, and the treatment of biometric data as particularly sensitive and confidential information.

Bright-line bans: We saw explicit prohibitions on certain technologies or surveillance practices, often reaching the level of unconditionality. In this regard, Portland and its ordinances very well illustrate how both private and public actors can be prohibited from using FRTs. Remarkably, the US prohibitions aim to protect vulnerable groups (such as children) and anticipate, or probably avoid, possible abuses of coercive powers (for instance, by prohibiting law enforcement from using surveillance cameras). Even where ban-techniques, such as moratoria, can end upon the (future) introduction of laws that would allow for relevant uses, the United States demands that such laws be particularly detailed in various terms, ranging from lists of authorised entities to operation-standards, auditing duties and compliance-mechanisms. Probably, the best example is given by section 3(a)–(b) of the Federal 2020 Facial Recognition and Biometric Technology Moratorium Act quoted earlier.[31]

Practical organisation of remedies: We found the United States's supremacy in combining several legal fields (e.g., market, competition or criminal law/procedure) with a view to enhancing effectiveness of their remedy-scheme. Good examples can be found in the 2019 Commercial Facial Recognition Privacy Act (section 4(a)),[32] and in the Ordinance 'Surveillance Technology in Baltimore'.[33]

One could argue that the EU's general approach allows for an always-present regime covering any technological implementation; and, in our recent EU–United States comparative analysis, we addressed pros and cons of both general and concrete law-making, finding persuasive arguments for both approaches.[34] However, in our opinion, what makes bright-line regulation more desirable (and more protective) is

[31] '[I]t shall be unlawful for any Federal agency or Federal official […] 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 […] (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 […].'

[32] 'A violation of section 3 shall be treated as a violation of a rule defining an unfair or deceptive act or practice […].'

[33] '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 […].'

[34] De Hert and Bouchagiar, 'Facial recognition, visual and biometric data in the US'.

the very principle of legality.[35] If laws are general and abstract by-design, then they risk becoming human rights-incompatible by default. If law enforcement and other state actors are not told by the lawmaker in simple, clear, and detailed language what they can and cannot do, not only are citizens under-protected, but also regulators are confused. Experience has indeed shown that lack of bright-line-rule-setting has confused and puzzled regulators, who may not be able to fully foresee or tell the legal grounds upon which proposed bans can be introduced.[36]

Today, with the tremendous challenges posed by the global reach of any anywhere-based tech-firm,[37] as well as the mass adoption of latest technologies and pilot programmes in both private and public arenas,[38] we encounter concrete risks from concrete uses (from school-areas involving vulnerable children to work environments obliging employees to be surveilled) that appear to demand concrete rule-setting.[39] And, in our view, effectiveness of such precise rule-making can be enhanced by uniform enforcement aimed at scrutinising, banning, or sanctioning specific surveillance practices. At least one case, namely Clearview (discussed in Section 10.4), can support the claim that the ideal solution can include both precise rule-making *and* uniform enforcement.

10.4 REGULATORY STRATEGY: UNIFORM ENFORCEMENT

In May 2021, several national data protection authorities and organisations submitted complaints against Clearview, an American face recognition-tech firm. The firm

[35] Paul De Hert and Gianclaudio Malgieri, 'One European legal framework for surveillance: The ECtHR's expanded legality testing copied by the CJEU' in Valsamis Mitsilegas and Niovi Vavoula (eds.), *Surveillance and Privacy in the Digital Age. European, Transatlantic and Global Perspectives* (Hart, 2021), p. 255.

[36] See, for instance, European Parliament, 'Parliamentary questions' (13 August 2021), European Parliament: 'In a joint opinion, the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) have called for a general ban on the use of AI for the automated recognition of human features – such as of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals – in publicly accessible spaces. The EDPS and EDPB recommend tightening the draft EU Artificial Intelligence Act, as they consider that the current proposal does not cover a wide enough scope. 1. To what extent does the Commission take the views of the EDPS, EDPB and the 175 civil society organisations mentioned in the article above into account? 2. Does the automated recognition of human features constitute interference with the fundamental rights of EU citizens? 3. Is the Commission aiming to ban the automated recognition of human features? If so, on what grounds? […]', www.europarl.europa.eu/doceo/document/E-9-2021-003888_EN.html.

[37] There is a discussion on serious challenges in the US in an interview of Helena Wootton and Stewart Dresner with Justin Antonipillai, Privacy Laws & Business, 'Privacy Paths' podcast, Episode 17: 'US privacy laws most likely to be adopted and when' (10 November 2021), www.privacylaws.com/podcasts/.

[38] On smart-contracting-programmes in the EU agenda targeted at the public sphere, from voting to establishing digital identities, see, among others, EU Blockchain, 'Observatory and forum' (n.d.), www.eublockchainforum.eu/initiative-map.

