

# **OAG Written Testimony SB 16.pdf**

Uploaded by: Abrams, Hanna

Position: FAV

**BRIAN E. FROSH**  
*Attorney General*

**WILLIAM D. GRUHN**  
*Chief*

**ELIZABETH F. HARRIS**  
*Chief Deputy Attorney General*



**CAROLYN QUATTROCKI**  
*Deputy Attorney General*

**STATE OF MARYLAND**  
**OFFICE OF THE ATTORNEY GENERAL**

FACSIMILE NO.

WRITER'S DIRECT DIAL NO.

(410) 576-6566 (F)

(410) 576-7296

January 27, 2021

**TO:** The Honorable Delores G. Kelley, Chair  
Finance Committee

**FROM:** Hanna Abrams, Assistant Attorney General

**RE:** Senate Bill 16 – Biometric Identifiers and Biometric Information Privacy  
– SUPPORT

The Office of the Attorney General supports Senate Bill 16 (“SB 16”). SB 16 provides Marylanders with privacy protections for biometric data to ensure that businesses do not keep this sensitive data longer than necessary and do not sell it without consumer consent. SB 16 complements Maryland’s Personal Information Protection Act which ensures that businesses that collect personal information maintain it securely<sup>1</sup> by creating timelines for the destruction of biometric data and restrictions on its transfer.

Biometric technologies measure and analyze people’s unique physical and behavioral characteristics, such as fingerprints, iris scans, voiceprints, and facial recognition. Businesses currently use this information to, among other things, verify identity, customize the consumer experience, and for security purposes. For example, the broad applications of facial recognition systems include supplanting time clocks at job sites,<sup>2</sup> replacing keys for housing units,<sup>3</sup> aiding security at stadiums,<sup>4</sup> and expediting check-in at hotels.<sup>5</sup> But it is important to recognize that biometric technology is not just used when a consumer knowingly provides the information such

---

<sup>1</sup> The Maryland Personal Information Act covers biometric data, but it simply requires companies that collect or store consumers’ personal information to: (1) reasonably protect it, and (2) notify consumers and the Attorney General’s Office if there is a data breach that exposes that information. Md. Code Ann., Com. Law §§ 14-3503; 14-3504.

<sup>2</sup> *4 Reasons to Use Time Clocks With Facial Recognition*, Buddy Punch (Jun. 19, 2018), available at <https://buddypunch.com/blog/time-clocks-facial-recognition>.

<sup>3</sup> Ginia Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?*, N.Y. Times (Mar. 28, 2019), available at <https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html>.

<sup>4</sup> Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, N.Y. Times (Mar. 13, 2018), available at <https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html>.

<sup>5</sup> *Facial recognition is coming to hotels to make check-in easier—and much creepier*, Fast Company (April 1, 2019), available at <https://www.fastcompany.com/90327875/facial-recognition-is-coming-to-hotels-to-make-check-in-easier-and-muchcreepier>.

as when they use a fingerprint or facial scan to unlock their phones. In many cases, the general public is unknowingly surveilled and targeted by facial recognition and has little control over the application of this technology.

Businesses currently have few limitations on their ability to harvest and aggregate Marylanders' biometric information, and they have no restrictions on using this data once it has been collected. SB 16 establishes reasonable limits on the use and storage of biometric data. It prohibits businesses from selling or sharing biometric data without consumer consent.<sup>6</sup> The Division understands that Senator Augustine will be offering an amendment that helps ensure that consumer consent is knowing and voluntary and we fully support the amendment. SB 16 also requires that biometric information be destroyed when it is no longer in use.<sup>7</sup> These protections are particularly important given the uniqueness of biometric identifiers. Unlike account numbers, which can be changed if compromised, biometrics are unique to an individual—you cannot change your fingerprint or iris if it gets stolen. Data thieves have already begun to target biometric data; in 2019, data thieves breached an international database and gained access to more than a million fingerprints and other sensitive data, including photographs of people and facial recognition data.<sup>8</sup>

Several other states have already enacted laws to protect consumers' biometric information, including California<sup>9</sup>, Illinois<sup>10</sup>, Texas<sup>11</sup>, and Washington.<sup>12</sup> SB 16 does not go nearly as far as any of those laws. All it asks is that companies that use biometric identifiers discard them when they are no longer in use and that they not profit from this unique information without consumer consent.

The Office of the Attorney General urges a favorable report.

Cc: Members, Finance Committee  
The Honorable Malcolm Augustine

---

<sup>6</sup> Section 14-4303(a)

<sup>7</sup> Section 14-4302(a).

<sup>8</sup> Scott Ikeda, *Breach of Biometrics Database Exposes 28 Million Records Containing Fingerprint and Facial Recognition Data*, CPO Magazine (Aug. 27, 2019), available at <https://www.cpomagazine.com/cyber-security/breach-of-biometrics-database-exposes-28-million-records-containing-fingerprint-and-facial-recognition-data/>.

<sup>9</sup> Cal. Civ. Code § 1798.100 *et seq.*

<sup>10</sup> 740 ILCS 14.

<sup>11</sup> Tex. Bus. & Com. § 503.001.

<sup>12</sup> Wash. Rev. Code § 19.35.

# **amendment 16.pdf**

Uploaded by: Augustine , Malcom

Position: FAV



**SB0016/133621/1**

AMENDMENTS  
PREPARED  
BY THE  
DEPT. OF LEGISLATIVE  
SERVICES

22 JAN 21  
10:24:18

BY: Senator Augustine  
(To be offered in the Finance Committee)

AMENDMENT TO SENATE BILL 16  
(First Reading File Bill)

On page 5, in line 15, strike “**THE**” and substitute “**EACH**”.

# **Hu Biometrics HB218 SB16 Testimony (1.25.21).pdf**

Uploaded by: Hu, Margaret

Position: FAV

Testimony in Support of HB 218/SB 16

“Commercial Law – Consumer Protection – Biometric Identifiers and Biometric Information Privacy”

January 25, 2021

Margaret Hu, Professor of Law and International Affairs, Penn State Law and School of International Affairs, Institute for Computational and Data Sciences, The Pennsylvania State University-University Park

Professor Hu has written multiple works on biometric surveillance, including: *Biometric ID Cybersurveillance* (2013); *Biometric Cyberintelligence and the Posse Comitatus Act* (2016); and *Algorithmic Jim Crow* (2017)

**Failing to regulate biometric data is dangerous.**

- Biometric data – fingerprints, iris scans, digital photos for facial recognition technology, DNA database screening, keystroke analysis, voice and gait analysis, and other identifiers - can be easily stolen and hacked if privacy and security requirements are not imposed under the law.
- A private right of action incentivizes preemptive security, including deletion of biometric data in a timely manner and storing biometric data with responsible cybersecurity measures.
- Corporations often suggest biometric data collection is necessary for consumer analysis, cybersecurity, authentication, software applications, training and assessment, research and development, client identification, etc.
- Governmental entities, especially law enforcement, are increasingly seeking and utilizing corporate biometric data in order to conduct criminal and national security assessments.
- Because biometric data collection methods, biometric databases, biometric data algorithms used for identification and security are not regulated, they can be inaccurate or use outdated technology.
- Algorithms/AI used to analyze biometric data has been found to have a disparate impact and result in discriminatory results (e.g., higher false positives for certain minority communities).

**Biometric data poses unique data privacy risks.**

- Biometric data is particularly sensitive in that it relies upon identification markers of the human body in order to serve various objectives, such as identity verification (are you who you say you are?); identity determination (who are you?); and identity inference (are you a risk?).
- Biometric data, in addition to being particularly sensitive, is also ubiquitous and difficult to safeguard for data privacy and data protection purposes (digital images of one’s face can be captured publicly and over the internet through the posting of digital images by others).
- In addition, the ability to integrate biometric databases with public and private databases allows for an aggregation of highly personal data. The predictive analytics capacity made possible through AI increases exponentially as the data that is analyzed becomes more personalized and linked to individuals’ identities.

