The State of Play and Open Questions for the Future

Amba Kak

This chapter synthesizes broad trends and open questions for the regulation of biometric systems. We draw insights primarily from the essays in this compendium to surface lessons from existing legal approaches across multiple countries and contexts. Beyond analysis of the current state of play, we pose open questions about where regulation needs revision, or reimagination. We explore the rapidly evolving policy conversation around new kinds of regulatory interventions but also, crucially, the limits of the law in capturing or resolving concerns about these technologies.

Regulation of biometric systems has largely been through data-protection laws. Biometric data is typically designated as an especially sensitive category of personal data and is regulated through a series of restrictions on the collection, retention, and disclosure of such data.[1] The 2016 European Union's General Data Protection law (GDPR) is emblematic of this approach, and there are currently over 140 countries with national data-protection laws that cover private- and public-sector use of data.[2] The United States lacks a comprehensive federal data privacy regulation similar to the GDPR, but state laws like the 2018 Illinois Biometric Information Privacy Act (BIPA)

1 This compendium does not analyze the regulation of DNA identifiers. While DNA is recognized as biometric information because of its ability to uniquely identify individuals, it is generally regulated under separate genetic privacy laws rather than biometric privacy laws, and its use in the criminal justice system has also been regulated under specific rules.

2 Graham Greenleaf and Bertil Cottier, "2020 Ends a Decade of 62 New Data Privacy Laws," Privacy Laws & Business International Report 163, no. 24-26 (January 29, 2020), https://ssrn.com/abstract=3572611. (According to this research, the count was at 142 at the end of 2019.)

follow a similar data-protection approach to regulating biometric data.[3] Key elements of this approach are also included in laws that establish and govern biometric ID systems like India's 2016 Aadhaar Act,[4] Australia's 2019 Identity Services Matching Bill,[5] and Kenya's 2019 Huduma Namba bill.[6] **Section 1** ("The Data-Protection Lens") examines these approaches to regulating biometrics, highlighting key concerns that have become apparent through their implementation.

While data-protection laws have made fundamental shifts in the way companies and government approach the collection, retention, and use of personal data, there are clear limitations on their ability to address the full spectrum of potential harms produced by new forms of data-driven technology, like biometric identification and analysis. Their focus on individual (rather than group) conceptions of harm fails to meaningfully address questions of discrimination and algorithmic profiling.[7] The focus on data as the object of regulation has also sometimes obscured the broader challenges to social and institutional practices that these systems and platforms exert on society, in which imperfect but established methods of accountability, contestation, and democratic decision-making are undercut by the introduction of opaque automated technology.[8] In contrast, there has been a flurry of legislation, mostly in the United States, that bans the use of these systems in particular sectors, across certain uses, or for lengths of time until there is a more participatory and deliberative process of decision-making in place. Sector-specific rules have also emerged, like those that address the harms of biometric systems in criminal justice or employment or education domains. **Sections 2 and 3 of this chapter** track these emergent concerns and legal approaches.

---

3 Illinois Biometric Privacy Act, 740 Ill. Comp. Stat. Ann. 14/15. Texas and Washington have passed similar biometric privacy laws (see Tex. Bus. & Com. Code §503.001; Wash. Rev. Code Ann. §19.375.020). Proposals like the Florida Biometric Privacy Act, Bill S.1385 in Massachusetts, and New York Biometric Privacy Act NY SB 1203 in New York are also explicitly modeled after BIPA. For other examples of a data privacy approach to biometric data, see California Consumer Privacy Act of 2018 (CCPA) [1798.100 - 1798.199]; N.Y. 2019 Stop Hacks and Improve Electronic Data Security (SHIELD) Act; N.Y. Lab. Law §201 (prohibiting fingerprinting as a condition of employment); Arkansas Code §4-110-103(7). On August 4 2020, as this compendium was going into print, the National Biometric Privacy Act was introduced by Senators Bernie Sanders and Jeff Merkley along similar lines to BIPA. See The National Law Review, "National Biometric Information Privacy Act, Proposed by Sens. Jeff Merkley and Bernie Sanders", The National Law Review, August 5, 2020 https://www.natlawreview.com/article/national-biometric-information-privacy-act-proposed-sens-jeff-merkley-and-bernie.

4 Ministry of Law and Justice (Legislative Department), Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, Pub. L. No. 18 of 2016, https://uidai.gov.in/images/the_aadhaar_act_2016.pdf.

5 Parliament of Australia, "Identity-Matching Services Bill 2019 (Cth)," https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6387.

6 The Huduma Bill, 2019, https://www.ict.go.ke/wp-content/uploads/2019/07/12-07-2019-The-Huduma-Bill-2019-2.pdf.

7 See generally Martin Tisné, "The Data Delusion: Protecting Individual Data Isn't Enough When the Harm Is Collective," Stanford Cyber Policy Center, n.d., https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/the_data_delusion_formatted-v3.pdf; Linnet Taylor, Luciano Floridi, and Bart van der Sloot, eds., *Group Privacy: New Challenges of Data Technologies* (Cham: Springer, 2016), https://www.springer.com/gp/book/9783319466064; Brent Mittelstadt, "From Individual to Group Privacy in Big Data Analytics," *Philosophy & Technology* 30, no. 4 (February 2017): 475–494, https://link.springer.com/article/10.1007/s13347-017-0253-7.

8 See generally Amba Kak and Rashida Richardson, "Artificial Intelligence Policies Must Focus on Impact and Accountability," CIGI Online, May 1, 2020, https://www.cigionline.org/articles/artificial-intelligence-policies-must-focus-impact-and-accountability.

The following is a summary of the questions that this compendium raises, pointing to research, regulation, and community engagement that will be needed to inform ongoing national policy and advocacy efforts:

1. **The Data-Protection Lens**
    - How should regulation define "biometric data"?
    - Why have data protection laws had limited effectiveness in curbing the expansion of biometric surveillance infrastructure by government?
    - Is meaningful notice and consent possible in the context of biometric systems? What are the limitations of a consent-based approach and what supplements or alternatives might be required?
2. **Beyond Privacy: Accuracy, Discrimination, Human Review, and Due Process**
    - How should regulatory frameworks address concerns about accuracy and non-discrimination in biometric systems?
    - To what extent should regulation rely on standards of performance and accuracy set by technical standards-setting bodies?
    - Does requiring "meaningful human review" of biometric recognition systems ensure oversight and accountability?
    - Should regulatory frameworks create a risk-based classification between "identification" and "verification" uses of biometric recognition?
        - What are the potential risks of a permissive regulatory approach to verification?
    - What kinds of due process safeguards are required for law enforcement use of biometric recognition?
        - Should law enforcement have access to these systems to begin with?
    - Are systems that process bodily data for purposes beyond establishing individual identity, like making inferences around emotional state, personality traits, or demographic characteristics covered under existing biometric regulation?
        - Should such systems be permitted at all, given their contested scientific foundations and mounting evidence of harm?
3. **Emerging Regulatory Tools and Enforcement Mechanisms**
    - What different types of "bans" and moratoria have been passed in the US over the past few years?
        - How can moratoria conditions be strengthened to ensure that eventual legislative or deliberative processes are robust?
    - How will bans and moratoria on government use impact the private development and production of biometric systems?
    - What regulatory tools can be used to create public transparency around the development, purchase, and use of biometric recognition tools?
    - What role can community-led advocacy play in shaping the priorities and impact of regulation?

SECTION 1. THE DATA-PROTECTION LENS

How should regulation define "biometric data"?

> *Under the dominant data-protection approach to regulating biometric systems, meeting the definition of "biometric data" has been the threshold condition for legal protections to apply. Recent regulatory attempts move away from this with "systems" rather than data as the object of regulation.*
>
> *In laws that establish and regulate biometric ID systems, the definition of biometric data has typically been left open-ended to allow governments to add or change the types of biometrics collected under these projects.*

In defining biometric data and systems, the law not only reflects but also entrenches certain perceptions about the stability and accuracy of biometrics as an identification technology. For example, the GDPR states that biometric data is bodily, physiological, and behavioral data that "allow or confirm the unique identification of that natural person,"[9] while the Illinois BIPA provides an exhaustive list of identifiers that count as biometric data and requires that they are "used to identify an individual."[10] These foundational beliefs about the ability of biometric data to uniquely identify an individual are not stable and are today highly contested. Research has demonstrated vulnerabilities as people age, and the inaccuracies that creep in when these systems are used to identify people of color, young and old people, manual laborers, those who speak English with a non-native accent, and many other demographic and phenotypic subgroups.[11] Biometric regulation does not interrogate these questions, but simply takes these claims of accuracy and equivalence to real identity as given.

