WORLD **PRIVACY** FORUM

Face Recognition Systems: Expanding solutions by using time-tested safety models to address face recognition risks

Pam Dixon,[1] Executive Director
03 September 2020

I. Introduction: Moving from a limited policy toolset to a mature systems approach

Face recognition systems and other biometrics such as iris and fingerprint are growing in use, alone and in combination, across many, if not most, international jurisdictions.[2] Along with this growth, biometric systems have become increasingly controversial, especially face recognition systems. The controversies around face recognition systems are a result of the meaningful privacy and civil liberties challenges these systems present, and equally, the documented potential for racial, gender, and age[3] bias in face

---

[1] Pam Dixon is the Executive Director of the World Privacy Forum, a non-profit public interest group. She has researched and written extensively about face recognition and biometrics, including peer-reviewed studies. See, Pam Dixon, *A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S., S*pringer Nature, Health Technology. DOI 10.1007/s12553-017-0202-6. http://rdcu.be/tsWv. Open Access via Harvard- Based Technology Science: https://techscience.org/a/2017082901/. See also: *RADPA: Proceedings of the first Roundtable of African Data Protection Authorities: Status and response to privacy risks in Identity Systems (English)* (Pam Dixon, rapporteur, ID4Africa event, June 2019.) Available at: http://www.id4africa.com/2019/files/RADPA2019_Report_Blog_En.pdf.

[2] *The facial recognition world map*, SurfShark. Available at: https://surfshark.com/facial-recognition-map.

[3] Age bias in face recognition occurs in both younger and older individuals. One of the authoritative experts regarding children and biometrics is Professor Anil Jain. See: Anil Jain, *Biometric Recognition of Children, Challenges and Opportunities*. Michigan State University, June 7, 2016. Available at: http://biometrics.cse.msu.edu/Presentations/AnilJain_UIDAI_June7_2016.pdf. Another ex- pert in this area is Clarkson University Endowed Professor in Engineering Science and CITeR Director and Stephanie Shuckers. See: Chris Burt, *CITer Director talks research to inform dialogue on children's biometrics and privacy*. Biometric Update, December 3, 2019. Available at: https://www.biometricupdate. com/201912/citer-director-talks-research-to-inform-dialogue-on-childrens-biometrics-and-privacy. For a discussion of age effects at the older end of the spectrum, see: Patrick Grother, Mei Ngan, Kayee Hanaoka. *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects in Facial Systems*, NIST, December 2019. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/ NIST.IR.8280.pdf.

recognition systems and their utilization.[4] Additionally, some face recognition systems have been built on unconsented data collections, which is also controversial.[5]

The lifecycle of face recognition systems from data collection to implementation to utilization has components that create, or can create, meaningful risk. With the increased utilization of face recognition systems, the risk level is high enough now that commonly-used regulatory controls such as simple consent mechanisms or indirect consent are no longer practicable for addressing the full range of risks that face recognition technologies present.

Solutions that have been proposed thus far to mitigate the risks of face recognition systems are extremely limited when compared to the full continuum of regulatory solutions that are actually available for use. The solutions generally utilized in face recognition today generally fall into four major categories:

- **Principles / Responsible use**
- **Limited legislative controls** (strong reliance on simple consent mechanisms)
- **Moratorium** (typically time-barred)
- **Outright ban**

To date, regulatory solutions for face recognition risks have overall had a strong emphasis on principles (responsible use, including the utilization of consent mechanisms as a control) and bans / moratoriums. In some jurisdictions, there are biometric regulations in the form of generalized privacy regulations, such as the EU General Data Protection Regulation (GDPR),[6] which covers biometrics as a sensitive data category. However, the GDPR does not address specific face recognition concerns and does not generally address with specificity face recognition uses for law enforcement or national security purposes. Some face recognition legislation currently exists in a number of other jurisdictions, but the legislation is often focused on narrow aspects of use, and has not been developed with a more mature risk model in mind.

