# REGULATING AND HARMONIZING BIOMETRIC ECOSYSTEMS: ADDRESSING THE FULL SPECTRUM OF RISKS USING GLOBAL SAFETY MODELS AND CONTROLS

*The spectrum of biometric technologies today is expansive, encompassing many types, or modalities, of biometrics, from face recognition to iris to fingerprint to DNA, used singly or in combination. Biometrics are a significant category of technology; at least 104 countries use fingerprint and/or iris as part of national ID systems,*[**] *and uses for biometrics extend well beyond the national ID system context in both private and public sector use.*[***] *Increasingly understood as a technology of concern based on scientific data, there is a growing body of law and regulations seeking to mitigate the risks associated with biometric technologies. Current approaches to biometric regulation thus far, however, have been insufficiently constructed, and do not address the full ecosystem of biometric modalities*[****] *and the risks that can arise from them.*

Pam Dixon[*]

TPQ

**Winter 2021/22**

[*] Pam Dixon is an author, researcher, and the founder and Executive Director of the World Privacy Forum, a non-profit public interest group. She writes extensively about face recognition and biometrics, including in peer-reviewed studies.

[**] ID4D 2018 Global Dataset, 2020 updates. World Bank, (2020). https://datacatalog.worldbank.org/search/dataset/0040787

[***] Uses range from authentication uses, such as face or fingerprint authentication for mobile phones, to uses in the criminal investigation context. Diverse commercial applications exist, for example, photo management applications that use face recognition, or biometric-based employee clock-in devices designed for workplaces.

[****] Biometric modalities include: DNA, face, fingerprint, speech, voice, iris, retina, periocular, ear, gait, tattoo, heartbeat, hand geometry, odor, behavioral, typing recognition, vein recognition, for example. See Biometrics Institute: https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

In recent years, biometrics have been advanced by deep learning architectures and techniques, and the advances far outpace policy adaptations.[1] The full biometric ecosystem – from data collection to algorithmic quality, from the hardware of biometric systems, to the implementation of the full systems – has components that create, or can create, meaningful risks. These risks have been rigorously documented and are no longer theoretical. The infrastructure components of face recognition systems, such as the cameras used, for example, can have a significant impact on the accuracy and functioning of the underlying algorithms.[2] In contactless fingerprint systems, which are still rapidly evolving, simple things such as how far away the fingers are to be scanned are making a difference in accuracy.[3] The primary controversies around face recognition systems[4] arise largely from the well-documented potential for racial, gender, and age[5] bias, as well as politically-driven utilization of such systems.[6] Additionally, some face recognition systems rely on unconsented data collections, which is also controversial.[7]

As compelling as it is to discuss biometric systems and risks in isolation, for example, by focusing on a single modality such as face recognition or DNA or even on a particular use case, it is essential to contextualize biometric systems in the broader context of all biometric modalities, and view biometrics as a complete ecosystem of multiple biometrics. Additionally, biometric modalities are often layered in what is called a multi-modal or multi-biometric approach, combining face

[1] Certain modalities of biometrics, particularly face recognition systems, have been profoundly changed by advances in certain AI architectures, specifically, Convolutional Neural Networks (CNNs). See, Mayank Vatsa, Richa Singh, Angshul Majumdar, Ed. *Deep Learning for Biometrics* (CRC Press, 2018).

[2] David Leslie, "Understanding bias in face recognition technologies, an explainer," *The Alan Turing Institute, October 2020.* https://www.turing.ac.uk/sites/default/files/2020-10/understanding_bias_in_facial_recognition_technology.pdf

[3] J. Libert, J. Grantham, B. Bandini, K. Ko, S. Orandi and C. Watson, *NIST Report (NISTIR) 8307: Interoperability Assessment 2019: Contactless-to-Contact Fingerprint Capture, NIST, (2019).* https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8307.pdf

[4] European Parliament Resolution A9-0232/2021: *Artificial Intelligence in Criminal Law and its Use by Police and Judicial Authorities in Criminal Matters, (2020/2016/INI), adopted 6 October 2021, Strasbourg, France.* https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html, sections 25-31 in particular.

[5] Age bias in face recognition occurs in both younger and older individuals. See Anil Jain, *Biometric Recognition of Children, Challenges and Opportunities* (Michigan: Michigan State University, 7 June 2016). http://biometrics.cse.msu.edu/Presentations/AnilJain_UIDAI_June7_2016.pdf. See also Patrick Grother, Mei Ngan, Kayee Hanaoka. *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects in Facial Systems*, NIST (December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/ NIST.IR.8280.pdf.