**Biometric data anchors the expansion of cybersurveillance.**

- Biometric data surveillance should be understood as the embrace of a dramatic expansion of mass surveillance in both the private and public sectors.
- Newly developed big data cybersurveillance tools fuse biometric data with biographic data and internet and social media profiling.

- Biometric data collection and analysis technologies should be considered within a broader context of cybersurveillance capacities and dataveillance trends in governance norms and by private corporations in the digital economy.

**Biometric data is susceptible to abuse and misuse.**

- “Identity management” is often defined as a method for granting, restricting, or denying access and privileges on the basis of one’s identity.
- The intersection between biometric data and identity management is critical to understanding how biometric data can facilitate identity theft, appropriation/misappropriation of identity through impersonating/spoofing digital identity, and other cybercrimes.
- Technological innovation is embracing biometric data as the gold standard for identity management, at the same time, there is a failure of law and regulation to properly safeguard this valuable and sensitive information.
- The rapid expansion of identity management opens the possibility for the misuse and abuse of biometric data if the collection, retention, and use of biometric data is not closely regulated.
- Once biometric databases are breached, biometric data cannot be reissued (e.g., can reissue a new password if a password is compromised, however, cannot reissue new fingerprints, DNA, etc. if biometric databases are hacked and biometric security systems are breached).



# **EPIC-MD-BiometricPrivacy-Jan2021.pdf**

Uploaded by: Scott, Jeramie

Position: FAV

January 25, 2021

The Honorable Dereck E. Davis, Chair  
House Economic Matters Committee  
Maryland General Assembly  
Room 231  
House Office Building  
Annapolis, MD 21401

The Honorable Dolores G. Kelley, Chair  
Senate Finance Committee  
Maryland General Assembly  
3 East  
Miller Senate Office Building  
Annapolis, MD 21401

Dear Chair Davis, Chair Kelley, and Members of the Committees:

EPIC writes in support of House Bill 218 and Senate Bill 16 regarding biometric identifiers and biometric information privacy. Biometric data is highly sensitive. A person's biometric data is linked to that person's dignity, autonomy, and identity.<sup>1</sup> Unlike a password or account number, a person's biometrics cannot be changed if they are compromised. HB218 and SB16 would protect Marylanders by requiring that the use and retention of biometric data is minimized and that data is kept secure.

The Electronic Privacy Information Center (EPIC) is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.<sup>2</sup> EPIC has long advocated for strict limits on the collection and use of biometric data.<sup>3</sup>

HB218 and SB16 are modeled after the Illinois Biometric Information Privacy Act (BIPA).<sup>4</sup> Passed in 2008, BIPA has been referred to as one of the most effective and important privacy laws in America.<sup>5</sup> BIPA, and HB218 and SB16, set out a simple privacy framework: businesses may not sell, lease, trade, or otherwise profit from a person's biometric information; businesses must comply with specific retention and deletion guidelines; and companies must use a reasonable standard of care in transmitting, storing, and protecting biometric information that is as protective or more protective than the company uses for other confidential and sensitive information.

<sup>1</sup> Woodrow Hartzog, Facial Recognition Is the Perfect Tool for Oppression, MEDIUM (Aug. 2, 2018), <https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66>.

<sup>2</sup> EPIC, *About EPIC*, <https://epic.org/epic/about.html>.

<sup>3</sup> See e.g. Brief for EPIC as Amici Curiae, *Patel v. Facebook.*, 932 F.3d 1264 (9th Cir. 2019), <https://epic.org/amicus/bipa/patel-v-facebook/>;

Brief for EPIC as Amici Curiae, *Rosenbach v. Six Flags Entm't Corp.*, 2017 Ill. App. 2d 170317 (Ill. 2019), <https://epic.org/amicus/bipa/rosenbach/>; Comments of EPIC to the Dept. of Homeland Security, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 F.R. 56338, 4 (Oct. 13, 2020), <https://epic.org/apa/comments/EPIC-DHS-BiometricNPRM-Oct2020.pdf>.

<sup>4</sup> 740 Ill. Comp. State. Ann. 14/15.

<sup>5</sup> Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI NOW INSTITUTE (2020), <https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf>;

BIPA also includes a requirement that a business obtains informed, written consent before collecting or otherwise obtaining a person’s biometric information.<sup>6</sup> This provision was included in the version of this bill passed by the Maryland House last session,<sup>7</sup> but was removed from HB218 and SB16. EPIC urges the Committees to restore the informed, written consent requirement in these bills. Though “notice-and-choice” regimes are not sufficient to protect privacy, the consent provision has proven to be effective in Illinois because it is easy to enforce. It is much easier for an individual to discover and prove that a company collected their biometric data without the requisite consent than it is to prove a violation of the retention and deletion rules that are implemented by businesses after the data is collected.

The inclusion of a private right of action in HB218 and SB16 is the most important tool the Legislature can give to Marylanders to protect their privacy. Modeled after BIPA’s private right of action, the bills would impose enforceable legal obligations on companies that choose to collect and store individuals’ biometric data. As EPIC Advisory Board member Professor Woody Hartzog recently wrote:

So far, only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses. Regulators are more predictable than plaintiffs and are vulnerable to political pressure. Facebook’s share price actually rose 2 percent after the FTC announced its historic \$5 billion fine for the social media company’s privacy lapses in the Cambridge Analytica debacle. Meanwhile, Clearview AI specifically cited BIPA as the reason it is no longer pursuing non-government contracts. On top of that, Clearview AI is being sued by the ACLU for violating BIPA by creating faceprints of people without their consent. [...] In general, businesses have opposed private causes of action more than other proposed privacy rules, short of an outright ban.<sup>8</sup>

We encourage the Committee to read Professor Hartzog’s case study in its entirety and have attached it to our testimony.

Many privacy laws include a private right of action to empower individuals and have made it possible to hold accountable those who fail to protect or respect personal data. In crafting liability provisions in privacy statutes, legislatures have frequently included a liquidated damages provision to avoid protracted disputes over quantifying privacy damages. This is necessary because it is often difficult to assign a specific economic value to the harm caused by a privacy violation.

For example, when federal legislators passed the Cable Communications Policy Act in 1984, they established privacy rights for cable subscribers and created a private right of action for recovery of actual damages not less than liquidated damages of \$100 per for violation or \$1,000, whichever is higher.<sup>9</sup> The Video Privacy Protection Act specifies liquidated damages of \$2,500.<sup>10</sup> The Fair Credit Reporting Act affords individuals a private right of action that can be pursued in federal or state

---

<sup>6</sup> 740 Ill. Comp. Stat. Ann. 14/15.

<sup>7</sup> MD House Bill 307 (2020).

<sup>8</sup> Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, *supra* note 5.

<sup>9</sup> 47 USC § 551(f).

<sup>10</sup> 18 USC § 2710(c)(2).

court against credit reporting agencies, users of credit reports, and furnishers.<sup>11</sup> In certain circumstances, individuals can also recover attorney's fees, court costs, and punitive damages. The Drivers Privacy Protection Act similarly includes a private right of action.<sup>12</sup> The Telephone Consumer Protection Act allows individuals who receive unsolicited telemarketing calls to recover actual monetary loss or up to \$500 in damages per violation.<sup>13</sup>

The statutory damages set in privacy laws are not exorbitant; they are necessary to ensure that privacy rights will be taken seriously and violations not ignored. In the absence of a private right of action, there is a very real risk that companies will not comply with the law because they think it is unlikely that they would get caught or fined. Private enforcement ensures that data collectors have strong financial incentives to meet their data protection obligations. EPIC strongly supports the private right of action provisions in HB218 and SB16.