In data-protection laws, fulfilling the definition of "biometric data" or "biometric information" is the threshold condition for legal protections to apply. It also determines the stage (for, e.g., collection, processing, storage, and use) at which these protections are activated. When part of a broader personal data-protection law like the GDPR, such definitions usually work to distinguish biometric data from other kinds of personal data in order to offer special or stricter levels of protection. In laws like BIPA, which is solely focused on biometric data, the definition determines the scope of the legislation as a whole. Laws that establish government biometric ID projects, on the other hand, have tended toward an expansive definition that allows agencies to expand on the kinds of biometric data they can collect. The Kenyan draft law[12] and the Indian Aadhaar legislation[13] list a series of identifiers that are currently collected under the project but allow the government to add to these categories of data collected at will.

---

9 Article 4(14), GDPR.

10 Section 10, BIPA.

11 See footnotes 34 and 35 of this compendium's Introduction.

12 The Huduma Namba Bill, 2019 defines biometric data as follows: "'(B)iometric data' includes fingerprint, hand geometry, earlobe geometry, retina and iris patterns, toe impression, voice waves, blood typing, photograph, or such other biological attributes of an individual obtained by way of biometrics."

13 The Aadhaar Act, 2016 defines biometric information as follows: "'biometric information' means photograph, fingerprint, iris scan, or such other biological attributes of an individual as may be specified by regulations."

As legislation moves beyond traditional data privacy and security concerns to questions of accountability around whether or how to use these systems, and who is liable if these systems fail, some recent bills shift the focus from "data" to "systems." For example, recent US legislation that restricts the use of these technologies does not define biometric data at all, and instead focuses on "face recognition systems" or "services,"[14] or face/biometric "surveillance systems" as the object of regulation.[15] The definitions of these terms emphasize the eventual uses or intentions that drive the application of such systems in social contexts (such as surveillance, identification, verification, or tracking).

> *The legal definition of biometric data is usually restricted to data that has been technically processed for use in an algorithmic system by specifying a particular digital representation (e.g., "template" or "print"). The definition often explicitly excludes photographs and voice recordings and creates a loophole around foundational stages when data is collected, processed, and stored.*

The definition of biometric data has generally been restricted to mean a technically defined digital representation of bodily traits that have already been processed for machine or algorithmic analysis. This is suggested by semi-technical terms like "templates," "geometry," "prints,"[16] or, in the GDPR, data that has already been subject to "specific technical processing." Terms like "template" refer to the initial stage of algorithmic processing where data is extracted from, say, an image or voice recording. Modern machine learning systems do not need "all" of the data, but instead rely on extracting meaningful subparts from voice or image data, which can then be easily compared to existing "templates" in a database.[17] This is the logic that leads to photographs of faces being expressly excluded from the definition of biometric data in the BIPA[18] and the GDPR.[19]

---

14 Recent US legislation uses terms like "facial recognition systems," as in the City of Boston Ordinance Banning Face Surveillance Technology, https://www.eff.org/document/ordinance-banning-face-surveillance-technology-boston; "facial recognition services," as in the Washington Senate Bill 6280, is defined as "technology that analyzes facial features and is used by a state or local government agency for the identification, verification, or persistent tracking." See SB 6280 (2019–20), https://app.leg.wa.gov/billsummary?BillNumber=6280&Year=2019&Initiative=false.

15 The phrase "face surveillance systems" appears in S.4084 (Facial Recognition and Biometric Technology Moratorium Act) introduced in June 2020, https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology. The term "biometric surveillance systems" is used in the California A.B. 1215 that bans face recognition on body-worn cameras; the bill refers to "any computer software or application that performs facial recognition or other biometric surveillance."

16 See, for example, the way biometric data is defined in BIPA and other state biometric privacy laws, which specify "facial geometry," "voice prints," and "fingerprints."

17 Kelly Gates, "Introduction: Experimenting with the Face," in *Our Biometric Future* (New York: New York University Press, 2011).

18 Several defendants sued under BIPA have unsuccessfully argued before the courts that the specific exclusion of photographs means that information derived from photographs should also be excluded. In *Rivera v. Google, Inc*. (238 F. Supp. 3d 1088, 1095 (N.D. Ill. 2017), Google argued that its facial templates were derived from photographs, and therefore excluded from BIPA's definition of biometric information, but the court held that templates were still biometric identifiers, since BIPA does not qualify the definition of biometric identifiers based on how they were derived. See Matthew T. Hays, "Technology Defendants Continue to Test Whether the Illinois BIPA Law Can Cope with Modern Facial Recognition Technology," *Firewall*, December 6, 2019, https://www.thefirewall-blog.com/2019/12/technology-defendants-continue-to-test-whether-the-illinois-bipa-law-can-cope-with-modern-facial-recognition-technology/.

19 Recital 51 of the GDPR notes that "[t]he processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person."

This narrow technical definition of biometric data creates a set of troubling loopholes. In her chapter, Els Kindt explains that the exclusion of photographs, voice recordings, or other forms of so called "raw" biometric data adversely limits the impact of the GDPR. She argues that heightened protections, like explicit consent, are foregone in the initial stage of data collection and storage (such as when a photo is uploaded to a social media site) and that use of such data without consent is often permitted by particular exceptions for law enforcement agencies after such data has been collected.

The exclusion of photographs and voice recording is also troubling given the realities of how commercial and government surveillance systems are developed and deployed today. The harvesting of face images matched to individual names from the web is a common method used to create face-name databases. These databases are the foundation of sophisticated and covert surveillance tools created by private firms, who often do so in secret and proceed with almost no oversight.[20] The same covert surveillance practices are emerging with voice recordings.[21]

The definition of biometric data offered in the California Consumer Protection Act (CCPA) of 2018 stands apart from existing definitions and could be instructive as a way to close this loophole. Rather than the current representation of the data, CCPA's definition focuses on *the ability to extract an identifier template* that can be algorithmically processed in order to determine whether it falls within the scope of the law.[22]

Why have data-protection laws had limited effectiveness in curbing the expansion of biometric surveillance infrastructure by government?

> *Principles of data minimization and purpose limitation have rarely been applied to challenge the creation or expansion of biometric systems. Rather than an evidence-based scrutiny of the link between the means and the ends, the broad rationale of security and efficiency in service delivery has usually served to enable rather than restrict the use of biometric systems.*

---

20 See Daniel Laufer and Sebastian Mainek, "A Polish Company Is Abolishing Our Anonymity," NetzPolitik, July 10, 2020, https://netzpolitik.org/2020/pimeyes-face-search-company-is-abolishing-our-anonymity/; and Louise Matsakis, "Scraping the Web Is a Powerful Tool. Clearview AI Abused It," *Wired*, January 25, 2020, https://www.wired.com/story/clearview-ai-scraping-web/.

21 Jeremy Kirk, "Hey Alexa. Is This My Voice or a Recording?," BankInfoSecurity, July 6, 2020, https://www.bankinfosecurity.com/hey-alexa-this-my-voice-or-recording-a-14562; George Joseph and Debbie Nathan, "Prisons across the U.S. Are Quietly Building Databases of Incarcerated People's Voice Prints," *Intercept*, January 30, 2019, https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus/.

22 See Section 3(e) of the CCPA of 2018: "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...*" (emphasis mine).

Necessity and proportionality are common legal principles in international human rights law and reflected in a number of data-protection laws across the world.[23] They require that any infringement of privacy or data-protection rights be necessary and strike the appropriate balance between the means used and the intended objective. The proportionality principle is also central to constitutional privacy case law across the world, and while there are regional differences, these tests generally involve a balancing exercise where the right to privacy is balanced against a competing right or public interest.[24]

In data-protection regulation, these principles are reflected in the types of data categories that are collected,[25] how the data can be used,[26] and how long it can be stored.[27] Under the GDPR and similar data-protection laws, the "data minimization" provision in Article 5 requires that entities limit personal data collection to that which is "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*." For law enforcement agencies, the Data Protection Law Enforcement Directive (DP LED) requires a higher standard of whether that biometric data collection is "strictly necessary."[28]

Taken seriously, these provisions question whether the collection of biometric data is necessary in the first place.[29] For example, the Swedish Data Protection Authority outlawed the use of facial recognition in schools on the grounds that its use for attendance was a disproportionate means to achieve this goal when far less intrusive means exist.[30] The French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés*, or CNIL) and the regional court of Marseille also ruled similarly to declare the trial of facial recognition attendance systems illegal in France.[31]

In Ben Hayes and Massimo Marelli's chapter, they explain how the International Committee of the Red Cross (ICRC) applied data-protection proportionality principles to the use of biometrics for aid distribution to people in need of humanitarian assistance. While the ICRC eventually determined that there was a "legitimate interest" in using biometric systems for this purpose, they limited the use to a "token-based system" (i.e., a card on which people's biometric data is securely stored). The ICRC decided not to collect, retain, or further process people's biometric data, and therefore not to establish a biometric database. If people want to withdraw or delete their biometric data, they can either return the card or destroy it themselves.

---

23 See Privacy International, "Towards International Principles on Communications Surveillance," November 20, 2012, https://privacyinternational.org/blog/1360/towards-international-principles-communications-surveillance. The article refers to a meeting of experts in Brussels in October 2012. See also European Data Protection Supervisor, "Necessity & Proportionality," n.d., https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en. See generally Charlotte Bagger Tranberg, "Proportionality and Data Protection in the Case Law of the European Court of Justice," *International Data Privacy Law* 1, no. 4 (November 2011): 239–248, https://doi.org/10.1093/idpl/ipr015.