[6] Patrick Grother, Mei Ngan, Kayee Hanaoka. *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects in Facial Systems*, NIST (December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/ NIST.IR.8280.pdf. Regarding political risks, see: Teki Falconer and S. Okedara, "National Security Exemptions, The Dark Side of Identity Systems," Episode 24, Segment 3. https://id4africa.com/livecast-ep24-the-dark-side-of-identity-part-2/

[7] *Facial Recognition: the CNIL orders Clearview AI to stop reusing photographs available on the Internet,* CNIL France, 16 December 2021. https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet

and iris, or iris and fingerprint, and so on.[8] As discussed, current legal frameworks do not yet effectively address the full range of biometric modalities and the risks associated with them, resulting in incomplete policy protections and fragmentation. Fragmented approaches toward the regulation of biometrics is a category risk in and of itself, and ultimately, fragmented approaches are not a sustainable solution for the types of meaningful risks biometrics can pose within jurisdictions, and across jurisdictional boundaries. Even the most robust policy solutions implemented thus far to mitigate the risks of face recognition systems are extremely limited when compared to the full continuum of biometric modalities that require regulatory attention.

> *"Further, the policy tools that have been the primary focus thus far for biometric controls are important, but nonetheless incomplete for the job; these include principles for responsible use, the utilization of consent mechanisms as a control, and bans or moratoriums."*

Currently, more than 145 jurisdictions have passed comprehensive national-level data governance and protection frameworks.[9] Because these frameworks often use generalized language regarding protections for biometric data, the existing rules cover biometrics, but often lack specifics tied to any particular modality of biometric. In the European Union (EU), the EU General Data Protection Regulation (GDPR),[10] covers biometrics as a sensitive data category. The GDPR does not address specific face recognition, iris, or multi-modal concerns, and does not address face recognition uses for some important use cases, for example, national security uses of biometrics are not covered under the GDPR. Beyond the GDPR, in multiple jurisdictions, regulatory solutions for biometric risks often have a strong emphasis on the modality of face recognition, iris, fingerprint, or DNA, and do not reflect a more mature legislative model.[11] The current approaches to biometric regulation are well-meaning but incomplete, and have created meaningful gaps in protections. On one hand, comprehensive legislation is too broad to be specific enough. On the other, a focus on single-modality biometric legislation is too narrow, and leaves gaps

[8] Multimodal biometrics and biometric fusion are instances when one or more biometric attributes are used together. The term *multibiometric may also be used. See:* Maneet Singh, Richa Singh, Arun Ross. "A comprehensive overview of biometric fusion," *Information Fusion,* Vol. 52 (2019): p. 187-205. https://www.cse.msu.edu/~rossarun/pubs/Singh-RossBiometricFusion_INFFUS2019.pdf

[9] Graham Greenleaf, "Global Data Privacy Laws 2021: Uncertain Paths for International Standards," (11 February 2021), p. 169; *Privacy Laws & Business International Report*, p. 23-27, Available at SSRN: https://ssrn.com/abstract=3836408

[10] *EU General Data Protection Regulation*, http://www.privacy-regulation.eu/en/index.htm. The GDPR went into effect 25 May 2018. See in particular Article 9.4.

[11] *Biometric Information Protection Act (760 ILCS 14) (Illinois)* https://ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004

regarding the other modalities, and gaps regarding multi-modal systems.

Further, the policy tools that have been the primary focus thus far for biometric controls are important, but nonetheless incomplete for the job; these include principles for responsible use, the utilization of consent mechanisms as a control, and bans or moratoriums. For example, subnational legislation in the United States tends to focus on single biometric modalities, such as face recognition, and consent is often the primary tool utilized for protection.[12] Consent, when utilized by itself without any other administrative or procedural controls or underlying protections, provides quite poor protections in the biometric context.[13] The failure to conceptualize biometric guardrails in a more sophisticated ecosystem approach will lock in fragmented approaches, which over time, promises to create regulatory havoc and gaps in protections. It is an unsustainable policy strategy for national or sub-national legislatures to craft multiple, stand-alone, and possibly rivalrous biometric policies for separate biometric modalities and selected biometric use cases.

The chemical safety model, because it is both broad and granular, reduces policy fragmentation with meaningful, measurable, and well-understood and documented risk evaluations and mitigations. The global body of chemical safety regulations exists in most countries to monitor chemicals that pose dangers to people and to protect people from a complex range of chemicals.[14] Chemical safety policies that are crafted at the national and subnational levels are built according to a common framework, use the same definitions, are fit for each jurisdiction, and are also harmonized globally while respecting jurisdictional contexts. Biometrics, as an equally complex data ecosystem with overarching risks and particular risks attached to specific modalities, could be similarly regulated under an umbrella of controls derived from safety and risk-oriented regulatory models, with each biometric modality receiving appropriate and granular regulatory attention befitting the modality being considered. Additional risks that arise from mandatory biometric enrolment in some systems is an additional type of risk to consider and mitigate, among other types of risks.