### **Conclusion**

An individual's ability to control access to his or her identity, including determining when to reveal it, is an essential aspect of personal security and privacy. The unregulated collection and use of biometrics threatens that right to privacy and puts individuals' identities at risk. We urge the Committees to restore the informed, written consent requirement and give HB218 and SB16 a favorable report.

If EPIC can be of any assistance to the Committees, please contact EPIC Policy Director Caitriona Fitzgerald at [fitzgerald@epic.org](mailto:fitzgerald@epic.org).

Sincerely,

/s/ Alan Butler  
Alan Butler  
EPIC Interim Executive Director  
and General Counsel

/s/ Caitriona Fitzgerald  
Caitriona Fitzgerald  
EPIC Interim Associate Director and  
Policy Director

/s/ Jeramie Scott  
Jeramie Scott  
EPIC Senior Counsel

Attachment: Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020).

---

<sup>11</sup> 15 U.S.C. §§ 1681n-1681o.

<sup>12</sup> 18 U.S.C. § 2724.

<sup>13</sup> 47 USC § 227(c)(5).

# BIPA: The Most Important Biometric Privacy Law in the US?

Woodrow Hartzog (Northeastern University)

In May 2020, Clearview AI abruptly ended all service contracts with all non-law enforcement entities based in Illinois.<sup>1</sup> The reason? It hoped to avoid an injunction and potentially large damages under one of the most important privacy laws in America: the Illinois Biometric Information Privacy Act (BIPA).<sup>2</sup>

Enacted in 2008 in the wake of the bankruptcy of a high-profile fingerprint-scan system, lawmakers designed BIPA to provide “safeguards and procedures relating to the retention, collection, disclosure, and destruction of biometric data.”<sup>3</sup> It was the first state law in the US to specifically regulate biometrics. Remarkably, as the bill was being deliberated by the Illinois legislature, “there were no questions or discussion, and the bill proceeded immediately to a vote and unanimously passed in the House.”<sup>4</sup>

BIPA’s substantive rules follow a traditional approach to data protection. Compared to omnibus and complex data-protection laws like GDPR, BIPA’s rules are simple. Private entities must get

---

1 Clearview AI scraped billions of images of people without their permission from social media websites to power their facial recognition app. Clearview filed legal documents in Illinois stating that “Clearview is cancelling the accounts of every customer who was not either associated with law enforcement or some other federal, state, or local government department, office, or agency.” See Ryan Mac, Caroline Haskins, and Logan McDonald, “Clearview AI Has Promised to Cancel All Relationships with Private Companies,” *BuzzFeed*, May 7, 2020, <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies>.

2 740 Ill. Comp. Stat. Ann. 14/15.

3 Charles N. Insler, How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act, 43 S. Ill. U. L.J. 819, 820 (2019).

4 Anna L. Metzger, The Litigation Rollercoaster of BIPA: A Comment on the Protection of Individuals from Violations of Biometric Information Privacy, 50 Loy. U. Chi. L.J. 1051, 1063 (2019).

informed consent before collecting or disseminating a person's biometric information.<sup>5</sup> They are prohibited from selling, leasing, trading, or otherwise profiting from a person's biometric information.<sup>6</sup> Companies must also follow specific retention and destruction guidelines.<sup>7</sup> Finally, the statute binds private entities to a standard of care in transmitting, storing, and protecting biometric information that is equal to or more protective than for other confidential and sensitive information.<sup>8</sup>

While other states such as Texas and Washington have passed standalone biometrics laws,<sup>9</sup> BIPA is the only biometric privacy law in the United States with a private cause of action. Multiple states require notice and consent before parties can collect biometric identifiers, require reasonable security measures for covered information, restrict the disclosure of biometric identifiers to specific circumstances, and limit companies' retention of biometric identifiers. But only in Illinois can people who have been aggrieved by companies that violated the rules bring their own action against the alleged violation instead of waiting for the government to file a complaint or levy a penalty.

Given the limited scope of biometric laws, BIPA's private cause of action might not seem monumental—yet it is revelatory in how it has distinguished itself from other biometrics laws. For example, Texas and Washington both authorize their state attorneys general to enforce their biometric privacy laws in ways similar to how states enforce their general data-privacy rules.<sup>10</sup> In contrast, BIPA's private cause of action has meaningfully shaped the practices of companies who deploy biometrics. It has also forced judges to resolve longstanding issues of injury and standing for privacy violations, among the most vexing issues for all privacy-related claims by plaintiffs in civil courts.

Plaintiffs alleging privacy-related harms from things like data breaches, abusive surveillance, and unauthorized disclosure have had a notoriously difficult time in court. Some of this is attributable to the general erosion of access to the American court system through tort reform. Plaintiffs struggle to certify classes for mass litigation, and arbitration clauses are embedded in the ubiquitous terms-of-use agreements online. But a huge roadblock for plaintiffs is the slippery nature of privacy harms.<sup>11</sup> Courts have long been skeptical of emotional and reputational

5 740 Ill. Comp. Stat. Ann. 14/15 (“§15(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it [informs the subject what is being collected and receives a written release]... §15(c) (d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless [the subject of the biometric identifier or biometric information consents or disclosure is required pursuant to a valid warrant or subpoena].”

6 Id. § 15(c).

7 Id. § 15(a). (“A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.”).

8 Id. § 15(e).

9 Tex. Bus. & Com. Code §503.001; Wash. Rev. Code Ann. §19.375.020; California Consumer Privacy Act (CCPA); N.Y. 2019 Stop Hacks and Improve Electronic Data Security (SHIELD) Act (broadening information covered by data breach response law to include biometric information); N.Y. Lab. Law §201-a (prohibiting fingerprinting as a condition of employment); Arkansas Code §4-110-103(7) (amending data breach response law to include biometric information).

10 For more information on the role of state attorneys general in privacy policymaking, see Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 *Notre Dame L. Rev.* 747, 748 (2016).

11 M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 *IND. L.J.* 1131, 1133 (2011); Daniel Solove and Danielle Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 *Texas Law Review* 737 (2018); Ryan Calo, *Privacy Harm Exceptionalism*, 12 *J. TELECOMM. & HIGH TECH. L.* 361, 361, 364 (2014); Paul Ohm, *Sensitive Information*, 88 *S. CAL. L. REV.* 1125, 1196 (2015).

damages absent a more obvious physical or financial harm.<sup>12</sup> The Federal Trade Commission, the premier privacy regulator in the US, creates waves when it even hints at the idea that something more than physical or financial harm or extreme emotional suffering should be considered in determining whether particular acts are unfair.<sup>13</sup> This is to say nothing of the high-stakes debate over whether less specific harms such as anxiety and exposure to risk of data abuses, standing alone, can constitute an actionable injury in the context of claims of negligence which led to a data breach.<sup>14</sup>

But most discrete and individual privacy encroachments are not catastrophic. The modern privacy predicament is more akin to death by a thousand cuts. Small intrusions and indiscreet disclosures could lead to compromised autonomy, obscurity, and trust in relationships. What's more, it can be difficult to specifically articulate and identify the ways in which data breaches make us more vulnerable. Torts require a clear line of causation from fault to harm. That's usually relatively easy to prove with things like physical injuries from car wrecks, though it is less so with data breaches. Even if it's clear that a malicious actor has gained access to peoples' information, criminals don't always straightforwardly use data obtained from a breach to inflict direct financial or emotional injury upon the data subject. They often aggregate the information in a pool for further exploitation or sit on it for years so as not to arouse suspicion. Often people have no idea who wronged them online. American data-privacy law simply isn't built to respond to this kind of diffuse and incremental harm.<sup>15</sup>

BIPA has spurred a key intervention into this morass. Specifically, with BIPA, several judicial opinions have affirmed the argument that regardless of whether wrongful acts with biometric information resulted in chilling effects or financial or emotional injury, the collection and processing of biometric data without notice and consent is alone a cognizable injury because it is an affront to a person's dignity and autonomy. Two cases in particular demonstrate the importance of BIPA.