24 See generally Alec Stone Sweet and Jud Mathews, "Proportionality Balancing and Global Constitutionalism," *Columbia Journal of Transnational Law* 47, no. 72 (2008–09): 112.

25 See Article 5(c), GDPR on "data minimization," and Article 9, GDPR on processing of special categories of personal data

26 See Article 5(b), GDPR on "purpose limitation."

27 See Article 5(e), GDPR on "storage limitation."

28 See Article 10, DP LED on processing of "sensitive categories" of personal data.

29 See Els Kindt, "Biometric Applications and the Data Protection Legislation: The Legal Review and the Proportionality Test," *Datenschutz und Datensicherheit* 31, no. 3 (2007):166–170, https://www.law.kuleuven.be/citip/en/archive/copy_of_publications/880dud3-2007-1662f90.pdf. See also Yue Liu, "The Principle of Proportionality in Biometrics: Case Studies from Norway," *Computer Law & Security Review* 25, no. 3 (December 2009): 237–250.

30 Sofia Edvardsen, "How to Interpret Sweden's First GDPR Fine on Facial Recognition in School," IAPP, August 27, 2019, https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school/.

31 EDRi, "Ban Biometric Mass Surveillance," May 13, 2020, https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf.

Unfortunately, the application of these principles to challenge the creation of biometric systems and databases is rare, especially during the key initial or "pilot" stages before these systems are built and used.[32] More often than not, inquiries into "necessity" are structured to enable rather than restrict the use of biometric systems. Even where data minimization principles exist, the notoriously broad but powerful rationale of "efficiency" or "law and order" and "national security" serve to grant most government uses of biometrics a free pass without any evidence-based scrutiny of the relationship between means and ends.[33] As noted in the European Digital Rights (EDRi) 2020 report on biometric mass surveillance, this uneven application of the law can also be attributed to the European Union's inadequately resourced and politically disempowered National Data Protection Authorities. On the other hand, in countries that still lack data-protection laws and data-protection authorities (DPAs), when biometric ID projects have faced constitutional challenges in the Court, the proportionality test is often overlooked in favor of broad claims around the efficiency of biometric service delivery systems, with scant analysis of alternative, less rights-infringing means to achieve that goal.[34]

> *Legal principles of "purpose limitation" are often ineffective given the broader political and institutional trends working to dissolve boundaries between civilian, criminal, and immigration biometric databases. Driver's license face databases are a key site for this kind of "function creep" and require urgent policy intervention.*

The "purpose limitation" principle restricts the use of data for purposes beyond what it was originally collected for; a specified purpose must not be used for another "incompatible" purpose. Yet pervasive "security" imperatives often blur the boundaries between criminal, welfare, and immigration processes and, consequently, obfuscate what is perceived and understood as a "compatible" purpose. Under the US federal Secure Communities program (S-COMM), states submit fingerprints of arrestees to criminal as well as immigration databases, allowing Immigration and Customs Enforcement (ICE) to access this information.[35] ICE has also requested face recognition searches of driver's license databases in multiple states in the US.[36] In Australia, the Home Affairs department has been centralizing state driver's license face databases to use for broader policing and law enforcement purposes.[37] India's biometric ID project Aadhaar is

---

32 See EDRi, "Evidence on Biometrics and Fundamental Rights," July 2020 (submitted to the European Commission consultation and on file with the author) for a list of projects, including multiple case studies from Europe that were not properly assessed due to the claim that they were in the "experimental" or "pilot" stage.

33 In the European context, see Fundamental Rights Agency (FRA), "Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement," 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf. The authors note than "[a]n objective of general interest—such as crime prevention or public security—is not, in itself, sufficient to justify an interference" with fundamental rights, meaning that the Law Enforcement Directive's data protections must apply.

34 See Mariyan Kamil, "The Aadhaar Judgment and the Constitution – II: On Proportionality," *Indian Constitutional Law and Philosophy*, September 30, 2018, https://indconlawphil.wordpress.com/2018/09/30/the-aadhaar-judgment-and-the-constitution-ii-on-proportionality-guest-post/.

35 As a result of this, anyone arrested for a state crime (even if they were never charged or were wrongly arrested) is vulnerable to deportation or detention. See Jennifer Lynch, "From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond," American Immigration Council, May 23, 2012, https://www.americanimmigrationcouncil.org/research/fingerprints-dna-biometric-data-collection-us-immigrant-communities-and-beyond; see also ACLU, "Secure Communities ('S-Comm')," n.d., https://www.aclu.org/other/secure-communities-s-comm.

36 Harrison Rudolph, "ICE Searches of State Driver's License Databases," Center on Privacy & Technology at Georgetown Law, Medium, July 8, 2019, https://medium.com/center-on-privacy-technology/ice-searches-of-state-drivers-license-databases-4891a97d3e19.

37 See Jake Goldenfein and Monique Mann, "Australian Identity-Matching Services Bill," in this compendium.

widely known as a welfare delivery system, yet government officials may use the data for national security purposes in limited circumstances,[38] and the National Crime Bureau has publicly stated their desire to use the system for criminal investigations.[39] These systems are *structured* to evade and remove the purpose limitations on data use.

> *The failure of proportionality safeguards is also borne out in the context of centralized biometric ID systems where legislation has frequently been introduced only after these systems are developed, and in some cases after they're already deployed and in use.*

Large-scale biometric ID projects that span welfare, criminal, and immigration contexts have typically been implemented as technocratic exercises driven by executive agencies, often with the glaring absence of law. Even as advocacy efforts focus on demanding legal frameworks to ensure legislative and public scrutiny, legislation often comes too little, too late. For one, many projects do not receive proper scrutiny or are passed through extraordinary measures that forgo scrutiny altogether.[40] In other cases, weak procedural safeguards are proposed, but the broader centralization of power in a few agencies remains unchallenged.

In Jake Goldenfein and Monique Mann's chapter, they argue that the Australian Identity Services Bill provided the Home Affairs department with authorization to become the central node ("the hub") through which all identity and suspect identification requests would be routed. They conclude that "a true proportionality analysis" might have questioned whether a centralized facial recognition database was in fact necessary to address the stated purpose of curbing identity fraud, but in reality "this framing is operationalized in ways that enable continuing expansion of surveillance systems."

The mere existence of procedural safeguards like data security or consent can obscure the root of the problem, only serving to legitimize the continued existence of these systems. When faced with existential threats, like the potential of being invalidated by the highest courts, data-privacy rules have repeatedly been held up as an adequate safeguard against the concerns raised, leading to widespread skepticism about the role these laws play.[41] In the case of India's nationwide biometric ID project (Aadhaar), legislation authorizing and regulating the project came nearly a decade after biometric data collection began. This massive delay is even more concerning given the absence of a data-privacy law that applied to government agencies. In her contribution to this compendium, Nayantara Ranganathan challenges foundational assumptions about the role of the

---

38 Vrinda Bhandari and Renuka Sane, "A Critique of the Aadhaar Legal Framework," *National Law School of India Review* 31, no. 4 (2019):1–23.

39 Aman Sharma, "Cannot Share Aadhaar Biometric Data for Crime Investigations," *Economic Times*, June 22, 2018, https://economictimes.indiatimes.com/news/politics-and-nation/cannot-share-aadhaar-biometric-data-for-crime-investigations-uidai/articleshow/64700379.cms.

40 See Nayantara Ranganathan's chapter in this compendium, "The Economy (and Regulatory Practice) That Biometrics Inspires: A Study of the Aadhaar Project," in which she describes the truncated and legally dubious passage of the Aadhaar as a "money bill." See also ADC, "ADC Files an Action of Unconstitutionality before GCBA after the Introduction of Face Recognition System," November 6, 2019, https://adc.org.ar/en/2019/11/06/adc-files-an-action-of-unconstitutionality-before-gcba-after-the-introduction-of-face-recognition-system/.

41 See commentary on the Kenyan data-protection law by Rasna Warah, "Data Protection in the Age of Huduma Namba: Who Will Benefit?," *Elephant*, November 29, 2019, https://www.theelephant.info/op-eds/2019/11/29/data-protection-in-the-age-of-huduma-namba-who-will-benefit/; and see Praavita, "Can the Aadhaar Act and a Data Protection Act Coexist?," *The Wire*, July 30, 2018, https://thewire.in/law/can-the-aadhaar-act-and-a-data-protection-act-coexist.

law in relation to these projects, characterizing regulation as a legitimizing force that reflects the interests of the powerful actors that drive these systems. She argues that Aadhaar's regulation functioned to "consolidate the developments of the first seven years of the project, and also presented a revisionist history of the actual goals of the project, obscuring the stakes for private interests...[M]any of the problems with Aadhaar should not be understood as failures of law or regulation, but products of law and regulation."

Is meaningful notice and consent possible in the context of biometric systems? What are the limitations of a consent-based approach and what supplements or alternatives might be required?