For example, The U.S. does not have any consolidated regulatory framework across sectors focused only on face recognition policy. Some laws touch on biometrics held by sectoral entities, like the federal government. But sectoral laws, like the Privacy Act of 1974, do not mention biometrics specifically. One of the specific laws that does discuss explicit consent for biometrics is currently at the state level, for example, an Illinois state law that generally requires consent prior to biometrics collection.[7] This law, the Biometric Information Privacy Act (BIPA), however, does not have a complex or complete regulatory approach to biometrics or face recognition. BIPA relies heavily on consent, and the consent model of BIPA is not complex. To find mature consent policy

---

[4] Patrick Grother, Mei Ngan, Kayee Hanaoka. *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects in Facial Systems*, NIST, December 2019. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/ NIST.IR.8280.pdf.

[5] An example of unconsented use in face recognition is when vendors "scrape" web sites for images, and utilize those images in a face recognition product at one or more points of the product lifecycle. See, for example, Anna Merlan, *Here's the file Clearview AI has been keeping on me, and probably on you too*, Vice, Feb. 28, 2020. Available at: https://www.vice.com/en_us/article/5dmkyq/heres-the-file-clearview-ai-has-been-keep- ing-on-me-and-probably-on-you-too. The author of this article used the California Consumer Protection Act (CCPA) to request the information that Clearview AI held on her. She found that the company had col- lected, or "scraped," photos of her from MySpace, Twitter, Instagram, and other websites.

[6] EU General Data Protection Regulation, (EU-GDPR). Available at: http://www.privacy-regulation.eu/en/index.htm The GDPR went into effect May 25, 2018.

[7] Illinois Biometric Information Privacy Act, (760 ILCS 14/) Available at: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

examples in the U.S., one has to study policy assertions apart from biometrics. The U.S. Food and Drug Administration (FDA) has a detailed definition of consent, for example, which specifies what must be done to ensure that the consent is meaningful, voluntary, and not coerced.[8] Some additional current legislative approaches in the U.S. regarding face recognition can be found in disparate pockets of work. For example, at least 11 states regulate the use of biometrics specifically in schools (fingerprint, face recognition).[9] There is also limited state-level legislation around some additional types of biometrics, but this type of legislation tends to be narrow in scope, for example, notification of biometric data breach.[10]

The end result is a scattershot approach to face recognition policy and risk mitigation. The U.S. is not alone in this regard; few if any jurisdictions have fully addressed face recognition risks at a systems level. Discussions about what to do about face recognition have generally lacked discussion of the kinds of specific procedural, administrative, and other meaningful regulatory mitigations and protections for the use of face recognition that exist in abundance in other contexts, such as drug safety or chemical safety. This oversight has meant that entire areas of effective and critically important regulatory solutions have been omitted from the discussion of how to address face recognition risks. This has left policymakers either writing narrow legislation that does not address the full cycle of face recognition, or writing bans on narrow aspects of face recognition while leaving other uses completely unregulated.

This is not necessary. Well-established, mature, and highly developed models for administrative and procedural protections, oversight, and surveillance (product observation) already exist in other domains where either dangerous or controversial technologies or products are brought to market. A more effective and fulsome *solutions continuum* for face recognition systems needs to include these mature models. Adding these more mature models, a more complete and matured solution continuum for face recognition would look more like this:

- **Principles / Responsible use**
- **Regulator - approved codes of conduct** (Under GDPR auspices, or similar, ie, regulatory codes)
- **Restricted use regulations** (backed up by legislation and statutory controls)
- **Moratorium or Proposed Ban**

---

[8] 21 CFR 50.20 General requirements for informed Consent: Except as provided in ß50.23, no investigator may involve a human being as a subject in research covered by these regulations unless the investigator has obtained the legally effective informed consent of the subject or the subject's legally authorized representative. An investigator shall seek such Consent only under circumstances that provide the prospective subject or the representative sufficient opportunity to consider whether or not to participate and that minimize the possibility of coercion or undue influence. The information that is given to the subject or the representative shall be in language understandable to the subject or the representative. No informed Consent, whether oral or written, may include any exculpatory language through which the subject or the representative is made to waive or appear to waive any of the subject's rights, or releases or appears to release the investigator, the sponsor, the institution, or its agents from liability for negligence. Available at: http://www.fda.gov/RegulatoryInformation/Guidances/ucm126431.htm

[9] *Without Consent: An analysis of student directory information practices in U.S. schools, and impacts on privacy,* World Privacy Forum, April 2020. Pages 93-94. Available at: https://www.worldprivacyforum.org/2020/04/without-consent/

[10] For example, the state of California amended its data breach statute in 2019 to include biometrics. The law went into effect January 1, 2020. *California extends data breach law to biometrics, passports,* Bloomberg Law, October 12, 2019. Available at: https://news.bloomberglaw.com/privacy-and-data-security/california-extends-data-breach-law-to-passports-biometric-data

- **Ban with regular review** (Scientific and stakeholder input and review)

It is important to note that by using all of the tools in this more complete toolset, face recognition risk can be mitigated in a more systematic, data-driven, effective, and non-adversarial manner.