In *Rosenbach v. Six Flags Entm't Corp.*, a mother brought a claim on behalf of her son against Six Flags amusement park for the company's failure to give notice or obtain consent when collecting the child's fingerprints for their biometric identification system.<sup>16</sup> At issue was whether the plaintiffs alleged sufficient actual or threatened injury to have standing to bring suit. Plaintiffs did not allege financial or extreme emotional harm, but rather a harm resulting solely from the prohibited collection and processing of personal biometric data without making the required

12 Id.

13 See *F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 623 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015) ("The parties contest whether non-monetary injuries are cognizable under Section 5 of the FTC Act...Although the Court is not convinced that non-monetary harm is, as a matter of law, unsustainable under Section 5 of the FTC Act, the Court need not reach this issue...").

14 Daniel Solove and Danielle Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 *Texas Law Review* 737 (2018).

15 Daniel J. Solove and Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 *Tex. L. Rev.* 737, 762 (2018) ("Hackers may not use the personal data in the near term to steal bank accounts and take out loans. Instead, they may wait until an illness befalls a family member and then use personal data to generate medical bills in a victim's name. They may use the personal data a year later but only use some individuals' personal information for fraud.")

16 *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 8, 129 N.E.3d 1197, 1200–01 ("The complaint alleges that this was the first time Rosenbach learned that Alexander's fingerprints were used as part of defendants' season pass system. Neither Alexander, who was a minor, nor Rosenbach, his mother, were informed in writing or in any other way of the specific purpose and length of term for which his fingerprint had been collected. Neither of them signed any written release regarding taking of the fingerprint, and neither of them consented in writing 'to the collection, storage, use sale, lease, dissemination, disclosure, redisclosure, or trade of, or for [defendants] to otherwise profit from, Alexander's thumbprint or associated biometric identifiers or information.'").

disclosures or obtaining written consent. The Appellate Court of Illinois held that “a plaintiff is not ‘aggrieved’ within the meaning of the Act and may not pursue either damages or injunctive relief under the Act based solely on a defendant’s violation of the statute. Additional injury or adverse effect must be alleged.”<sup>17</sup> However, the Supreme Court of Illinois disagreed.

Chief Justice Lloyd A. Karmeier, writing the opinion of the court, noted that if the Illinois legislature had wanted to impose an injury requirement beyond disclosure and consent failures, they likely would have done so, as they have in other legislation.<sup>18</sup> Using accepted principles of statutory construction, the court interpreted BIPA’s language that “[a]ny person aggrieved by a violation of this Act shall have a right of action” according to its commonly understood legal meaning. Specifically, they found that “to be aggrieved simply ‘means having a substantial grievance; a denial of some personal or property right.’”<sup>19</sup> Justice Karmeier wrote, “A person who suffers actual damages as the result of the violation of his or her rights would meet this definition of course, but sustaining such damages is not necessary to qualify as ‘aggrieved.’”<sup>20</sup>

The court in *Rosenbach* found that Six Flags violated BIPA’s “right to privacy in and control over their biometric identifiers and biometric information.”<sup>21</sup> BIPA’s disclosure and consent requirements give shape to that right. Thus, if a company violates BIPA, then the data subject is legally “aggrieved” because their right to privacy in and control over their biometric data has been compromised.<sup>22</sup>

Perhaps the most significant passage in *Rosenbach* concerned the court’s response to the defendant’s argument that its BIPA violations were merely “technical” in nature. The court argued that such a characterization misunderstands not only what the legislature was trying to accomplish but also the unique nature of how biometrics threaten peoples’ privacy and how procedural rules mitigate that threat. “The Act vests in individuals and customers the right to control their biometric information by requiring notice before collection and giving them the power to say no by withholding consent.”<sup>23</sup> Peoples’ unique biometric identifiers, now easily wholesale collected and stored, are not like other kinds of authenticators like passwords and social security numbers because if they are compromised, they cannot be changed. Even beyond identity theft, the court noted that biometrics are particularly concerning because their full risks are not known. The court was direct in its finding:

17 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 15, 129 N.E.3d 1197, 1202 (citing *Rosenbach v. Six Flags Entm’t Corp.*, 2017 IL App (2d) 170317, rev’d, 2019 IL 123186, 129 N.E.3d 1197).

18 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 25, 129 N.E.3d 1197, 1204. (“Defendants read the Act as evincing an intention by the legislature to limit a plaintiff’s right to bring a cause of action to circumstances where he or she has sustained some actual damage, beyond violation of the rights conferred by the statute, as the result of the defendant’s conduct. This construction is untenable. When the General Assembly has wanted to impose such a requirement in other situations, it has made that intention clear.”).

19 *Id.* (citing *Glos v. People*, 259 Ill. 332, 340, 102 N.E. 763 (1913)).

20 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 30, 129 N.E.3d 1197, 1205 (“Rather, [a] person is prejudiced or aggrieved, in the legal sense, when a legal right is invaded by the act complained of or his pecuniary interest is directly affected by the decree or judgment.”) (citing *Glos v. People*, 259 Ill. 332, 340, 102 N.E. 763 (1913)).

21 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 33, 129 N.E.3d 1197, 1206.

22 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 33, 129 N.E.3d 1197, 1206 (“No additional consequences need be pleaded or proved. The violation, in itself, is sufficient to support the individual’s or customer’s statutory cause of action.”).

23 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 34, 129 N.E.3d 1197, 1206.



When a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, “the right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.”...This is no mere “technicality.” The injury is real and significant.<sup>24</sup>

The court also highlighted how integral a private cause of action was in implementing the legislature’s privacy goals for BIPA. When companies face liability for legal violations without burdening plaintiffs to show some additional injury, “those entities have the strongest possible incentive to conform to the law and prevent problems before they occur and cannot be undone.”<sup>25</sup> The court noted that the cost of complying with BIPA is “likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded; and the public welfare, security, and safety will be advanced.”<sup>26</sup> According to the court, to force plaintiffs to wait until they could prove some sort of financial or emotional harm would counteract BIPA’s prevention and deterrence goals.

The other case illustrative of BIPA’s potency, *Patel v. Facebook*,<sup>27</sup> involves federal standing doctrine as required by Article III of the US Constitution, a concept linked to injury and harm thresholds. Standing doctrine requires that plaintiffs “must have suffered an ‘injury in fact’—an invasion of a legally protected interest which is (a) concrete and particularized; and (b) actual or imminent, not conjectural or hypothetical.”<sup>28</sup> In a landmark 2016 US Supreme Court case, *Spokeo, Inc. v. Robins* affirmed that an injury-in-fact for information-related complaints like those against data brokers for mishandling, inaccuracies, and indiscretion must be “concrete,” though the court was frustratingly vague about what kinds of harms met that threshold.<sup>29</sup>

*Patel v. Facebook* involved a complaint that Facebook violated BIPA with its use of facial recognition tools. The Ninth Circuit applied a two-part test to determine “(1) whether the statutory provisions at issue were established to protect [the plaintiff’s] concrete interests (as opposed to purely procedural rights), and if so, (2) whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests.”<sup>30</sup> The Ninth Circuit answered yes to both questions.

In determining that BIPA protected a concrete interest rather than a purely procedural protection, the Ninth Circuit noted that privacy rights have long served as the basis for legal action in the common law, constitutional law, and in statutes at both the state and federal level. The court noted the significant vulnerabilities created by facial recognition technology:

24 *Id.*

25 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 37, 129 N.E.3d 1197, 1206.