> *Given the predominance of the data-protection approach, notice and consent has been a cornerstone of biometric regulation, yet the well-documented limitations of this model underscore the need for additional necessity and proportionality limits even after consent has been obtained. Recent AI legislation also requires broader "explainability" requirements as a core component of meaningful notice.*

While notice and consent has traditionally been the cornerstone of data-protection and privacy approaches globally, its limitations have been laid bare in recent years, leading to skepticism about (if not outright rejection of) the idealized conception of "individual control."[42] In their chapter, Ben Hayes and Massimo Marelli explain why the Red Cross removed consent as a legal "ground of processing"[43] in emergency humanitarian contexts where, the authors argue, consent can never be assumed to be "freely given."

At the same time, the individual's right to refuse or revoke permission for the collection or use of their data has been an important tool in challenging biometric systems like live facial recognition in public spaces that are designed to evade such active permission. As described in Woodrow Hartzog's chapter, under BIPA, the failure to obtain consent from individuals before using their biometric data has led to several successful lawsuits against some of the largest tech companies in the world and is the basis for the lawsuit recently launched against Clearview AI.[44]

---

42 For a rejection of the idea of privacy as "control," see generally Ruth Gavison, "Privacy and the Limits of Law," *Yale Law Journal* 89, no. 3 (January 1980): 421–471. See also Woodrow Hartzog, "The Case Against Idealising Control," *European Data Protection Law Review* 4, no. 4 (2018): 423–432.

43 *Grounds of processing* is a legal term of art popularized by the GDPR. It refers to a number of legal justifications, of which at least one must be met in order to "process" (i.e., collect, store, use, etc.) personal data. Grounds of processing include consent, performance of a contract, legitimate interests of a business, and so on.

44 Woodrow Hartzog, "BIPA: The Most Important Biometric Privacy Law in the US?," in this compendium.

In the GDPR, consent is supplemented by several general limits of proportionality and necessity[45] that hold irrespective of whether consent is obtained. By contrast, US state laws like BIPA focus on notice and consent with few additional restrictions on collection or use beyond the prohibition against selling biometric data for profit and limits on retention.

As Hartzog concludes, BIPA has done "very little to bring about the kind of structural change and substantive limits necessary." For one, he explains how most of us are simply "not capable of meaningfully exercising our agency over modern data practices" and argues that BIPA provides little protection from the "post-permission risks" of biometric technologies.[46] This underscores the need for additional transparency and accountability, including bright-line restrictions alongside a robust notice and consent regime.

Emerging regulatory approaches for algorithmic or AI systems include a broader understanding of notice that goes beyond simply informing the individual that algorithmic tools are being used. These newer approaches also take into account how these systems work, the context in which these systems are used, and what criteria are informing algorithmic decisions. This broad scope will be especially valuable in regulating biometric systems that serve purposes beyond identification and verification. The Illinois Artificial Intelligence Video Interview Act is an example of a notice provision tailored to the specific context of job interviews; it requires that all job applicants be informed when AI systems used to assess their performance as a candidate are deployed during interviews. In addition to this, it requires that each applicant be provided clear information about "how the artificial intelligence works and what general types of characteristics it uses to evaluate applicants."[47] Whether such explanations are possible, and whether they can work to inform meaningful choices on the part of job seekers given the power dynamics at work in the context of a job interview, have yet to be seen.

45 See Article 5 GDPR including principles of data minimization, collection limitation, purpose limitation, storage limitation principles.
46 Ibid.
47 See Section 5, "Artificial Intelligence Video Interview Act," http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=101-0260.

SECTION 2. BEYOND PRIVACY: ACCURACY, DISCRIMINATION, HUMAN REVIEW, AND DUE PROCESS

How should regulatory frameworks address concerns about accuracy and non-discrimination in biometric systems?

To what extent should regulation rely on standards of performance and accuracy set by technical standards-setting bodies?

> *While accuracy and discrimination concerns are at the forefront of public debate, corresponding legal protections have been rare in existing regulatory frameworks. However, recent legislation and advocacy efforts in the US have mandated accuracy and nondiscrimination audits for facial recognition systems, going as far as to require such audits as a condition for lifting a moratorium on use.*
>
> *While technical standards (e.g., NIST's Face Recognition Vendor Test) are evolving to account for bias and inaccuracy, they generally underperform in "real-life" contexts and are limited in their ability to address the broader discriminatory impact of these systems as they are applied in practice. If such standards are positioned as the sole check on facial recognition systems, they could function to obfuscate, rather than mitigate, harm.*

Accuracy and "error rates" metrics are a staple of the mainstream conversations around biometrics and are used as a tool in the machine learning field to compare systems and assess progress. Accuracy claims have been a simple way for those developing, marketing, and applying these systems to "prove" effectiveness, and to demonstrate that automation offers an improvement over manual processes. In the past two years, however, the same facial recognition systems that boast high accuracy rates according to such narrow metrics have been shown to perform less well when accuracy rates are stratified across demographics like age, race, gender, and disability.[48] "Errors" in these systems are not evenly distributed, and reflect historical

48 Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81 (2018):1–15, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; KS Krishnapriya et al., "Characterizing the Variability in Face Recognition Accuracy Relative to Race," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops* (2019), https://arxiv.org/abs/1904.07325; Cynthia M. Cook et al., "Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems," *IEEE Transactions on Biometrics, Behavior, and Identity Science* 1, no. 1 (Jan. 2019): 32–41, https://ieeexplore.ieee.org/document/8636231; Inioluwa Deborah Raji and Joy Buolamwini, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products," *Proceedings of the Conf. on Artificial Intelligence, Ethics, and Society* (2019), https://www.aies-conference.com/2019/wp-content/uploads/2019/01/AIES-19_paper_223.pdf; Morgan Klaus Scheuerman, Jacob M. Paul, and Jed R. Brubaker, "How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis Services," *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (November 2019): 1–33, https://doi.org/10.1145/3359246.

patterns of racism, gender bias, and ableist discrimination. To remedy this problem, researchers have called for auditing on accuracy across specific demographic and phenotypic subgroups, accompanied by measures that can close performance gaps where they arise.[49]

To accomplish such audits, many are turning to technical standard-setting bodies that set benchmarks for accuracy, performance and safety. Auditing protocols like the National Institute of Standards and Technology (NIST) 2019 Face Recognition Vendor Test (part three) evaluate whether the algorithm performs differently across different demographics in the dataset.

Regulators and lawmakers have also begun to take notice, calling for audits by technical standards-setting bodies that set benchmarks for accuracy, performance, and safety. In March 2020, the UK Equality and Human Rights Commission called to suspend the use of facial recognition in England and Wales until discrimination against protected groups has been independently scrutinized. Recent legislation in the US includes accuracy and nondiscrimination audits as a condition for the use of facial recognition. The Washington State Bill SB 6280, passed in March 2020, requires that face recognition companies cooperate to allow for independent testing for "accuracy and unfair performance" across subgroups including race, skin tone, ethnicity, gender, age, or disability status. If independent testing reveals "material unfair performance differences," companies are required to rectify the issues within ninety days. Another proposed federal bill (S.2878: the Facial Recognition Technology Warrant Act of 2019) requires federal law enforcement agencies to work with NIST[50] to establish testing systems to ensure consistent accuracy across gender, age, and ethnicity.

While these standards are a step in the right direction, it would be premature to rely on them to assess performance, and they do not adequately capture the broader discriminatory impacts these systems might have when they are used. First, researchers and advocacy organizations have found that many of the systems that "pass" current benchmark evaluations continue to underperform in real-life contexts.[51] Additionally, there is currently no standard practice to document and communicate the histories and limits of benchmarking datasets, and thus no way to determine their applicability to a particular system or suitability for a given context.

Moreover, creating a solely technical threshold to judge discriminatory impact can distort the biased practical implementation of these technologies and their weaponization against specific groups. For example, facial recognition systems are deployed disproportionately in minority communities, so even the most accurate systems will be discriminatory. They also "run the risk of providing 'checkbox certification,' allowing vendors and companies to assert that their technology is safe and fair without accounting for how it will be used, or its fitness for a given context."[52]

---

49 See Raji and Buolamwini, "Actionable Auditing," and Buolamwini et al., Gender Shades, MIT Media Lab, http://gendershades.org.

50 NIST is a non-regulatory federal agency within the US Department of Commerce. Its mission is to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. Auditing protocols like the NIST 2019 Face Recognition Vendor Test (part three) evaluate whether the algorithm performs differently across different demographics in the dataset.

51 See Inioluwa Deborah Raji and Genevieve Fried, "About Face: A Survey of Facial Recognition Evaluation," Meta-Evaluation workshop at AAAI Conference on Artificial Intelligence (forthcoming, 2020); Pete Fussey and Daragh Murray, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology," The Human Rights, Big Data and Technology Project, July 2019, https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf.

52 Written Testimony of Meredith Whittaker, US House of Representatives Committee on Oversight and Reform, "Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy, January 15, 2020, https://oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/WRITTEN%20testimony%20-%20MW%20oversight.pdf/.