[12] *Biometric Information Protection Act (760 ILCS 14) (Illinois)* https://ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004, Capture or use of Biometric Identifiers, Sec. 503.001. Title 11. (Texas) https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm

[13] Consent has important uses, particularly in human subject research, where consent must be meaningful. International norms have developed around this context for consent. See: 21 CFR 50.20 *General Requirements for Informed Consent. See also: 45 CFR part 46 and HHS, Federal Policy for the Protections of Human Subjects ('Common Rule')* https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html. Consent as a primary tool for all data protection and privacy contexts, however, has been replaced by policies around legitimate basis for processing, among other protections. See "Click to Consent? Not good enough anymore," *Privacy Commissioner of New Zealand, 2019.* https://privacy.org.nz/blog/click-to-consent-not-good-enough-anymore/

[14] United Nations, *GHS*, https://www.unece.org/trans/danger/publi/ghs/ghs_welcome_e.html; The World Health Organization operates the International Programme on Chemical Safety (IPCS), https://www.who.int/health-topics/chemical-safety#tab=tab_1

The most salient hallmark of chemical safety regulation models is the robust procedural and administrative controls they use, joined with highly granular applicability. For example, the regulations present an umbrella under which many types of chemicals can be individually regulated. Lead and arsenic, for example, are regulated under the same overarching framework, but lead and arsenic have differing protections and cutoff points, as is appropriate given the toxicological differences. In chemical safety regulations, the country-level legal frameworks are then harmonized by two multilateral institutions, the World Health Organization and the United Nations. The UN has a program called the *Globally Harmonized System of Classification and Labelling of Chemicals* (GHS), which is regularly updated.[15] The idea of the UN GHS is to bring a global, standardized approach to chemical safety across all jurisdictions.[16] Labeling is to be the same, level or grade of the risk is the same, and risk mitigation strategies would be similarly harmonized internationally. The UN GHS plan is part of the implementation of the Sustainable Development Goals (SDGs).

> *“These administrative and procedural controls provide a toolbox of options that go beyond best practices, simple consent structures, and narrow bans, and could readily be utilized in biometrics. Under this type of framework, all biometric modalities would be regulated under one umbrella.”*

The key controls in chemical safety models include:

- Pre-market safety, quality, and other risk assessments and requirements
- Registration of products
- Ongoing product documentation
- Audits
- Post-implementation surveillance (observation) and documentation
- Compliance labeling

[15] *GHS, Rev. 8, (2019). United Nations.* https://unece.org/ghs-rev8-2019

[16] United Nations, *GHS*, https://www.unece.org/trans/danger/publi/ghs/ghs_welcome_e.html

- Safety certifications

- Technological proof of compliance and risk mitigation

- Ongoing review, oversight, and multistakeholder feedback (and complaint mechanisms).

These administrative and procedural controls provide a toolbox of options that go beyond best practices, simple consent structures, and narrow bans, and could readily be utilized in biometrics. Under this type of framework, all biometric modalities would be regulated under one umbrella. Each modality would be subject to meaningful administrative and procedural controls. All biometrics -- DNA and face recognition, along with the other biometric modalities -- would be evaluated under the auspices of the regulation, with their own measures for accuracy and pre-market fitness.

In practice, this would mean that before a biometric product could be put out in the market, it would have to be assessed for pre-market safety, quality, and other risks. For face recognition systems, this would mean that the product could not be discriminatory in its operations, and the risk points would have rigorous testing. For example, age, gender, and race biases would be tested. Each biometric product, after passing the assessment, would be registered, labelled, and would be required to submit documentation to regulators. Regulators would be able to conduct audits, and there would be a post-implementation market surveillance and documentation program. Safety certifications would need to be met, and biometric products would need to proactively provide proof of compliance and mitigate known risks. And finally, there would be an ongoing review of the biometric products, consumer and end-user feedback, as well as formal complaint mechanisms.

In considering how this system could be worked out in practice, it is useful to review some exemplar implementations regarding chemical safety regulatory models. The regulations are notable, in that they are harmonized across borders, yet the regulations are also fit for each country-level context of economic and technological development. This is important and would need to be present for any harmonized biometric approaches.