[39] On face recognition in schools, see Asress Adimi Gikay, 'On facial recognition technology in schools, power imbalance and consent: European data protection authorities should re-examine their

https://doi.org/10.1017/9781009321211.013 Published online by Cambridge University Press

had in its hands the (allegedly) largest known database (more than 3 billion facial images). With its AI technology, it searches for human (face) photographs in the web, stores them on its proprietary database, and sells access to other firms or law enforcement authorities.[40]

Elsewhere, we have critically approached the Clearview-case, questioning the legal grounds for data collection and further processing, as well as doubting the lawfulness of sharing practices – particularly in relation to EU law enforcement authorities.[41] These concerns were recently shared by two national authorities.

Upon joint scrutiny conducted by the United Kingdom's Information Commissioner's Office (ICO) and the Office of the Australian Information Commissioner (OAIC), initiated in July 2020, these authorities gathered evidence from the web and searched separately for uses of relevant data by their law enforcement entities.[42] After stressing the global nature of the digital space and the resulting need for a global regulatory approach, they highlighted new challenges posed by Clearview's practices.[43] According to the ICO's preliminary opinion, the firm had probably failed to comply with data protection laws in various respects (including unfair processing, lack of mechanisms to avoid forever-storage, no legal basis, and opaque processing).[44] After expressing its intent to impose on the firm a provisional

approach' (20 December 2021), EU Law Analysis, http://eulawanalysis.blogspot.com/2021/12/on-facial-recognition-technology-in.html. On recent initiatives in the United States, introducing concrete duties to employers who use monitoring technologies, see Hunton Andrews Kurth, 'New York State requires private employers to notify employees of electronic monitoring' (12 November 2021), Hunton Privacy Blog, www.huntonprivacyblog.com/2021/11/12/new-york-state-requires-private-employers-to-notify-employees-of-electronic-monitoring/#more-20908. This refers to New York's law A.430/S.2628, introduced in 2021 (effective from May 2022), demanding private employers to give employees prior written notice (before hiring) of their monitoring technologies.

[40] Privacy International, 'Challenge against Clearview AI in Europe' (2 June 2021), EDRi, https://edri.org/our-work/challenge-against-clearview-ai-in-europe/.

[41] De Hert and Bouchagiar, 'Visual and biometric surveillance in the EU'.

[42] OAIC, 'OAIC and ICO conclude joint investigation into Clearview AI' (3 November 2021), www.oaic.gov.au/updates/news-and-media/oaic-and-ico-conclude-joint-investigation-into-clearview-ai.

[43] Ibid. 'Our digital world is international and so our regulatory work must be international too, particularly where we are looking to anticipate, interpret and influence developments in tech for the global good […] The issues raised by Clearview AI's business practices presented novel concerns in a number of jurisdictions. By partnering together, the OAIC and ICO have been able to contribute to an international position, and shape our global regulatory environment […].'

[44] ICO, 'ICO issues provisional view to fine Clearview AI Inc over £17 million' (29 November 2021), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/11/ico-issues-provisional-view-to-fine-clearview-ai-inc-over-17-million/. 'The ICO's preliminary view is that Clearview AI Inc appears to have failed to comply with UK data protection laws in several ways including by […] failing to process the information of people in the UK in a way they are likely to expect or that is fair […] failing to have a process in place to stop the data being retained indefinitely […] failing to have a lawful reason for collecting the information […] failing to meet the higher data protection standards required for biometric data (classed as 'special category data' under the GDPR and UK GDPR) […] failing to inform people in the UK about what is happening to their data; and asking for additional personal information, including photos, which may have acted as a disincentive to individuals who wish to object to their data being processed […].'

https://doi.org/10.1017/9781009321211.013 Published online by Cambridge University Press

fine and after issuing its provisional notice to halt processing and erase relevant data,[45] the ICO imposed a fine of £7.5 million and ordered deletion.[46] While it was clarified that the firm's services are no longer offered in the United Kingdom, the ICO stated that there is no guarantee that Clearview will stop processing data of UK citizens, in light of its opaque practices.[47]

What the Clearview-case can reveal is that uniform enforcement, collaboration (in the sense of looking for ways to make different approaches work), and co-ordination can successfully tackle the transnational, global reach, risk, and potential harm of surveillance practices. The success is not the imposition of the huge fine; rather, it is the desire of the regulators (ICO and OAIC), which was actually expressed and materialised via rigorous investigations and targeted application of the law, to a concrete technological use: Clearview's risky, opaque, and harmful practice, exercised at global level, potentially affecting each individual citizen.