26 *Id.*

27 *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019), cert. denied, 140 S. Ct. 937, 205 L. Ed. 2d 524 (2020).

28 *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992).

29 *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548–49, 194 L. Ed. 2d 635 (2016), as revised (May 24, 2016). (“When we have used the adjective ‘concrete,’ we have meant to convey the usual meaning of the term—‘real,’ and not ‘abstract.’...Concreteness, therefore, is quite different from particularization. ‘Concrete’ is not, however, necessarily synonymous with ‘tangible.’ Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.”) The Court went on to muddy the waters in *Spokeo* even further, writing, “Article III standing requires a concrete injury even in the context of a statutory violation. For that reason, [Plaintiff] could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III...This does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness.” *Id.* at 1549.

30 *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1270–71 (9th Cir. 2019), cert. denied, 140 S. Ct. 937, 205 L. Ed. 2d 524 (2020) (citing *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1113 (9th Cir. 2017) (*Spokeo II*)).

[T]he facial-recognition technology at issue here can obtain information that is “detailed, encyclopedic, and effortlessly compiled,” which would be almost impossible without such technology...Once a face template of an individual is created, Facebook can use it to identify that individual in any of the other hundreds of millions of photos uploaded to Facebook each day, as well as determine when the individual was present at a specific location. Facebook can also identify the individual’s Facebook friends or acquaintances who are present in the photo...[It] seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building. Or a biometric face template could be used to unlock the face recognition lock on that individual’s cell phone.<sup>31</sup>

The court concluded that “the development of a face template using facial-recognition technology without consent (as alleged here) invades an individual’s private affairs and concrete interests. Similar conduct is actionable at common law.”<sup>32</sup> The court cited the language in *Rosenbach* in holding that “the statutory provisions at issue’ in BIPA were established to protect an individual’s ‘concrete interests’ in privacy, not merely procedural rights,” and that by alleging a BIPA violation the “the plaintiffs have alleged a concrete injury-in-fact sufficient to confer Article III standing.”<sup>33</sup>

BIPA has a number of virtues. Thanks to BIPA’s private cause of action, it has become the key for holding companies that use biometric systems accountable.<sup>34</sup> In the absence of a private cause of action, enforcement of biometrics and consumer protection laws is generally left to state attorneys general (AG). While state AGs are certainly key to privacy policymaking in the US, they have limited resources and a host of issues on their plate.<sup>35</sup> Even with unlimited bandwidth, state AGs have limited legal ability and political capital to extract the kind of fines necessary to sufficiently deter companies. The same holds true for the Federal Trade Commission, which is America’s primary privacy regulator.<sup>36</sup>

So far, only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses. Regulators are more predictable than plaintiffs and are vulnerable to political pressure. Facebook’s share price actually rose 2 percent after the FTC announced its historic \$5 billion fine for the social media company’s privacy lapses in the Cambridge Analytica debacle.<sup>37</sup> Meanwhile, Clearview AI specifically cited BIPA as the reason it is no longer pursuing non-government contracts.<sup>38</sup> On top of that, Clearview AI is being sued by the ACLU for violating

31 *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019), cert. denied, 140 S. Ct. 937, 205 L. Ed. 2d 524 (2020) (citations omitted). BIPA’s focus on face templates as a creation that grants surveillance and other affordances is properly distinguished from a standard photograph, which does not provide the same affordance of serving as a beacon.

32 *Id.*

33 *Id.* at 1274.

34 Over three hundred class action lawsuits have been brought under BIPA as of June 2019. See Seyfarth Shaw, “Biometric Privacy Class Actions by the Numbers: Analyzing Illinois’ Hottest Class Action Trend,” Seyfarth, June 28, 2019, <https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/>.

35 See Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 *Notre Dame L. Rev.* 747 (2016).

36 See Daniel Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 *Columbia Law Review* 583 (2014); Woodrow Hartzog and Daniel Solove, *The Scope and Potential of FTC Data Protection*, 83 *George Washington Law Review* 2230 (2015).

37 Charlotte Jee, “Facebook Is Actually Worth More Thanks to News of the FTC’s \$5 Billion Fine,” *MIT Technology Review*, July 15, 2019, <https://www.technologyreview.com/2019/07/15/134196/facebook-is-actually-richer-thanks-to-news-of-the-ftcs-5-billion-fine/>.

38 Nick Statt, “Clearview AI to Stop Selling Controversial Facial Recognition App to Private Companies,” *Verge*, May 7, 2020, <https://www.theverge.com/2020/5/7/21251387/clearview-ai-law-enforcement-police-facial-recognition-illinois-privacy-law>.

BIPA by creating faceprints of people without their consent.<sup>39</sup> It is no wonder that the private cause of action is one of two reasons the United States does not have an omnibus federal data privacy law (the other being federal preemption of state privacy frameworks).<sup>40</sup> In general, businesses have opposed private causes of action more than other proposed privacy rules, short of an outright ban.<sup>41</sup>

Even given BIPA's virtues and remarkable effectiveness, it is probably not the best model for America's biometric privacy identity. A private cause of action is necessary, but not sufficient, to respond to the risk of biometrics. BIPA is rooted in a myopic and atomistic "notice and choice" approach to privacy.

There are two major problems with building a biometric privacy framework almost exclusively around concepts of transparency and informational self-determination. First, by focusing on giving people control over their data and mandating procedural disclosure obligations, these frameworks fail to impose substantive limits on how far companies can encroach into our lives and how deeply these systems can be entrenched. Procedural transparency and consent regimes end up serving as a justification mechanism for all kinds of encroachments without any clear backstop to how vulnerable we can be made to these systems, so long as we consent. Furthermore, BIPA fails to address the issues around privacy in public spaces or in data that already has been exposed to the public. For example, judges considering privacy claims have said repeatedly that "there can be no privacy in that which is already public."<sup>42</sup>

Privacy is about more than just informational self-determination. It is about trust, dignity, freedom from oppression, and laying the preconditions for human flourishing. But those values are not necessarily reflected in the net outcome of billions of individual decisions. Moreover, companies create structured environments that can heavily influence these discrete choices, with powerful incentives to get us to say "yes" any way they can.<sup>43</sup>

39 ACLU, American Civil Liberties Union, American Civil Liberties Union of Illinois, Chicago Alliance Against Sexual Exploitation, Sex Workers Outreach Project Chicago, Illinois State Public Interest Research Group, Inc., and Mujeres Latinas en Acción v. Clearview AI, Inc., [https://www.aclu.org/sites/default/files/field\\_document/aclu\\_v\\_clearview\\_complaint\\_final.pdf](https://www.aclu.org/sites/default/files/field_document/aclu_v_clearview_complaint_final.pdf).

40 See Makena Kelly, "Congress Is Split over Your Right to Sue Facebook," *Verge*, December 3, 2019, <https://www.theverge.com/2019/12/3/20993680/facebook-google-private-right-of-action-sue-data-malpractice-wicker-cantwell>; and Emily Birnbaum, "Lawmakers Jump-Start Talks on Privacy Bill," *The Hill*, August 7, 2019, <https://thehill.com/policy/technology/456459-lawmakers-jump-start-talks-on-privacy-bill>; and Ben Kochman, "Senate Privacy Hearing zeroes in on Right to Sue, Preemption," *Law360*, December 4, 2019 (paywall), <https://www.law360.com/articles/1224809/senate-privacy-hearing-zeroes-in-on-right-to-sue-preemption>; and Cameron F. Kerry, John B. Morris, Caitlin Chin, and Nicol Turner Lee, "Bridging the Gaps: A Path Forward to Federal Privacy Legislation," *Brookings*, June 3, 2020, <https://www.brookings.edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation/>.