The EU has two significant member state-wide regulatory models in chemical safety. Both regulations offer excellent tools for mitigating harms. REACH[17] is the European Regulation on Registration, Evaluation, Authorization and Restriction of Chemicals. It entered into force in 2007, replacing the former legislative framework for chemicals in the EU. This important and precedent-setting regulation applies

[17] European Commission, *REACH*, https://ec.europa.eu/growth/sectors/chemicals/reach_en

to essentially every chemical product manufactured, imported, or sold within the EU. Manufacturers and importers must register all substances produced above a set yearly volume, and must identify risks associated with the substances they produce, demonstrate compliance in mitigating the risks, and establish safe use guidelines for the product so that the use of the substance does not pose a health threat.

Another precedent-setting regulation, RoHS,[18] applies to any business that sells electrical or electronic products, equipment, sub-assemblies, cables, components, or spare parts directly to RoHS-directed countries. Products must be cleared for market prior to launch. All parties in the supply chain must provide documentation/recordkeeping, regularly update information, mandatory compliance labeling. All of these features could be helpful in regulating biometric products. Other countries that have enacted RoHS include Japan, Korea, and China. In the U.S., the states of California, Colorado, Illinois, Indiana, Minnesota, New Mexico, New York, Rhode Island, and Wisconsin, among others, have enacted RoHS-like and e-waste regulations.

In the U.S., a federal statute, the Chemical Safety for the 21st Century Act,[19] regulates chemical substances of concern. The statute has these compliance requirements: pre-manufacture notification for new chemical substances prior to manufacture, where risks are found (after risk assessment), testing by manufacturers, importers, and processors, certification compliance, reporting and record keeping. If a substance presents a substantial risk of injury to health or the environment, the party must immediately inform the EPA. As mentioned earlier, in addition to the Chemical Safety for the 21st Century Act, some states adopted additional EU-style regulations after the European RoHS model.

Most countries in Africa already have regulations in place that assert legally binding controls on toxic substances. Lead is one example of a regulated toxic substance under a variety of such laws in African countries. In Algeria, for example, Arrêté No. 004/MINEPDED/CAB of 21 September 2017, modifies and completes the list of chemicals in Décret No. 2011/2581/PM of 23 August 2011, which regulates dangerous chemicals. Among other controls, the regulations prohibit the manufacture, sale and import of paints containing more than 90 ppm of lead (10/8/17). Algeria, Cameroon, Ethiopia, Kenya, South Africa, and Tanzania are among the African countries that have similar regulations.

India has adopted the National Action Plan for Chemicals; India's version of

[18] European Commission, *RoHs Directive*, Current: (2011/ 65/ EU). First RoHS Directive: (2002/95/EC), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex%3A32011L0065

[19] U.S. Environmental Protection Agency, *Chemical Safety for the 21st Century Act*, https://www.epa.gov/assessing-and-managing-chemicals-under-tsca/frank-r-lautenberg-chemical-safety-21st-century-act

safety regulations for hazardous chemicals.[20] In the past, India's regulations were not modeled after "REACH," the EU regulation. In late 2019 and continuing into 2020, however, India embarked on the creation of a National Action Plan for Chemicals (NAPC) to move into a more REACH-like system.[21] The idea is to create a harmonized system of classification of toxic chemicals that complies with the UN's Global Harmonization Strategy for chemical safety. Helping this effort is India's standing committee for chemical safety legislation, the National Coordination Committee (NCC) under the Ministry of Environment, Forest and Climate Change (MoEF&CC).[22] The late 2019 draft National Action Plan for chemical safety for India recommendations to compile a national chemicals inventory; analyze and assess the risks of those chemicals; implement the UN Global Harmonization Strategy (GHS); and develop risk mitigation strategies, policies and regulations.

The rich, adaptable, comprehensive, and yet granular chemical safety models in use today provide a pathway to move biometric regulation away from the fragmented and ineffective current practices that rely on consent, bans, and single-modality regulations. It is essential that complex biometric ecosystems are regulated consistently, comprehensively, and in a manner that is harmonized across jurisdictions so that biometrics are not subject to fragmentation that results in inconsistent or weak data governance, security, and privacy protections. Biometrics, as a technology of concern, merits high levels of attention to administrative and procedural controls, as well as a focus on harmonization on key aspects of regulation, such as agreement on definitions.

[20] National Disaster Management Authority of India, *Chemical Disaster Page*, https://ndma.gov.in/en/2013-05-03-08-06-02/disaster/man-made-disaster/chemical.html

[21] *Chemical Watch*, "India's draft national plan includes inventory and registration," 6 January 2020, https://chemicalwatch.com/86343/indias-draft-national-chemical-plan-includes-inventory-and-registration

[22] Government of India, Ministry of Environment, Forest, and Climate Change, http://moef.gov.in