Northwestern Journal of Technology and Intellectual Property

Volume 23 | Issue 1 Article 5

Fall 2025

Unregulated and Unacceptable: Facial Recognition Technology's History, Privacy Concerns, and Impact on Society

Alyssa Pequignot

Follow this and additional works at: https://scholarlycommons.law.northwestern.edu/njtip

Recommended Citation
Alyssa Pequignot, *Unregulated and Unacceptable: Facial Recognition Technology's History, Privacy Concerns, and Impact on Society*, 23 NW. J. TECH. & INTELL. PROP. 249 (2025).
https://scholarlycommons.law.northwestern.edu/njtip/vol23/iss1/5

This Note is brought to you for free and open access by Northwestern Pritzker School of Law Scholarly Commons. It has been accepted for inclusion in Northwestern Journal of Technology and Intellectual Property by an authorized editor of Northwestern Pritzker School of Law Scholarly Commons.

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

UNREGULATED AND UNACCEPTABLE: FACIAL RECOGNITION TECHNOLOGY'S HISTORY, PRIVACY CONCERNS, AND IMPACT ON SOCIETY

Alyssa Pequignot

December 2025 VOL. 23, NO. 1

© 2025 by Alyssa Pequignot

Copyright 2025 by Alyssa Pequignot
Volume 23, Number 1 (2025)
Northwestern Journal of Technology and Intellectual Property

UNREGULATED AND UNACCEPTABLE: FACIAL RECOGNITION TECHNOLOGY'S HISTORY, PRIVACY CONCERNS, AND IMPACT ON SOCIETY

Alyssa Pequignot[*]

ABSTRACT—*This Note provides a general review of the current state of Facial Recognition Technology (FRT), including Illinois state regulation and past federal regulation attempts. This Note asserts that even as datasets become more diverse and "fairer," FRT may still have discriminatory impacts on minority populations, as evidenced by a few highlighted examples that focus on race and gender. This Note suggests that one option to mitigate these dangers is to implement national regulations for its use. Ultimately, this Note suggests what a federal regulation might look like, informed by the societal impacts discussion.*

After an introduction in Section I, Section II provides a brief overview of the history of FRT, how it works, and where it is used. Next, Section III dives into the Illinois Biometric Information Privacy Act (BIPA), focusing on what distinguishes it from the plaintiff's perspective and recent amendments to the Act. To expand on this discussion, Section IV discusses two case illustrations that exemplify what BIPA litigation should look like and the impact that these court holdings have had on the statute. Section V looks at the past and current federal FRT regulation, including past failed federal enactment attempts. Finally, Section VI discusses the societal impacts of FRT and the benefits of a united federal regulatory system. This Note concludes with an idealized federal regulation suggestion, grounded in BIPA and the American Data Privacy and Protection Act.

The focus of this Note is to provide a foundational understanding of FRT and ultimately provide an explanation for how the information fed into FRT models is analyzed. By looking through the lens of BIPA and homing in on the inner workings of a single state's statute, this Note focuses on a few of the current rights and regulations in place and how they are used to protect against the misappropriation of biometric data. As the Note shifts toward a discussion about the societal impacts of FRT, the focus is on the discriminatory outcomes as a main danger of FRT.

[*] J.D. Candidate, Northwestern Pritzker School of Law

The introductory information laid before the societal implications discussion helps to highlight how the impacts discussed are a direct result of FRT systems and current regulations. This Note contributes to the current discussion about potential bias in face surveillance and biometrics technology, seeking to fill gaps in the current literature by using BIPA as a lens for viewing current regulations, combined with a societal impact analysis. This Note presents an idealistic suggestion for federal regulation that would harmonize national usage and protections for FRT and biometrics in the future.

TABLE OF CONTENTS

I. INTRODUCTION

Biometric technology is a measurable biological and/or behavioral characteristic that can be used for automated recognition.[1] Biometrics use a person's physical characteristics to identify them, including but not limited to: their faceprints, fingerprints, walking patterns, iris scans, voice prints, and

[1] *Biometrics*, DEP'T OF HOMELAND SEC. (Aug. 28, 2025), https://www.dhs.gov/biometrics [https://perma.cc/RE9X-NPUA].