Regarding best practices, many of the best practice principles for biometrics are quite good.[11] Written best practice principles need granular, specific, and practical codes of conduct to help governments, vendors, businesses, schools, and others how to fully implement them and achieve daily compliance. Very few specific, formal, regulator-approved [12] codes of conduct for face recognition exist yet under the GDPR or other regulations.[13] This is a rich area for future work for Data Protection Authorities and other regulators, and an important piece of the regulatory toolset.

Regarding existing legislative models, there is not currently a large legislative history of restricted use models for face recognition that is backed up by significant procedural controls across the lifecycle and ecosystem of the technology. Some of the existing face recognition legislation of today has a strong reliance on consent, as discussed in the U.S. BIPA context. Consent is not generally utilized as a regulatory tool in strong safety regulations because it is not appropriate to the level of risk that, for example, toxic chemicals, pose. The regulatory models that are used for the level of risk that dangerous chemicals pose are built to have multiple points of contact, control, and oversight. Face recognition would benefit from a more mature system that utilizes these types of mature use restriction models, backed up by legislation.

To make progress, it will be necessary to mature the regulatory dialogue around face recognition systems and biometrics and to pull practices from existing, useful safety models into the discussion. This discussion falls into the area of Restricted Use on the solutions continuum. There is no need to reinvent the wheel — the current safety regulation models already in use could be adapted to work quite well for biometric technologies or face recognition systems. Some things to consider:

- Chemical safety regulations manage dangerous substances with administrative, procedural, and other meaningful, robust controls with clear accountability.
- Bans are included in these models, but the bans are not ad hoc or political. There are meaningful procedures to be followed that lead to a ban. These procedures are based in science, fact, meaningful regulatory oversight, and multistakeholder work. This work is non-adversarial.
- These regulatory models are in use globally.

---

[11] *Ethical principles for biometrics*, Biometric Institute, March 2019. Available at: https://www.biometricsinstitute.org/ethical-principles-for-biometrics/.

[12] We are not including self-regulatory regimes in this analysis, as the enforceability mechanisms are insufficient for face recognition systems. Regulator-approved codes of conduct are a much more formal process, and require input from a regulator, often a Data Protection Authority, and in some cases the country's governing body. For example, the Information Commissioner's Office of the UK lays their Codes of Conduct before Parliament for approval. See the ICO's The *Age Appropriate Design Code* or *Children's Code* as an exemplar. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/09/ico-s-children-s-code-will-help-protect-children-online/.

[13] Regulators can issue enforceable opinions, and can create enforceable codes of conduct with multiple stakeholders. One recent face recognition code from the UK's Information Commissioner is strong, and enforceable. See: *The use of live facial recognition technology by law enforcement in public spaces,* 31 October 2019, ICO Opinion. Available at: https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

- Africa, Asia, EU, US, India, and almost all other jurisdictions all have meaningful regulatory safety frameworks[14]
- WHO and other global multilateral institutions track these types of safety regulations closely.[15]

In mature regulatory environments, there is a place for carefully considered bans and moratoriums. We see this reflected in chemical safety regulations and in drug regulations across the globe. Some drugs, devices, and chemicals present enough risk to have been designated as banned outright.[16] Outright bans on dangerous drugs or chemicals are rare, but when they occur, safety bans are created with copious scientific data and a meaningful, fair procedure inclusive of all stakeholders. The process is deliberative and non-adversarial. The safety bans, when decided upon by all stakeholders, occur across the lifecycle and context of the drug in question, and are actively overseen by regulators, complete with ongoing compliance oversight regarding adherence to the ban. There are procedures in place that formalize how bans are sought, placed, and handled over time.