41 See Issie Lapowsky, "New York's Privacy Bill Is Even Bolder than California's," *Wired*, June 4, 2019, <https://www.wired.com/story/new-york-privacy-act-bolder/>; DJ Pangburn, "How Big Tech Is Trying to Shape California's Landmark Privacy Law," *Fast Company*, April 25, 2019, <https://www.fastcompany.com/90338036/how-big-tech-is-trying-to-shape-californias-landmark-privacy-law>; John Hendel and Cristiano Lima, "Lawmakers Wrangle over Consumer Lawsuits as Privacy Talks Drag," *Politico*, June 5, 2019, <https://www.politico.com/story/2019/06/05/privacy-advocates-consumer-lawsuits-1478824>; and "Potentially Expanded Private Right of Action Increases Risk of Class Action Exposure under the California Consumer Privacy Act," *Dorsey*, May 1, 2019, <https://www.dorsey.com/newsresources/publications/client-alerts/2019/04/private-right-of-action-increases-risk>.

42 Woodrow Hartzog, *The Public Information Fallacy*, 98 *Boston University Law Review* 459 (2019). The FBI alleges it does not need permission to conduct surveillance using powerful technologies like cell-site simulators (often called "Stingrays"), so long as they are doing so in public places. Judges have refused to punish people for taking "upskirt" photos because the women photographed have no reasonable expectation of privacy "in public," no matter how fleeting their exposure. *Id.*

43 Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge, MA: Harvard University Press, 2018).

BIPA is simply not capable of providing individuals with meaningful agency over modern data practices.<sup>44</sup> “Informed consent” is a broken privacy regulatory mechanism.<sup>45</sup> It doesn’t scale, it offloads risk onto the person giving the consent, and it is easily manufactured by companies who control what we see and what we can click. Companies deploy malicious user interfaces and a blizzard of dense fine print to overwhelm our decision-making process. Consent regimes give the illusion of control while justifying dubious practices that people don’t have enough time or cognitive resources to understand. Even if people were able to adequately gauge the risks and benefits of consenting to biometric practices, they often don’t have a meaningful choice in front of them since they cannot afford to say no and decline a transaction or relationship. While people should be protected regardless of what they consent to, BIPA is largely agnostic to the post-permission risks of biometric technologies.

BIPA is far more effective than any other law on the books in protecting our biometric privacy with respect to private companies. However, it does not confront the structural change and substantive limits necessary for a sustainable future with biometric technologies. BIPA allows companies to exploit people as their consent is harvested through systems designed to have them hurriedly click “I Agree” and get on with their busy lives. BIPA’s success entrenches an overly individualistic and procedural approach to privacy, but has shown lawmakers what is indispensable in a biometric privacy framework. It is a guide not just because of what it provides but also because of what it lacks.

---

44 Woodrow Hartzog, *The Case Against Idealising Control*, 4 *European Data Protection Law Review* 423 (2018).

45 Neil Richards and Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 *Washington University Law Review* 1461 (2019); Evan Selinger and Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 *Loyola Law Review* 101 (2019).

# **SB16 - CGDP - Support w Amendments .pdf**

Uploaded by: McDonough, Caitlin

Position: FWA

January 27, 2021

The Honorable Delores Kelley  
Chair, Senate Finance Committee  
Miller Senate Office Building, 3 East  
11 Bladen Street  
Annapolis, MD 21401

**RE: SENATE BILL 16 – COMMERCIAL LAW – CONSUMER PROTECTION – BIOMETRIC IDENTIFIERS AND BIOMETRIC INFORMATION PRIVACY - TESTIMONY IN SUPPORT WITH AMENDMENT**

Dear Chair Kelley:

The Coalition for Genetic Data Protection (CGDP) serves to provide a unified and proactive voice to advance policies that ensure the privacy and security of an individual's genetic data and enable responsible innovation. Consumer genetic testing can empower consumers to take a proactive role in their health, wellness, ethnicity, and origin in unprecedented ways – and millions of consumers have taken advantage of these opportunities. At the same time, genetic data provides unprecedented opportunities for the research community to better understand the role genetics play in our health and well-being as a human population. While we recognize the significant opportunities genetic testing and research present, we also support and advocate for reasonable and uniform privacy regulation that will ensure the responsible and ethical handling of every person's genetic data.

Senate Bill 16, as introduced, generally requires each “private entity” in possession of “biometric identifiers” or “biometric information” to develop a publicly available written policy establishing a retention schedule and guidelines for permanently destroying the biometric identifiers and information and sets minimum standards for such policies. The legislation creates a definition of “confidential and sensitive information” that includes “A GENETIC MARKER” and “GENETIC TESTING INFORMATION”, which essentially aligns this type of genetic data with other personal information as information that can be used to uniquely identify an individual.

CGDP believes that genetic data is very different from other types of both biometric information and personal information, in that it is not used in the same manner to directly, and often immediately, identify an individual for security or other purposes. In fact, genetic data on its own, without the addition of other personal identifying information, cannot be used to directly identify an individual. Due to the unique nature of genetic data, statutes and regulation at both the state and federal level that regulate biometric data do not expressly include genetic data in that regulation. The Maryland General Assembly has several other pieces of legislation before it in the 2021 Legislative Session that address the protection and privacy of personal information and lay out specific parameters for the use and protection of genetic data. These bills define this type of data separately and differently than general biometric data, and CGDP seeks a similar application of the standards set in SB16.

The attached amendment does not alter the proposed standards for private entity use of biometric data in Maryland, other than to remove references to genetic data. In keeping with CGDP's stated mission, it is not opposed to the reasonable regulation of genetic data collected and used by private entities, but urges the Committee to pursue privacy policy that recognizes the unique nature of genetic data and how it differs from the other biometric information that is the primary focus in SB16. CGDP looks forward to working with the bill



sponsor and the members of the Committee on SB16 and other legislation before the General Assembly that specifically addresses the use of genetic data.

Sincerely,

A handwritten signature in blue ink that reads "Eric Heath".

Eric Heath  
Chief Privacy Officer  
*Ancestry*

A handwritten signature in black ink that reads "Jacquie Haggarty".

Jacquie Haggarty  
VP, Deputy General Counsel & Privacy Officer  
*23andMe*

A handwritten signature in black ink that reads "Steve Haro".

Steve Haro  
Executive Director  
*Coalition for Genetic Data Protection*

cc:

**Ext. Comm. - Letter - 2021 - Maryland SB 16 - Biom**

Uploaded by: Fisher, Joshua

Position: UNF





January 25, 2021

The Honorable Delores Kelley  
Chair, Senate Finance Committee  
3 East, Miller Senate Office Building  
Annapolis, Maryland 21401

**RE: SB 16 - Biometric Identifiers and Biometric Information Privacy  
Position: Unfavorable**

Chair Kelley:

The Alliance for Automotive Innovation<sup>1</sup> (Auto Innovators) is writing to inform you of **our opposition to SB 16**, which establishes requirements & restrictions on private entities use, collection, & maintenance of biometric identifiers & biometric information.

***Maintaining Consumer Privacy and Cybersecurity***

The protection of consumer personal information is a priority for the automotive industry. Through the development of the “Consumer Privacy Protection Principles for Vehicle Technologies and Services,” Auto Innovators’ members committed to take steps to protect the personal data generated by their vehicles. These Privacy Principles are enforceable by the Federal Trade Commission and provide heightened protection for certain types of sensitive data, including biometric data.<sup>2</sup> Consumer trust is essential to the success of vehicle technologies and services. Auto Innovators and our members understand that consumers want to know how these vehicle technologies and services can deliver benefits to them while respecting their privacy. Our members are committed to providing all their customers with a high level of protection of their personal data and maintaining their trust.