Does requiring "meaningful human review" of biometric recognition systems ensure oversight and accountability?

> *Recent legislation includes provisions that mandate "meaningful human intervention" in the results of biometric systems. However, a large body of research suggests that the people who review the results of biometric systems overwhelmingly overestimate credibility, and often respond inaccurately and with bias.*

"Human intervention" in automated decisions has gained considerable acceptance as a legal approach to provide a meaningful check on the potential harms these systems represent. Article 22 of the GDPR, for example, includes a restriction on "solely automated decisions," and requires human intervention when automated systems impact "legal or similarly significant" decisions about people's lives. The recently passed and heavily criticized[53] Washington State facial recognition law similarly includes provisions for "meaningful human review" and periodic officer training as conditions for the use of biometric technology. Human review is defined in terms of "*review or oversight by one or more individuals...who have the authority to alter the decision under review*."[54]

However, a large body of research demonstrates that human intervention in these systems does not address major concerns about transparency or control. Individuals who review results are often unable to accurately evaluate the quality or fairness of the outputs, and often respond to predictions in biased and inaccurate ways.[55] The ACLU has pointed to the imprecisely defined notion of meaningful human review as "deeply flawed" given its vague definition. They maintain that it should not become a rubber stamp that allows for the use of facial recognition or similar systems in sensitive social domains like welfare and criminal justice.[56]

In their chapter, Peter Fussey and Daragh Murray show that human operators who asses live facial recognition "matches" often defer to the algorithm's output, despite the known inaccuracy of such output—a phenomenon referred to as "automation bias." In their research, they found that "humans overwhelmingly overestimated the credibility of the system."[57] The Indian government established a system of "manual overrides" to address the issue of biometric errors that lead to

---

53 Jennifer Lee, "We Need a Face Surveillance Moratorium, Not Weak Regulations: Concerns about SB 6280," ACLU, March 31, 2020, https://www.aclu-wa.org/story/we-need-face-surveillance-moratorium-not-weak-regulations-concerns-about-sb-6280.

54 Section 2(7), Washington Senate Bill 6280, http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf?q=20200331083729.

55 See Ben Green and Yiling Chen, "Disparate Interactions: An Algorithm-in-the-Loop Analysis of Fairness in Risk Assessments," January 2019, https://www.benzevgreen.com/wp-content/uploads/2019/02/19-fat.pdf; Ben Green and Yiling Chen, "The Principles and Limits of Algorithm-in-the-Loop Decision Making," November 2019, https://www.benzevgreen.com/wp-content/uploads/2019/09/19-cscw.pdf; Megan Stevenson, "Assessing Risk Assessment in Action," *Minnesota Law Review* 103, no. 303 (2018), https://dx.doi.org/10.2139/ssrn.3016088; Berkeley J. Dietvorst, Joseph P. Simmons, and Cade Massey, "Algorithm Aversion:People Erroneously Avoid Algorithms after Seeing Them Err," *Journal of Experimental Psychology* 144, no. 1 (February 2015): 114–126, https://psycnet.apa.org/fulltext/2014-48748-001.html; Amirhossein Kiani et al., "Impact of a Deep Learning Assistant on the Histopathologic Classification of Liver Cancer," *npj Digital Medicine* 3, no. 23 (2020), https://doi.org/10.1038/s41746-020-0232-8.

56 Lee, "We Need a Face Surveillance Moratorium."

57 See Peter Fussey and Daragh Murray, "Policing Uses of Live Facial Recognition in the United Kingdom," in this compendium.

exclusion from government benefits and systems.[58] However, studies suggest that even these legal norms did not always govern the behavior of those operating the biometric systems on the ground. Those managing these systems often failed to exercise this option and refused people access to services because of "'incorrect' (or rather complete lack of) human intention in overcoming technological failure."[59]

An open question for future legal approaches is how to incentivize and ensure real capacity for human oversight. This would include an assessment of the gaps in knowledge, biases, or inefficiencies that limit accountability and prevent human operators from assessing or anticipating problems with these systems.

Should regulatory frameworks create a risk-based classification between "identification" and "verification" uses of biometric recognition?

What are the potential risks of a permissive regulatory approach to verification?

> *Recent official policy documents in the EU suggest that "verification" (1:1) is an inherently less risky use compared to identification (1:n) in terms of accuracy, data security vulnerabilities, and the capacity for meaningful consent.*
>
> *However, any broad-brush permissive approach to verification in the law should be avoided. Even if participation in a verification system is with knowledge, these systems might not afford individual's real choice when they act as gatekeepers to access essential spaces or services.*

The distinction between verification and identification is often described in terms of the technical shorthand 1:1 versus 1:n. 1:1 verification (or authentication) aims to determine whether people are who they claim to be through a one-to-one match that queries biometric information (e.g., a facial scan by a smartphone) against the data that the person has previously provided (e.g., the person stores their photograph on the phone when they first purchase it).[60] Identification, or 1:n, is a more technically involved process that compares the biometric information of an

58 Ronald Abraham et al., "State of Aadhaar Report 2017–18," IDinsight, May 2018, https://static1.squarespace.com/static/5b7cc54eec4eb7d25f7af2be/t/5bbd2874c8302561862f03d4/1539123330295/State+of+Aadhaar+Report_2017-18.pdf.

59 See Bidisha Chaudhuri, "Paradoxes of Intermediation in Aadhaar: Human Making of a Digital Infrastructure," *Journal of South Asian Studies* 42 (2019):572–587, https://doi.org/10.1080/00856401.2019.1598671.

60 See Stan Z. Li and Anil K. Jain, *Handbook of Face Recognition* (New York: Springer, 2005), 1–15.

unknown person against a database of many people's biometric data. An algorithm determines if the person is represented in the database and who they might be. Some identification systems provide a number of "similar faces" that meet a specified confidence or accuracy threshold.[61]

Recent official policy documents[62] as well as data-protection authorities in the EU[63] suggest that verification is an inherently less risky use of biometrics in terms of accuracy, data security vulnerabilities, and the capacity for meaningful consent. Biometric locks on phones are a common example used to demonstrate these claims, and San Francisco recently amended its facial recognition moratorium to allow employees to use biometric lock features on government-issued cell phones.[64] By contrast, some of the most controversial reported cases of facial recognition largely pertain to identification (1:n) systems like live facial recognition (LFR), which has a record of high error rates.

These accounts of verifications often link or even conflate the claim of higher accuracy with meaningful consent. The claim is that with verification systems, people are willing to present their biometrics in a "cooperative" way (like a frontal face with eyes open), whereas with identification, people could be unaware of being identified, which increases the error rates.[65] Any general assumption that verification systems involve the active and targeted participation of the individual, however, rests on shaky foundations. While these systems might have higher accuracy rates than identification systems, they are still predictive and not immune to the same kinds of errors and biases across lines of race, gender, and other demographic traits. More importantly, even if participation is done with volition and knowledge, these systems might not afford individuals real choice when they act as gatekeepers to access to essential spaces and services. This became a focal point in the opposition against biometric ID systems in India and Kenya,[66] as well as in the use of biometric systems in humanitarian contexts.[67]

---

61 Ibid.

62 See Luana Pascu, "New EU AI Strategy Puts Remote Biometric Identification in 'High-Risk' Category," BiometricUpdate.com, February 19, 2020, https://www.biometricupdate.com/202002/new-eu-ai-strategy-puts-remote-biometric-identification-in-high-risk-category; Paul de Hert and Koen Christianen, "Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data," Tilburg Institute for Law, Technology, and Society, April 2013, https://rm.coe.int/progress-report-on-the-application-of-the-principles-of-convention-108/1680744d81; see also, e.g., Article 29—Data Protection Working Party, "Working Document on Biometrics (WP 80)," 2003, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf; "Opinion 02/2012 on Facial Recognition in Online and Mobile Services (WP192)," March 23, 2012, https://www.pdpjournals.com/docs/87997.pdf; and "Opinion 3/2012 on Developments in Biometric Technologies (WP193)," April 2012, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf; and see CNIL, "Facial Recognition: For a Debate Living Up to the Challenges," December 19, 2019, https://www.cnil.fr/en/facial-recognition-debate-living-challenges.

63 See French data-protection authority CNIL, Communication central storage fingerprint, 2007; and cf. Els Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Dordrecht: Springer, 2013), 540.

64 Tim Cushing, "San Francisco Amends Facial Recognition Ban after Realizing City Employees Could No Longer Use Smartphones," *Techdirt*, December 20, 2019, https://www.techdirt.com/articles/20191219/18253743605/san-francisco-amends-facial-recognition-ban-after-realizing-city-employees-could-no-longer-use-smartphones.shtml.

65 See Li and Jain, *Handbook of Face Recognition*, 1–15.

66 Abdi Latif Dahir and Carlos Mureithi, "Kenya's High Court Delays National Biometric ID Program," *New York Times*, January 31, 2020, https://www.nytimes.com/2020/01/31/world/africa/kenya-biometric-ID-registry.html; see also reportage on the farcical nature of "consent camps" for Aadhaar discussed during the People's Tribunal on Aadhaar-related Issues, February 28, 2020, https://threadreaderapp.com/thread/1233608762604154880.html.