II. Discussion: Expanding face recognition solutions by drawing from administrative and procedural protections in chemical safety models

Face recognition systems have known and scientifically quantified risks. Aspects of well-understood chemical safety models could be adapted to be put in place to provide appropriate protections and mitigation procedures for those risks, including:

- Pre-market safety, quality, and other risk assessments and requirements,
- Registration of the product,
- Ongoing product documentation,
- Audit,
- Post-implementation surveillance (observation) and documentation,
- Compliance labeling,
- Safety certifications,
- Technological proof of compliance and risk mitigation, and
- Ongoing review, oversight, and multistakeholder feedback

Some use cases of face recognition may have a clear pathway where there is proven utility for people, and the clear creation of a public good. In these cases, if the existing risks can be mitigated, the specific face recognition use case can continue with mitigations in place and full and ongoing documentation of mitigation.

In some instances, certain use cases of biometrics will pose such substantial risks, that after evaluation, the use case will need substantial restrictions, and in rare cases, a moratorium or proposed ban may be necessary. In the instances where the harms and risks cannot be reduced, and biometrics do not serve a public good, then specific use cases or entire areas of use can be designated to be considered for a proposed ban.

---

[14] UN GHS list of countries, United Nations. Available at: https://www.unece.org/trans/danger/publi/ghs/implementation_e.html

[15] World Health Organization, *WHO Chemical Risk Assessment Network*. Available at: https://www.who.int/ipcs/network/en/. United Nations, GHS. Available at: https://www.unece.org/trans/danger/publi/ghs/ghs_welcome_e.html

[16] For example, in the US, three medical devices are outright banned. See: *Medical device bans*, US Food and Drug Administration, Medical Device Safety. Available at: https://www.fda.gov/medical-devices/medical-device-safety/medical-device-bans.

Procedures to create a proposed ban are also well-established in the safety arena and are thoughtful, robust, non-adversarial, and non-political.[17]

The following regulatory safety models are already in place, and have already been functioning for years. They provide multiple new approaches to apply to the issue of mitigating harms relating to the use of face recognition and other biometrics. We present the overviews of the safety models here to provide examples of the types of regulatory controls these models utilize to mitigate harms from risky chemicals.

We do not suggest that all of the regulatory controls described in the models be attempted for face recognition systems; rather, we propose that the following administrative and procedural controls be seen as a toolbox of options with a lot more power and utility than simply best practices, simple consent structures, and narrow bans.

EU Models

The EU has two significant EU-member state-wide regulations in the area of chemical safety. Both regulations offer excellent tools for mitigating harms.

REACH: REACH[18] is the European Regulation on Registration, Evaluation, Authorisation 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 to essentially every product manufactured, imported, or sold within the EU. Manufacturers and importers are required to **register all substances** produced above a set yearly volume, and:

- **Identify risks associated with the substances they produce**;
- **Demonstrate compliance in mitigating the risks** to ECHA; and
- **Establish safe use guidelines for their product** so that the use of the substance does not pose a health threat.

RoHS: Another precedent-setting regulation,[19] RoHS 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 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.

---

[17] *Medical device bans*, US Food and Drug Administration, Medical Device Safety. Available at: https://www.fda.gov/medical-devices/medical-device-safety/medical-device-bans.

[18] REACH, European Commission. Available at: https://ec.europa.eu/growth/sectors/chemicals/reach_en

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

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.

U.S. Models

The U.S. has a Federal statute, the Chemical Safety for the 21st Century Act,[20] that regulates chemical substances of concern. The statute has meaningful compliance requirements.

Chemical Safety for the 21st Century Act:

- Requires **pre-manufacture notification** for new chemical substances prior to manufacture.
- Where risks are found (**risk assessment)**, **requires testing** by manufacturers, importers, and processors.
- Sets requirements for **certification compliance**.
- **Reporting and record keeping** requirements.
- 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 After for the 21st Century Act, some states have adopted additional EU-style regulations after the European RoHS model. Specifically, California, Colorado, Illinois, Indiana, Minnesota, New Mexico, New York, Rhode Island, and Wisconsin have enacted RoHS-like e-waste regulations.

African Models

Most countries in Africa already have regulations in place that assert legally binding controls on toxic substances. Lead is one example of a toxic substance that has been regulated, and is covered 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 such regulations.