Such global exercise can very well be halted and sanctioned by collaborating regulators at national level(s). One could claim that Clearview's fine and order to delete data may fail to 'frighten' gigantic firms; albeit, if collaboration between national authorities were embraced by various states, then analogous fines and orders imposed/issued by various domestic entities could have a considerable impact on the financial status of Clearview and similar big firms. Indeed, state authorities, finding absence of a legal basis, have taken steps in that direction and against Clearview: Italy, for example, imposed a fine of EUR 20 million,[48] and France ordered the firm to halt processing.[49] For a further discussion of the Clearview case, we refer to the discussion by Orla Lynskey, insisting on the limits of a European human rights approach.[50] Judges and data protection authorities are inclined to avoid general statements about facial recognition and limit their intervention to cases involving facial recognition brought before them. The UK and French data protection authorities demand 'settled evidence' about the negative impact of this technology. Rather than banning a technology, they opt for prohibiting a certain processing activity. The Greek and Italian data protection authorities did indeed ban the Clearview

[45] Ibid.

[46] ICO, 'Clearview AI Inc.' (26 May 2022), https://ico.org.uk/action-weve-taken/enforcement/clearview-ai-inc-mpn/.

[47] ICO, 'ICO issues provisional view'. 'Clearview AI Inc's services are no longer being offered in the UK. However, the evidence we've gathered and analysed suggests Clearview AI Inc were and may be continuing to process significant volumes of UK people's information without their knowledge. We therefore want to assure the UK public that we are considering these alleged breaches and taking them very seriously […].'

[48] Hermes Center and Reclaim Your Face, 'Italian DPA fines Clearview AI for illegally monitoring and processing biometric data of Italian citizens' (23 March 2022), EDRi, https://edri.org/our-work/italian-dpa-fines-clearview-ai-for-illegally-monitoring-and-processing-biometric-data-of-italian-citizens/.

[49] CNIL, 'Facial recognition: The CNIL orders CLEARVIEW AI to stop reusing photographs available on the internet' (16 December 2021), www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet.

[50] Lynskey, 'Keynote address in facial recognition in the modern state'.

processing activity, but only for future collection and processing of data through the company's facial recognition system. The Italians moreover only ordered the company to erase the data relating to individuals in Italy. The United Kingdom's ICO only 'banned' the web scraping by Clearview, but did not put a ban on Clearview's facial recognition activities.

While in the EU Clearview's abuses were sanctioned with fining and halting-orders, in Illinois, the firm was given a clear, quasi-permanent, and almost *erga omnes*-ban. More concretely, the American Civil Liberties Union (ACLU), a US-based organisation fighting for human rights and freedoms, brought its case against the giant firm, claiming violation of the Illinois Biometric Information Privacy Act. On 11 May 2022, there was a settlement accepted by the court, under which Clearview is permanently prohibited from offering its services to numerous private entities in the entire United States, as well as all entities (including the police) of the state of Illinois (the latter ban for the following five years).[51] The result is a settlement with compromises.[52] Clearview AI settled the lawsuit without admission of liability. There is a nationwide 'Private Entity Ban',[53] supplemented with an 'Illinois State Ban' (no facial recognition services for state or local government entities including Illinois law enforcement),[54] but for the law enforcement services outside Illinois there is also a law enforcement friendly 'Savings Clause',[55] a shaky system to prevent further web scraping without consent for Illinois residents, and with no obligation to delete past collected data.[56] It is not simple to compare the outcomes of this settlement with the preceding outcomes

[51] For the text of the settlement, see www.aclu.org/cases/aclu-v-clearview-ai. See also ACLU, 'In big win, settlement ensures Clearview AI complies with groundbreaking Illinois biometric privacy law' (9 May 2022), www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois. See also Security.nl, 'Clearview AI beperkt gebruik van massale gezichtsherkenningsdatabase' (10 May 2022), www.security.nl/posting/752955/Clearview+AI+beperkt+gebruik+van+massale+gezichtsherkenningsdatabase.

[52] Compare Arti, 'Clearview *Ai vs ACLU* lawsuit is nothing but a facade of fake hopes and claims' (18 May 2022), Analytics Insight, www.analyticsinsight.net/clearview-ai-vs-aclu-lawsuit-is-nothing-but-a-facade-of-fake-hopes-and-claims/.

[53] Clearview AI has agreed to a nationwide injunction barring access to the Clearview App by (1) any private entity or private individuals unless such access is compliant with BIPA; or (2) any governmental employee not acting in his or her official capacity.

[54] Clearview has agreed to a five-year injunction against access to the Clearview App (1) by Illinois state and local agencies and their contractors; (2) by any private entity located in Illinois even if permissible under BIPA; and (3) by employees of Illinois state and local agencies and their contractors, whether in their individual or official capacities.

[55] There will be no restrictions on Clearview's ability to work with or contract with (1) third parties outside Illinois; (2) federal agencies whether in Illinois or outside Illinois; and (3) state or local government agencies outside Illinois.