***Practical Concerns***

We have concerns about this legislation and recommend an unfavorable report from the committee. Our concerns are outlined below:

---

<sup>1</sup> Formed in 2020, the Alliance for Automotive Innovation is the singular, authoritative and respected voice of the automotive industry. Focused on creating a safe and transformative path for sustainable industry growth, the Alliance for Automotive Innovation represents the manufacturers producing nearly 99 percent of cars and light trucks sold in the U.S. The organization, a combination of the Association of Global Automakers and the Alliance of Automobile Manufacturers, is directly involved in regulatory and policy matters impacting the light-duty vehicle market across the country. Members include motor vehicle manufacturers, original equipment suppliers, technology and other automotive-related companies and trade associations. The Alliance for Automotive Innovation is headquartered in Washington, DC, with offices in Detroit, MI and Sacramento, CA. For more information, visit our website <http://www.autosinnovate.org>.

<sup>2</sup> [https://autoalliance.org/wp-content/uploads/2017/01/Consumer\\_Privacy\\_Principlesfor\\_VehicleTechnologies\\_Services.pdf](https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf)

First, privacy requirements of this nature require a standardized, nationwide approach so there is not a dizzying array of varied state requirements. Privacy protections regarding biometrics are being enforced by the Federal Trade Commission (FTC)<sup>1</sup>. The FTC has been the chief regulator for privacy and data security for decades, and its approach has been to use its authority under Section 5 of the FTC Act to encourage companies to implement strong privacy and data security practices. The auto industries “Privacy Principles” are enforceable under Section 5 of the FTC Act.

Second, the current definition of “biometric identifier” is extremely broad and could capture several important safety-related technologies that are not used or intended to be used for the unique personal identification of an individual. For example, external-facing vehicle sensors that are integral to an Advanced Driver Assistance Systems or automated driving systems may be used to recognize that an object in the path of the vehicle is a pedestrian. In addition, internal-facing cameras may be used on some lower-level automated vehicle systems to detect driver abuse or disengagement. While these “images” are not used by an auto company to identify individuals, they could theoretically be used by someone for this purpose and are therefore potentially captured by the definition of “biometric identifier.”

This issue could be remedied by modifying the definition of “biometric identifier” so that it explicitly excludes images obtained by vehicle safety technologies. It could also be remedied by striking the references to “biometric identifiers” throughout 14-4302 and 14-4303 and limiting the applicability of these provisions to “biometric information.” Since “biometric information” is defined as information that is used identify an individual (as opposed to information that can be used to identify an individual), it would presumably exclude the images captured by these vehicle safety technologies.

Third, while the requirement to have a written policy that lays out a retention schedule is conforms with the industry’s existing Privacy Principles, the requirement to destroy the information no later than three years after the company’s last interaction seems somewhat arbitrary. A requirement to provide clear disclosure to consumers about how long such information will be maintained should be sufficient. Moreover, in practice, this requirement may prove challenging because, in the automotive case, manufacturers do not generally have visibility into who is driving or using a particular vehicle at a particular time and using vehicle technologies that may utilize biometric technology. In addition, manufacturers may not always know when a vehicle has been sold to another owner.

Fourth, the bill creates a private right of action. Businesses may very well find themselves in a position of facing severe penalties for even very minor and inadvertent infractions and where there are no actual damages.

Thank you for your consideration of the Auto Innovators’ position. Please do not hesitate to contact me at [jfisher@autosinnovate.org](mailto:jfisher@autosinnovate.org) or 202-326-5562, should I be able to provide any additional information.

Sincerely,

A handwritten signature in black ink that reads "Joel Fisher". The signature is written in a cursive style with a large, stylized initial "J".

Josh Fisher  
Director, State Affairs

---

<sup>i</sup> <https://www.ftc.gov/news-events/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers>



# **SB 16\_Consumer\_Protection - Biometric\_Identifiers\_**

Uploaded by: Griffin, Andrew

Position: UNF



**LEGISLATIVE POSITION:**

**UNFAVORABLE**

**Senate Bill 16**

**Commercial Law – Consumer Protection –  
Biometric Identifiers and Biometric Information Privacy  
Senate Finance Committee**

**Wednesday, January 27, 2021**

Dear Chairwoman Kelley and Members of the Committee:

Founded in 1968, the Maryland Chamber of Commerce is the leading voice for business in Maryland. We are a statewide coalition of more than 5,000 members and federated partners, and we work to develop and promote strong public policy that ensures sustained economic recovery and growth for Maryland businesses, employees, and families.

Maryland Chamber of Commerce members place a high priority on consumer privacy, however, as drafted, SB 16 would create significant hardships for Maryland employers and could result in stifling important advances in safety and security.

Chamber members believe that privacy laws should provide strong safeguards for consumers, while allowing the industry to continue to innovate. SB 16 adopts language from an Illinois law passed in 2008 and does not account for over a decade of innovation in technology and business practices. It does not identify and protect against specific privacy harms, instead utilizing a definition of “Biometric identifier” that is overbroad and difficult to implement.

In addition to significant compliance costs, this legislation would further burden local businesses with the threat of frivolous class action litigation. As has been shown in Illinois, the threat of liability will prevent Maryland companies from developing or utilizing pro-consumer, pro-privacy uses of biometric data like building security, user authentication, and fraud prevention.

Maryland residents and employers deserve privacy protections that safeguard sensitive data while promoting innovation and job creation. The Maryland Chamber of Commerce urges the bill sponsor to work alongside industry partners in addressing the issue surrounding the safety and security of personal data.

For these reasons, the Maryland Chamber of Commerce respectfully requests an **unfavorable report** on **SB 16**.

**SIA Letter of Concerns\_MD SB 16.pdf**

Uploaded by: Jamali, Drake

Position: UNF



January 27, 2020

Chair, Senator Delores Kelley  
3 East  
Miller Senate Office Building  
Annapolis, Maryland 21401

Dear Chairwoman Kelley and members of the committee:

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with MD SB 16, which establishes requirements & restrictions on private entities use, collection, & maintenance of biometric identifiers & biometric information, while creating a private cause of action for relief on violations of the act.

The Security Industry Association (SIA), which is based in Silver Spring, is a nonprofit trade association representing businesses that provide a broad range of security products for government, commercial and residential users in the U.S., including businesses headquartered in Maryland and many more with employees and significant business operations in the state. Our members include many of the leading manufacturers of biometric technologies, as well as those who are integrating these technologies into a wide variety of building security and life-safety systems.

At the outset, I want to stress that our members intend their technology products only be used for purposes that are lawful, ethical and non-discriminatory. While we generally support the data policies outlined in S.B. 16 as good practice, careful consideration should be given to whether biometric information should be singled out for regulation separate from other personal data it is often associated with, including biographic information like date of birth, physical characteristics, Social Security number, address, employment, health and education history – the type of information that so far has proven to be more vulnerable to compromise and misuse.

Biometric authentication enhances identity protections while increasing the effectiveness of security systems developed by our industry. Many sectors of the business community stand to benefit from technologically advanced equipment that utilizes biometric identifiers for security purposes, such as authentication, for employee access to buildings or computer networks, and security systems that protect buildings, their occupants and the assets contained therein.

At a minimum, an exemption to a notification and consent requirement for safety and security uses is essential. A good example is the security provision included in Washington State's current biometric data law enacted in 2017. This law generally requires notice and consent of an individual before their biometric information is enrolled in a database for commercial use, but provides an express exception where the collection, capture or enrollment and storage of a biometric identifier is in furtherance of a security purpose (RCW 19.375.020, §7). Such an exemption is necessary, because requiring written

consent would be unworkable for building systems intended for safety or security applications, as an individual with malicious intent would likely not consent to having their information captured.