In Africa, **water safety regulations** also mirror some of the procedural protections used in chemical safety regulations, and provide regulatory models for face recognition regulation. Water safety regulations are widespread among the countries in Africa.[21]

For example, in most African countries:

- Drinking water is **monitored** for certain chemicals and biohazards
- There are specific, agreed-upon scientific **benchmarks**
- **Testing** is frequent and impartial
- There are **controls** on hazardous water

---

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

[21] *Progress on household drinking water, sanitation and hygiene*, *focus on inequalities*. UNICEF, 2000-2017. Available at: https://washdata.org/report/jmp-2019-wash-households.

In an effective regulatory regime, products that cause harms to people will be reduced or eliminated as much as is possible, and products that provide an affirmative public good are allowed. There are well-established pathways across jurisdictions that facilitate this, and these patterns of regulation can be applied effectively to face recognition systems.

India Models

National Action Plan for Chemicals: India has safety regulations in place for hazardous chemicals.[22] In the past the regulations have not been modeled after "REACH," the strong regulation the EU has utilized. In late 2019 and continuing into 2020, India has embarked on the creation a National Action Plan for Chemicals (NAPC) to move into a more REACH-like system.[23] The idea is to create a harmonized system of classification of toxic chemicals that complies with the UN's Global Harmonization Strategy regarding chemical safety. Helping this effort is India's standing committee that is responsible for chemical safety legislation, the National Coordination Committee (NCC) under the Ministry of Environment, Forest and Climate Change (MoEF&CC).[24]

The late 2019 draft National Action Plan for chemical safety for India makes the following recommendations:

- Compile a **national chemicals inventory**;
- **analyse and assess the risks** of those chemicals;
- **implement The UN Global Harmonization Strategy** (GHS) ; and
- **develop risk mitigation strategies, policies and regulations**.

The UN GHS is worth discussing in the context of the safety regulations. The idea of UN GHS is to bring a global, standardized approach to chemical safety across all jurisdictions.[25] Labeling would be the same, level or grade of risk would be 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).

III. Conclusion: Forging a new path forward

Even if more face recognition and / or biometric best practice principles were to be published, and even if the current bans on face recognition were to proliferate and become permanent, both approaches are quite limited in terms of long and even mid-term effectiveness. More is needed. Generally, meaningful controls on the whole *lifecycle* of face recognition systems, and the whole of the data and biometric *ecosystems* within which face recognition systems exist and function have will need to be fully taken into account in a regulatory approach.

The history of drug safety regulations and chemical regulations has already taught many lessons on a global scale; it would be helpful to learn from this history instead of repeating the darker aspects of it. It

---

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

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

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

[25] United Nations, GHS. Available at: https://www.unece.org/trans/danger/publi/ghs/ghs_welcome_e.html.

was only in 1962, after the FDA allowed the use of thalidomide, a drug that caused severe birth defects,[26] that modern drug safety regimes were created. "The thalidomide crisis and subsequent infant malformation epidemic provided the motivation to establish more stringent drug testing and approval procedures worldwide. In the U.S., the Food, Drug, and Cosmetic Act was amended to require new drug sponsors to demonstrate the safety and effectiveness of their products prior to receiving FDA approval."[27] Today, thalidomide is now a safety-restricted drug.[28] Also today, much better regulatory models are the norm globally in this area.

Now, it is time to create modern safety regulations for face recognition systems. Simple regulatory approaches that only address narrow aspects of face recognition systems are insufficient. Regulatory concepts designed for less complex, lower risk technologies are highly unlikely to yield a positive result when applied to complex face recognition systems. Now that the risks of face recognition systems have been well-documented and understood, it is time to get to work. Much of this work will involve stakeholders learning how to talk with each other and develop non-adversarial relationships. Another aspect of this work is ensuring that legislators have a fulsome understanding of the complexity of face recognition systems, and do not fall into the trap of regulating disparate pieces of the system using incompatible regulatory structures. And it will be crucial for governments to hear from — and listen to — their citizenry about face recognition uses.

---

[26] Katie Thomas, The story of thalidomide in the US, told through documents, New York Times, March 23, 2020. Available at: https://www.nytimes.com/2020/03/23/health/thalidomide-fda-documents.html.

[27] Sana Loue, Martha Sajatovic. Encyclopedia of Women's Health. Springer Science and Business Media, 2004.P page 644.

[28] Thalidomide, drug description and safety information. FDA. Available at: https://www.fda.gov/drugs/postmarket-drug-safety-information-patients-and-providers/thalidomide-marketed-thalomid-information