[56] This is the 'Opt-Out Program' for Illinois residents in the settlement, by which an Illinois resident will be allowed to submit a photo to Clearview and compel Clearview, on a best-efforts basis, to block search results and prevent any future collection of facial recognition data or images of such person. A last element of the settlement is 'Illinois Photo Screening', in which Clearview has agreed, on a best-efforts basis, not to access or use any of its existing 'Illinois-based' facial recognition data.

in the EU. Within the state of Illinois, the Illinois Biometric Information Privacy Act has delivered some of its promises and even more: Clearview is permanently banned, nationwide, from making its faceprint database available to most businesses and other private entities. The company also has to cease selling access to its database to any entity in Illinois, including state and local police, for five years. The Illinois Act was already used successfully to settle facial recognition practices by Facebook,[57] and IBM,[58] and has clearly brought the message to the United States that even for publicly available data, a citizen may claim that processing personal data without consent violates the law.[59]

Two remarks before concluding. First, in the EU, national authorities successfully defended citizens' rights and freedoms by jointly investigating the firm's practices and, after seeing the harm done, enforced the law and proceeded to various sanctions including halting and fining. Second, in the United States, there was a forever – and almost toward-any-party – ban prohibiting Clearview from selling its technology. Clearly enough, if the United States's clear law-making was combined with the EU's uniform enforcement, citizens would be better and more effectively protected against surveillance practices.

10.5 CONCLUSION: PRECISE RULE-MAKING AND UNIFORM ENFORCEMENT AS A TWOFOLD SOLUTION AGAINST UNDESIRED SURVEILLANCE PRACTICES

This analysis has shown that new technological trends, from monitoring of emotions to attempts to predict feelings, can pose novel, serious challenges that existing laws have failed to adequately tackle. This has in turn created new needs for global citizens: in particular, enhanced protection against increasing tech-interference. Looking to other jurisdictions for insights into how their targeted and precise regulations may better address new threats can offer useful lessons. Indeed, the US approach could offer insights into how specific uses and concrete harms could be more effectively avoided. Our argument for supremacy of the US initiatives is neither to dignify nor to deify the United States. Rather, it is to support the view that targeted and precise law-making is a matter of legality; in its absence, laws risk violating human rights by simply being abstractly designed. This is a claim we have already raised in previous publications;[60] in this chapter, we have engaged in a meta-analysis to further argue

[57] On the *In re Facebook Biometric Information Privacy Litigation* settlement of 2020, see J. Cleary, 'Facial recognition: Clearview-ACLU settlement charts a new path for BIPA and the First Amendment' (2022) *September The National Law Review* 1.

[58] On *Vance v. IBM* and *Janecyk v. International Business Machines*, see D. Bernard, Susan Fahringer, and Nicola Menaldo, 'New biometrics lawsuits signal potential legal risks in AI' (2020) 3/5, *The Journal of Robotics, Artificial Intelligence & Law* 353–356.

[59] Ibid.

[60] De Hert and Bouchagiar, 'Facial recognition, visual and biometric data in the US'; De Hert and Bouchagiar, 'Visual and biometric surveillance in the EU'.

that effectiveness of bright-line-ruling can be enhanced by uniform enforcement. The Clearview-section exemplifies how collaboration in enforcing the rules can work.

In our opinion, precise laws banning, halting, and sanctioning certain practices are not to be seen as vengeance; as revenge, fighting back against firms and their mass and over-surveilling technologies. Rather, they are to be seen as sincere manifestations of legality. And, when uniformly enforced, they are to be seen as honest manifestations of fairness. If numerous firms are bringing technologies into the market, into the court, into the law enforcement area, into the school, into the employment arena, and into any other domain one might imagine, technologies could be abused by strong entities such as the state, and used against weak parties such as the individual citizen; it would therefore make sense to demand that multiple actors (from investigating entities to administrative supervisory authorities) jointly enforce precise rules from various areas, such as competition or criminal law.

With these recommendations, we do *not* suggest that all tech-pioneers be treated as possible criminals, who should be chased by the entire enforcement-mechanism for designing technologies that might then be abused by the state. Such a far-reaching scenario, an *erga omnes*-regime attacking any tech-developer, would probably *not* be desirable. What is desirable in our opinion is a targeted, clear, and rigorous scheme applicable to those disrespecting legality and fairness at the detriment of anyone – from our children to our neighbours, ethnic or other minorities. If, for instance, a law bans our kids being watched in classrooms or when they play in the schoolyard, because such a monitoring would have a hostile impact on their personality development, their freedom of expression, their privacy, or their very dignity, then maybe the tech-developer that violated that law by selling surveillance cameras to schools should have its criminal record permanently marked to remind society of the harm suffered by those kids. Even though, in this example, no blood was spilled and no kid died of the camera-watching, citizens may want to remember the detriment this for-profit designer caused to our kids, their personality, their freedom of expression, their privacy, and their dignity – things any citizen would die and spill blood for.