An increasingly important benefit of biometric data is that it gives employers the ability to alert staff and other building occupants of immediate threats to the safety of a building's occupants, such as where a disgruntled former employee attempts to enter the workplace. Requiring consent or automatic deletion of data after employment would run contrary to ensuring public safety in this case.

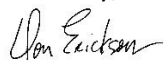
Additionally, a consent requirement makes participation optional, thus limiting the ability to effectively deploy safety and security systems that utilize biometric technologies throughout a building, due to the presence of a mixed population of consenting and non-consenting individuals. Without an exception, a consent requirement would essentially preclude using these technologies for the enhancement of access control, intrusion detection, anti-theft, fire alarm, active shooter and other safety and security purposes throughout a building.

The private right of action in the bill should be replaced with enforcement by the attorney general. This mechanism would preserve the protective intent without the potential catastrophic consequences for businesses subjected to unwarranted lawsuits. This is the approach Washington and Texas have taken with their biometrics laws.

In conclusion, due to the wide-ranging negative consequences for Marylanders and Maryland businesses from implementing a Biometric Information Privacy Act (BIPA)-type approach to regulating use of biometric data, we urge the Committee not to advance S.B. 16 in its current form. Instead, we ask that the issue be thoroughly and thoughtfully studied before any legislation or regulations restricting its use are passed.

SIA and our members welcome the opportunity to work with you to identify the best ways to achieve the objective of safeguarding biometric and other personal data, ensuring it is captured, stored and utilized in a responsible manner than benefits Maryland's citizens.

Sincerely,



Don Erickson

Chief Executive Officer

Security Industry Association

Staff contact: Drake Jamali, [djamali@securirtyindustry.org](mailto:djamali@securirtyindustry.org)



# **SB0016\_UNF\_MTC\_Consumer Protection - Biometric Ide**

Uploaded by: Rosendale, Martin

Position: UNF



# MARYLAND TECH COUNCIL

TO: The Honorable Delores G. Kelley, Chair  
Members, Senate Finance Committee  
The Honorable Malcolm Augustine

FROM: Pamela Metz Kasemeyer  
J. Steven Wise  
Danna L. Kauffman

DATE: January 27, 2021

RE: **OPPOSE** – Senate Bill 16 – *Commercial Law – Consumer Protection – Biometric Identifiers and Biometric Information Privacy*

---

The Maryland Tech Council (MTC) is a collaborative community, actively engaged in building stronger life science and technology companies by supporting the efforts of our individual members who are saving and improving lives through innovation. We support our member companies who are driving innovation through advocacy, education, workforce development, cost savings programs, and connecting entrepreneurial minds. The valuable resources we provide to our members help them reach their full potential making Maryland a global leader in the life sciences and technology industries. On behalf of MTC, we submit this letter of **opposition** for Senate Bill 16.

MTC members place a high priority on consumer privacy, however, as drafted, the legislation would create significant hardships for Maryland employers and could actually result in stifling important advances in safety and security as well as exposing member businesses and customer data to greater degrees of fraud and cybercrime. For example, Senate Bill 16 has no exception for fraud prevention. Biometric data is used today for security, authentication, and fraud prevention purposes, such as to secure access to highly sensitive buildings, to detect fraudulent callers, and to improve security on financial accounts. Because the bill does not allow for the use of biometric data for fraud prevention, and does not even have a clear security exception, the bill would put Maryland residents at greater risk of fraud and security threats.

In addition, this legislation would leave Maryland businesses vulnerable to class action lawsuits for even minor violations. This is especially true as the bill also does not distinguish between service providers and consumer-facing entities and therefore every business is liable for failing to provide consumers with consent, even when consumers never interact directly with the product. The threat of liability will prevent Maryland companies from developing or utilizing pro-consumer, pro-privacy uses of biometric data like building security, user authentication, and fraud prevention and may dissuade startups and other companies from choosing to do business in the state. Experience with an existing Illinois law upon which these provisions seem to be based bears this out.

MTC recognizes the importance of protecting consumer information, including biometric identifiers and information, the matters that Senate Bill 16 addresses should and must be resolved on the federal level. Meaningful consistent compliance by industry would be more reliably satisfied with a uniform nationwide solution. This bill would have the effect of imposing millions of dollars of compliance costs on tech businesses and would harm the State's economy more than it would protect consumer privacy. MTC respectfully requests an unfavorable report.

**For more information call:**

Pamela Metz Kasemeyer  
J. Steven Wise  
Danna L. Kauffman  
410-244-7000

# **WPF\_ExpandingSolutions\_FaceRecognition\_03Sept2020\_**

Uploaded by: dixon, pamela

Position: INFO



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

Pam Dixon,<sup>1</sup> 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.<sup>2</sup> 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<sup>3</sup> bias in face

---

<sup>1</sup> 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.*, Springer 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](http://www.id4africa.com/2019/files/RADPA2019_Report_Blog_En.pdf).

<sup>2</sup> *The facial recognition world map*, SurfShark. Available at: <https://surfshark.com/facial-recognition-map>.

<sup>3</sup> 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](http://biometrics.cse.msu.edu/Presentations/AnilJain_UIDAI_June7_2016.pdf). Another expert 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.<sup>4</sup> Additionally, some face recognition systems have been built on unconsented data collections, which is also controversial.<sup>5</sup>

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),<sup>6</sup> 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.<sup>7</sup> 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

---

<sup>4</sup> 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>.

<sup>5</sup> 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](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 collected, or “scraped,” photos of her from MySpace, Twitter, Instagram, and other websites.

<sup>6</sup> 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.

<sup>7</sup> 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.<sup>8</sup> 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).<sup>9</sup> 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.<sup>10</sup>

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**

---

<sup>8</sup> 21 CFR 50.20 General requirements for informed Consent: Except as provided in §50.23, 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>

<sup>9</sup> *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/>

<sup>10</sup> 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.<sup>11</sup> 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<sup>12</sup> codes of conduct for face recognition exist yet under the GDPR or other regulations.<sup>13</sup> 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.

---

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

<sup>12</sup> 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/>.

<sup>13</sup> 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<sup>14</sup>
- WHO and other global multilateral institutions track these types of safety regulations closely.<sup>15</sup>

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.<sup>16</sup> 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.

---

<sup>14</sup> UN GHS list of countries, United Nations. Available at: [https://www.unece.org/trans/danger/publi/ghs/implementation\\_e.html](https://www.unece.org/trans/danger/publi/ghs/implementation_e.html)

<sup>15</sup> 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](https://www.unece.org/trans/danger/publi/ghs/ghs_welcome_e.html)

<sup>16</sup> 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.<sup>17</sup>

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<sup>18</sup> 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,<sup>19</sup> 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.

---

<sup>17</sup> *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>.

<sup>18</sup> REACH, European Commission. Available at: [https://ec.europa.eu/growth/sectors/chemicals/reach\\_en](https://ec.europa.eu/growth/sectors/chemicals/reach_en)

<sup>19</sup> 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,<sup>20</sup> 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 Safety 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.<sup>21</sup>

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

---

<sup>20</sup> *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>

<sup>21</sup> *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.<sup>22</sup> 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.<sup>23</sup> 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).<sup>24</sup>

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.<sup>25</sup> 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

---

<sup>22</sup> *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>

<sup>23</sup> *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>

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

<sup>25</sup> United Nations, GHS. Available at: [https://www.unece.org/trans/danger/publi/ghs/ghs\\_welcome\\_e.html](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,<sup>26</sup> 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.”<sup>27</sup> Today, thalidomide is now a safety-restricted drug.<sup>28</sup> 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.

---

<sup>26</sup> 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>.

<sup>27</sup> Sana Loue, Martha Sajatovic. Encyclopedia of Women’s Health. Springer Science and Business Media, 2004.P page 644.

<sup>28</sup> 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>