67 Petra Molnar, "The Contested Technologies That Manage Migration," CIGI Online, December 14, 2018, https://www.cigionline.org/articles/contested-technologies-manage-migration.

Proponents of permissive approaches to verification typically argue that these systems involve local data storage, which minimizes the data security risks that come with centralized databases. However, access control at borders, airports, and buildings often centralize biometric authentication systems for access to services, and many of these systems maintain centralized storage and authentication records.[68] Risks associated with biometric use are certainly contextual, but any broad-brush permissive approach to verification in the law should be avoided, especially where it can create loopholes that allow more harmful implementations of verification.

What kinds of due process safeguards are required for law enforcement use of biometric recognition?

Should law enforcement have access to these systems to begin with?

> *Outside of a complete ban on law enforcement use, recent regulatory approaches have focused on strengthening due process safeguards. This includes requiring warrants for ongoing surveillance, restricting the use of facial recognition to serious crimes, and ensuring defendants get meaningful access to biometric evidence that is used against them.*
>
> *While facial recognition has received special regulatory attention, these tools should be understood as part of a broader set of algorithmic police surveillance tools, including drone surveillance, license plate recognition, and predictive policing.*

The use of biometric technologies in policing raises a range of legal issues, many of which have been debated and litigated over the years in the context of fingerprinting and DNA.[69] These include the conditions under which biometric data can be taken (whether it should be at arrest or upon conviction), and the circumstances under which it should be deleted from such databases (for example, if a person is never convicted or if a conviction is overturned). The increasing shift to use of face and voice identifiers has exacerbated some of these existing concerns and created new ones. Indeed, law enforcement use of facial recognition has been the subject of intense public and regulatory scrutiny recently. These systems have misidentified people and been disproportionately used to target communities of color. Moreover, the vast majority of cases involving face recognition searches are not disclosed, depriving defendants of the ability to challenge evidence that could determine their fate in criminal trials.[70]

---

68 For an enumeration of concerns with centralized or centrally linked biometric ID infrastructures, see Access Now, #WhyID campaign, 2019, https://www.accessnow.org/whyid/.

69 See Robyn Caplan et al., "Data & Civil Rights: Biometric Technologies in Policing," *Data & Society*, October 27, 2015, https://datasociety.net/library/data-civil-rights-biometric-technologies-in-policing/; Brandon L Garrett, "DNA and Due Process," *Fordham Law Review* 78, no. 6 (2010): 2919–2960; Elizabeth N. Jones, "'Spit and Acquit': Legal and Practical Ramifications of the DA's DNA Gathering Program," *Orange County Lawyer Magazine* 51, no. 9 (September 2009), http://papers.ssrn.com/sol3/papers.cfm?abstractid=1809997.

70 See section on Florida case involving FACES facial recognition system used in the case against Willie E. Lynch in Rashida Richardson, Jason M. Schultz, and Vincent M. Southerland, "Litigating Algorithms 2019 US Report: New Challenges to Government Use of Algorithmic Decision Systems," AI Now Institute, September 2019, https://ainowinstitute.org/litigatingalgorithms-2019-us.pdf.

Outside of complete bans, there are multiple proposals that seek to regulate different aspects of law enforcement use. In their chapter, Jameson Spivack and Clare Garvie outline emergent regulatory approaches in the US that focus on limiting the use of facial recognition. Some limitations are based on the seriousness of the crime (e.g., only for violent felonies), while others ban the use in conjunction with body cameras or drones. There are also bills that would require a court order to run facial recognition searches,[71] as well as one that would require that defendants have access to source code and other information necessary to exercise their due process rights when algorithms are used to analyze evidence in their case.[72]

While facial recognition has received special regulatory attention, these tools should be understood as part of a broader set of algorithmic surveillance tools, including drone surveillance, license plate recognition, and predictive policing.[73] These systems raise similar challenges for established principles around procedural fairness, such as notice, hearing, the disclosure of evidence, establishing reasons for decisions, and the ability to challenge these decisions.

> *Law enforcement use of live facial recognition (LFR) has been the subject of intense public and regulatory scrutiny. Advocacy demands range from requiring a specific authorizing law to calls to ban law enforcement use of LFR altogether.*

Live facial recognition systems in public spaces are particularly controversial. Typically, cameras are deployed at a fixed location and the list of people who are identified is communicated to law enforcement officers on the ground.[74] Despite LFR's implications for privacy, criminal due process, and freedom of speech or expression, these tools have largely been rolled out without undergoing public and parliamentary scrutiny.

In their chapter, Peter Fussey and Daragh Murray describe London's expansive LFR program,[75] and discuss how the London Metropolitan Police successfully argued before the High Court that LFR was part of their inherent powers, and thus did not need new legislation to explicitly authorize its use.[76] The case is on appeal, but one of the factors that contributed to the Court's decision was the notion that LFR was not "invasive" technology and therefore did not require special sanction. Buenos Aires has also conducted an expansive LFR program.[77] In this case, the municipal government pushed through a resolution with truncated processes that authorized the use of these systems with minimal safeguards. Advocacy organizations have challenged the constitutionality of this ordinance.[78]

---

71 See, e.g., the proposed Facial Recognition Technology Warrant Act Of 2019, https://www.coons.senate.gov/imo/media/doc/FRTWA%20One-Pager%20FinalFinal.pdf.

72 "H.R. 4368: Justice in Forensic Algorithms Act of 2019," https://www.congress.gov/bill/116th-congress/house-bill/4368/text.

73 See Jay Stanley, "The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy," ACLU, 2019, https://www.aclu.org/report/dawn-robot-surveillance.

74 LFR refers to facial recognition that is "always on," identifying people in real time as they move through public and private space.

75 Metropolitan Police UK, "Live Facial Recognition," n.d., https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/.

76 *R(Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin), Case No. CO/4085/2018, 4 September 2019, para. 78. ("AFR Locate" is South Wales Police's nomenclature for LFR.)

77 Dave Gershorn, "The U.S. Fears Live Facial Recognition. In Buenos Aires, It's a Fact of Life," OneZero, Medium, March 4, 2020, https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d.

78 ADC, "ADC Files an Action of Unconstitutionality before GCBA."

Increasingly, privacy advocates are calling for a complete ban on LFR, viewing it as incompatible with fundamental rights and entailing risks that cannot be mitigated through procedural safeguards.

Are systems that process bodily data for purposes beyond establishing individual identity, like making inferences around emotional state, personality traits, or demographic characteristics, covered under existing biometric regulation?

Should such systems be permitted at all, given their contested scientific foundations and mounting evidence of harm?

> *Since many emotion recognition and personality prediction systems rely on face and voice data that could be used to identify an individual (even if that is not its current purpose), these systems could fulfill the definitional threshold of data-protection laws like the GDPR. Many recent moratorium bills in the US include systems that infer "emotion, associations, activities, or the location of an individual."*
>
> *However, many organizations are calling to ban these systems altogether given discredited scientific foundations and mounting evidence of harm.*

It is unclear whether existing biometric regulation will apply to systems where the primary purpose is to infer emotional states, interior characteristics, or identities like gender, race, ethnicity, and age.[79] The fact that these systems rely on face or voice data that could be used to confirm or establish an individual's identity (even if that is not its current purpose) could mean that these systems fulfill the definitional threshold of biometric data under data-protection laws like the GDPR. The European Digital Rights Initiative (EDRi) has also argued that biometric processing under the GDPR should be interpreted to include "detection of appearance, inferred behavior, predicted emotions or other personal characteristics."[80]

---

79 Some technical literature uses the term "soft biometrics" to define the process of "categorizing information about bodily traits where a person may not be identified in the process." See U. Park and A. K. Jain, "Face Matching and Retrieval Using Soft Biometrics," *IEEE Transactions on Information Forensics and Security* 5, no. 3 (September 2010): 406–415, https://doi.org/10.1109/TIFS.2010.2049842; and see A. Dantcheva, "What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics," *IEEE Transactions on Information Forensics and Security* 11, no. 3 (March 2016): 441–467, https://doi.org/10.1109/TIFS.2015.2480381.

80 Sarah Chander, "Recommendations for a Fundamental Rights-Based Artificial Intelligence Regulation," EDRi, June 4, 2020, https://edri.org/wp-content/uploads/2020/06/AI_EDRiRecommendations.pdf.

Many recent moratorium bills in the US include systems that use facial data for broader inferences, such as inferring "emotion, associations, activities, or the location of an individual."[81] The 2019 moratorium bills introduced in New York[82] and Washington[83] include any automated process by which characteristics of a person's face are analyzed to determine "the person's sentiment, state of mind, or other propensities including, but not limited to, the person's level of dangerousness." In specific contexts, these systems will require additional norms around explainability or transparency about how inferences are made, such as in the Illinois AI Videoconferencing Act 2019, which regulates the use of these tools in hiring.

81 E.g., Bill S.1385/H.1538. See ACLU Massachusetts, "Face Surveillance Moratorium," n.d., https://www.aclum.org/en/legislation/face-surveillance-moratorium. See also Ed Markey, "Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology," June 25, 2020, https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology; and Cory Booker, "Booker Introduces Bill Banning Facial Recognition Technology in Public Housing," November 1, 2019, https://www.booker.senate.gov/news/press/booker-introduces-bill-banning-facial-recognition-technology-in-public-housing.

82 Bill A6787D, New York https://www.nysenate.gov/legislation/bills/2019/a6787.

83 Bill HB 2856, Washington, https://app.leg.wa.gov/billsummary?BillNumber=2856&Year=2019&Initiative=false.

SECTION 3. EMERGING REGULATORY TOOLS AND ENFORCEMENT MECHANISMS

What are the different types of "bans" and moratoria that have been passed in the US over the last few years?

How can moratoria conditions be strengthened to ensure that eventual legislative or deliberative processes are robust?

How will bans and moratoria on government use impact the private development and production of biometric systems?

> *Over the past few years, a wave of municipal legislation has sought to ban government use of facial recognition in the US, and some states have also proposed similar bills. Many of these bans focus on law enforcement use. While some large tech companies have come out in favor of regulation, they have consistently pushed back against bans, often favoring much less stringent approaches.*
>
> *The term "moratorium" is shorthand for a range of regulatory interventions with varying conditions for when the restrictions would be lifted—from straightforward time-bound goals for drafting and authorizing legislation to the establishment of deliberative, consultative processes. Some moratorium bills prescribe specific conditions to ensure the quality of the legislation and meaningful community participation in any deliberative process.*

Many cities and states in the US have recently introduced legislation that bans government use of facial recognition, with a primary focus on law enforcement use.[84] These legislative interventions have played an outsize role in shaping the regulatory landscape by introducing a complete prohibition as a regulatory option against which other, less strict interventions will be compared. As Jameson Spivack and Clare Garvie point out in their chapter, advocates have been critical of weaker regulatory bills for "using up available political capital" and potentially undercutting demands for bans in the future.[85]

---

84 In their contribution to this compendium, Jameson Spivack and Clare Garvie track this legislative activity, noting that "[a]s of July 2020, the following municipalities had banned face recognition: Alameda, California; Berkeley, California; Boston, Massachusetts; Brookline, Massachusetts; Cambridge, Massachusetts; Easthampton, Massachusetts; Northampton, Massachusetts; Oakland, California; San Francisco, California; and Somerville, Massachusetts. A number of states proposed bans on face recognition during the 2019–2020 legislative session: Nebraska, New Hampshire, New York, and Vermont."

85 See Spivack and Garvie, "A Taxonomy of Legislative Approaches to Face Recognition in the United States," in this compendium.

Some of the largest technology companies that develop and sell these systems to law enforcement have been deeply engaged in these legislative processes, often publicly championing the need for some "regulation" but simultaneously lobbying against moratoria and bans. For example, Microsoft celebrated Washington State's SB 6280 ("Finally, progress on regulating facial recognition," Brad Smith, the company's general counsel, announced), only to face questions and criticisms about their involvement in pushing through a law that was considered weak by many organizations, and that effectively undercut a potential ban on government use.[86]

Moratoria and bans are often used interchangeably, yet Spivack and Garvie argue that this shorthand conceals a wide spectrum of regulatory interventions. Moratoria, in particular, contain a range of approaches that vary widely in terms of strictness and the conditions for lifting restrictions. While some moratoria stop all use of face recognition for a predetermined time, there is a risk that the legislature fails to act before the period is over and facial recognition use recommences without any further legislative intervention. On the other hand, directive moratoria ban the use of facial recognition until a law is passed and/or a statutory body (e.g, a task force or committee) is formed to submit recommendations for what to include in the law.

Moratoria can work to fast-track a deliberative or legislative process where one might not otherwise have been possible. While this is welcome, it is also eventually susceptible to the vested public and private interests that will push for weak or no legislation. There is a risk that a task force created by these laws "may not be representative of affected communities; may lack authority; or may be inadequately funded."[87] Some moratoria do more to prevent weak regulation than others. A 2019 Massachusetts law sets minimum requirements for what future legislation should achieve, including data privacy safeguards, auditing requirements, and protection for civil liberties. Similarly, the recently passed Washington State law specifies that the legislative task force be comprised of "advocacy organizations that represent consumers or protected classes of communities historically impacted by surveillance technologies including, but not limited to, African American, Hispanic American, Native American, and Asian American communities, religious minorities, protest and activist groups, and other vulnerable communities."[88]

---

86 See Dave Gershgorn, "A Microsoft Employee Literally Wrote Washington's Facial Recognition Law," *OneZero*, Medium, April 3, 2020, https://onezero.medium.com/a-microsoft-employee-literally-wrote-washingtons-facial-recognition-legislation-aab950396927; and see Lee, "We Need a Face Surveillance Moratorium."

87 See Spivack and Garvie, "A Taxonomy of Legislative Approaches"; see also Rashida Richardson, ed., "Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force," AI Now Institute, December 2019, https://ainowinstitute.org/ads-shadowreport-2019.html.

88 Section 10, Washington Senate Bill 6280, http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf?q=20200331083729

What regulatory tools can be used to create public transparency around the development, purchase, and use of biometric recognition tools?

> *Transparency around the development, purchase, and use of biometric recognition tools remains a key barrier to creating public awareness and enforcing existing regulation. Recent advocacy demands include mandatory impact assessments, public notice comment periods, and publicly accessible registries of vendors and uses.*

Enforcing existing regulations has been a challenge in part because the development, purchase, and use of biometric tools is often shrouded in secrecy, driven by private firms that have no duty to reveal such "proprietary information." Once these tools are built, the purchase and subsequent implementation by government, particularly law enforcement agencies, proceeds in ways that are often deliberately hidden from the public. Yet as scrutiny of Clearview AI and subsequent investigations have made clear, there are hundreds of globally distributed vendors selling biometric recognition technology without people's knowledge or explicit consent. It was only when the Clearview AI story broke that lawsuits were filed under Illinois BIPA, prompting quick action from the company that had violated informed consent requirements when scraping millions of face images off the web.[89]

In recent years, privacy advocates have demanded regulatory tools that ensure transparency as early in the process as possible. Many of these policies target government use to ensure that there is public notice and consultation before these tools are acquired and implemented. For example, in June 2020, after years of civil society advocacy, and in the context of sustained protest against anti-Black police brutality, New York City passed The POST Act, a law that would require the New York Police Department (NYPD) to issue a surveillance impact and use policy about any surveillance technology in use (including biometric recognition tech).[90] This assessment would include information about capabilities, processes and guidelines, and any safeguards and security measures in place. In the EU, advocacy organizations like Access Now and Algorithm Watch have called for a mandatory disclosure scheme for all AI systems used in the public sector, in conjunction with a mandatory human rights or algorithmic impact assessment.[91]

Advocates have also demanded that regulation should ensure that external researchers and auditors have access to algorithmic systems in order to understand their workings, as well as the design choices and incentives that informed their development and commercialization, and to engage the public and impacted communities in the process. Meaningful access includes making software toolchains and APIs open to auditing by third parties.

---

89 Even these faced the barrier of establishing legal standing because it was difficult to confirm that an Illinois resident was in fact part of Clearview's dataset due to the lack of publicly available information. See *ACLU v. Clearview AI*, https://www.aclu.org/cases/aclu-v-clearview-ai.

90 The surveillance impact and use policy would first be released in draft form for review by the public. See STOP Spying, POST Act, signed July 7, 2020, https://www.stopspying.org/post-act.

91 Access Now, "Access Now's Submission to the Consultation on the 'White Paper on Artificial Intelligence—a European Approach to Excellence and Trust," May 2020, https://www.accessnow.org/cms/assets/uploads/2020/05/EU-white-paper-consultation_AccessNow_May2020.pdf.

While advocates continue to push for more transparency, some laws have already enacted certain checks and balances. The GDPR currently has provisions for data-protection impact assessments (DPIA) and "privacy by design" assessments that kick in when there is any "large-scale" processing of biometric data and also in cases of surveillance in publicly accessible spaces. In theory, these offer a robust assessment of the rights implications of the use of these systems, including fundamental questions about necessity and proportionality. However, as Els Kindt notes in her chapter, DPIAs have been challenging to implement in practice, with wide variations across different member countries of the EU. Moreover, the predominant focus on data-protection concerns can leave out inquiries about accuracy or discriminatory impact. Recent proposals around algorithmic impact assessments (AIAs) are structured to include this broader range of concerns and ensure the participation of directly impacted communities in the risk-identification process.[92]

While transparency and accountability measures have gained momentum, procurement contracts with third-party vendors can inhibit the government's ability to comply.[93] Government procurement of biometric and other forms of AI systems is often confidential due to trade secrecy or other intellectual property claims. When challenged, governments have denied any knowledge or ability to explain and remedy the problems created by these systems. Recent advocacy by civil society organizations and certain city governments in Europe focuses on including standard contractual clauses in these contracts that include waivers to trade secrecy, non-disclosure agreements, or other confidentiality clauses, as well as terms that ensure the process of procurement involves open bidding and public notice.[94]

What role can community-led advocacy play in shaping the priorities and impact of regulation?

> *Community advocacy to regulate biometrics is growing, playing a crucial role in surfacing evidence of harm, and shaping the rights and protections that policy interventions eventually offer.*

Advocacy and mobilization against the use of biometric systems have taken many forms. While traditional digital rights or privacy groups remain active, over the past few years, directly impacted communities have also organized to push back against these systems based on their lived experiences of harm.

---

92 See AI Now's detailed AIA framework that public agencies can draw from when implementing AIAs: Dillon Reisman et al., "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability," AI Now Institute, April 2018, https://ainowinstitute.org/aiareport2018.pdf. The Canadian government's Algorithmic Impact Assessment tool is also a useful template for regulatory agencies; see Government of Canada, AIA, 2019, https://canada-ca.github.io/digital-playbook-guide-numerique/views-vues/automated-decision-automatise/en/algorithmic-impact-assessment.html. ICO's draft auditing framework for AI systems also has helpful guidance on how to document risks, manage inevitable trade-offs, and increase reflexivity at every stage of ADS procurement or development.

93 See *Houston Federation of Teachers v. Houston Independent School District* and *Ark. Dep't of Human Servs. v. Ledgerwood* cases in Richardson, Schultz, and Southerland, "Litigating Algorithms 2019 US Report."

94 AI Now Institute, City of Amsterdam, City of Helsinki, Mozilla, and Nesta, "Using Procurement Instruments to Ensure Trustworthy AI," June 15, 2020, https://foundation.mozilla.org/en/blog/using-procurement-instruments-ensure-trustworthy-ai/.

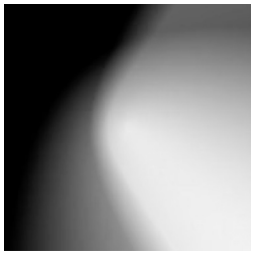
In India, a coalition of privacy groups and grassroots welfare activists formed to publicly protest and legally challenge the Aadhaar biometric ID project.[95] Against the broad claims of efficiency by the government, the coalition surfaced specific examples of exclusion due to the technical and bureaucratic failures of the system. In their chapter, Stefanie Coyle and Rashida Richardson recount the community-driven advocacy in Lockport, New York, where a group of parents organized against the school district's decision to purchase and deploy facial recognition in schools. Eventually, Coyle and Richardson note, "[p]arents shifted the discourse from debating whether the biometric surveillance system was necessary to focus on the real harms posed to students if the school district decided to move forward." As a result of that advocacy, the New York State Senate introduced a moratorium bill that "mirrors the concerns raised by residents in the community and advocates across the state and country."

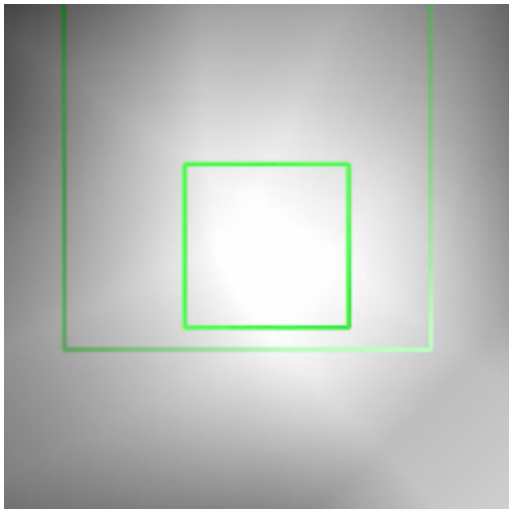
Large-scale biometric projects are often promoted in terms of lofty claims about security, accuracy, and efficiency. Community advocacy, particularly on the part of those directly impacted by these systems, has been critical in surfacing key questions like: Efficiency for whom? (In) security for whom? Those required to live under biometric surveillance possess an expertise that cannot be gained by examining these systems at a technical or policy level. There is no way to guarantee the just use of these technologies without centering the experiences of those affected by their use. Recent attempts demonstrate how community interventions can be structured, for example, the "Citizen Biometric Councils" run by the Ada Lovelace Institute in the UK,[96] and the New York City ADS Task Force "Shadow Report" prepared by a civil society coalition with detailed recommendations to ensure community engagement is meaningful and equitable.[97] Ultimately, this underscores the importance of community deliberation to the processes that decide whether these systems are used, but also to the kinds of rights and protections that policy interventions eventually offer.

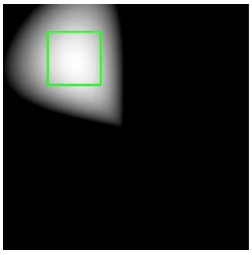
95 See Rethink Aadhaar, https://rethinkaadhaar.in/.

96 See Ada Lovelace Institute, "Citizen's Biometric Council" https://www.adalovelaceinstitute.org/our-work/identities-liberties/citizens-biometrics-council/

97 Rashida Richardson, ed., "Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force", AI Now Institute, 2019, https://ainowinstitute.org/ads-shadowreport-2019.html.







TIMELINE OF LEGAL DEVELOPMENTS

This timeline tracks the key legal and regulatory developments analyzed in this compendium. The specific chapters where they are discussed are noted below.

October 2008

United States
Illinois Biometric Information Privacy Act (BIPA) enacted *(See Chapter 8)*

March 2016

India
Aadhaar Act enacted *(See Chapter 3)*

April 2018

European Union

General Data Protection Regulation (provisions on biometric data) enacted *(See Chapter 4)*

Data Protection Law Enforcement Directive enacted *(See Chapter 4)*

September 2018

India
Indian Supreme Court restricts private use of Aadhaar Biometric ID system *(See Chapter 3)*

2008 2016 2017 2018 2019

April 2019

Jamaica
Jamaican Supreme Court rules biometric ID system unconstitutional *(See Chapter 1)*

May 2019

United States
San Francisco ban on government use of facial recognition technology passed *(See Chapter 7)*

June 2019

United States
Somerville, MA ban on government use of facial recognition technology *(See Chapter 7)*

July 2019

United States
Oakland, CA ban on government use of facial recognition technology *(See Chapter 7)*

Australia
Identity Service Matching Bill introduced *(See Chapter 2)*

Kenya
Huduma Bill (legal authorization for NMIMS project) introduced *(See Chapter 1)*

August 2019

International Committee of Red Cross
ICRC assembly adopts Biometrics Policy *(See Chapter 5)*

September 2019

United States
California Body Camera Accountability Act (A.B 1215) (moratorium on existing use of face recognition on body-worn cameras till 2023) passed *(See Chapter 7)*

United Kingdom
UK High Court finds Live Facial Recognition permissible, rules out need for new authorizing legislation *(See Chapter 6)*

United States
Justice in Forensic Algorithms Act of 2019 (HR 4368) introduced *(See Chapter 1)*

October 2019

United States
No Biometric Barriers to Housing Act (S 2689) introduced *(See Chapter 1)*

Australia
Identity Service Matching Bill rejected by Australian Parliament *(See Chapter 2)*

United States
Berkeley, CA ban on government use of facial recognition technology passed *(See Chapter 7)*

Argentina
Constitutional challenge to Buenos Aires Live Facial Recognition project *(See Chapter 1)*

November 2019

United States
The Facial Recognition Technology Warrant Act of 2019 (S 2878) introduced *(See Chapter 1)*

December 2019

United States
Northampton, MA ban on government use of facial recognition technology passed *(See Chapter 7)*

United States
Alameda, CA ban on government use of facial recognition technology passed *(See Chapter 7)*

United States
Brookline, MA ban on government use of facial recognition technology passed (*See Chapter 7*)

2019 | 2020

January 2020

United States
Cambridge, MA ban on police use of facial recognition technology passed *(See Chapter 7)*

Kenya
Kenyan High Court suspends NMIMS biometric ID project *(See Chapter 1)*

United States
California Consumer Privacy Act (provisions on biometric data) enacted *(See Chapter 1)*

February 2020

United States
Springfield, MA moratorium on government use of facial recognition technology passed *(See Chapter 7)*

March 2020

United States
Washington SB 6280 (regulates government use of facial recognition technology) passed *(See Chapter 7)*

June 2020

United States
Facial Recognition & Biometric Technologies Moratorium Bill S 4084 introduced *(See Chapter 7)*

United States
New York Public Oversight of Surveillance Technology (POST) Act (Int 0487-2018) passed *(See Chapter 1)*

July 2020

United States
New York Senate Bill S5140B (regulating biometric technologies in school) passed *(See Chapter 9)*

August 2020

United States
National Biometric Privacy Act (S ___) introduced *(See Chapter 1)*