DNA.[2] Face printing is a "fundamental step in the process of face recognition, [it] is the automated analysis and translation of visible characteristics of a face into a unique mathematical representation of that face."[3] Put another way, face printing turns an image of a face into digital code that is read by the FRT model. A faceprint is the product of FRT. Yet, face printing is not exclusive to the current era of FRT. Automated biometric systems have been around for the past few decades, but other forms of biometric recognition have been used before.[4] For instance, the modern biometrics industry as we know it today began with fingerprints, when Sir Francis Galton created the first fingerprint classification system.[5] Seventy years later, the beginnings of today's FRT emerged.[6] Earlier systems of biometrics required human operators to detect patterns from the data provided. Today, FRT no longer requires a human operator to babysit it, but this element of human involvement is still prevalent in the technology through bias.[7] The homogeneity in initial builds of FRT has contributed to "'demographic bias' [being] built into the technology."[8]

Although FRT is only one aspect of surveillance and biometric data technology, it may be the most dangerous.[9] Today, there is heavy investment in maximizing the technology. For example, government agencies have been investing heavily in FRT and are one of the top users of surveillance.[10] With

---

[2] *Face Surveillance and Biometrics*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/surveillance-oversight/face-surveillance/ [https://perma.cc/L2W9-TXFY].

[3] Adam Schwartz et al., *Face Recognition Technology: Commonly Used Terms*, ELEC. FRONTIER FOUND. (Oct. 7, 2021), https://www.eff.org/deeplinks/2021/10/face-recognition-technology-commonly-used-terms [https://perma.cc/RF9V-U5FL].

[4] *See* Diana Bretherick, *The 'Born Criminal'? Lombroso and the Origins of Modern Criminology*, HISTORYEXTRA (Feb. 14, 2019, at 11:39 CT), https://www.historyextra.com/period/victorian/the-born-criminal-lombroso-and-the-origins-of-modern-criminology/ [https://perma.cc/2BBH-H2UT]. In the late 1800s in Italy, Cesare Lombroso used older methods of "facial recognition." Lombroso was a criminal anthropologist and is regarded as "the father of modern criminology." Lombroso believed that certain "savage" physical features indicated who was a criminal and believed that criminality was inherited. Lombroso's methods and beliefs were discriminatory in their own right, just as the beginnings of FRT datasets were inherently discriminatory.

[5] *Biometrics*, *supra* note 1.

[6] *Id.*

[7] Sidney Perkowitz, *The Bias in the Machine: Facial Recognition Technology and Racial Disparities*, MIT CASE STUD. IN SOC. & ETHICAL RESP. OF COMPUTING (Feb. 5, 2021), at 5.

[8] Sidney Perkowitz, *The Bias in the Machine*, NAUTILUS (Aug. 19, 2020), https://nautil.us/the-bias-in-the-machine-237935/ [https://perma.cc/NNG5-X548].

[9] *Face Surveillance and Biometrics*, *supra* note 2.

[10] Tonya Riley, *Feds' Spending on Facial Recognition Tech Expands, Despite Privacy Concerns*, CYBERSCOOP (Jan. 10, 2022), https://cyberscoop.com/feds-spending-on-facial-recognition-tech-continues-unmitigated-despite-privacy-concerns/#:~:text=In%20September%2C%20U.S.%20Immigration%20and,up%20to%20%241.5%20million%20dollars [https://perma.cc/A6GE-RYLR] (noting that in September 2022, U.S. Immigration and Customs Enforcement spent "almost $4 million on facial recognition technology from a company called

this focused investment, FRT is the key to unlocking mass surveillance from the comfort of a computer screen.[11] FRT allows anyone with access to the technology and its outputs to readily identify individuals, track movements, and gather sensitive information—all without the subjects' consent. Other surveillance and biometric data tools raise concerns, but none are as pervasive in everyday life as FRT. Although modern FRT and previous iterations of the technology have been around for decades, there is a lack of understanding about how it works, how it is used, or how to regulate it. Although not every user is a bad actor, there are some who are left to their own devices to decide how, when, where, and for what to use FRT. The current lack of federal regulations leaves FRT users open to use without much oversight.

Surveillance and biometric data technology is at the forefront of many industries, including the U.S. government, law enforcement,[12] and the private sector. Artificial intelligence (AI) and "big data" analytics continue to drive innovation in surveillance technology.[13] FRT brings many concerns for society, including serious privacy and discrimination issues stemming from its usage. These concerns will continue to persist or intensify unless federal regulations are implemented to put guardrails around the technology.

The lack of uniformity in protections for biometric data, coupled with the growing use of FRT, has exacerbated FRT's looming threat to minority populations. Uniformity would create a federal foundation of protections, raising the bar for states currently without any regulation or consumer protections in place. The gravity of the lack of protections necessitates federal intervention, specifically to protect those most vulnerable to the negative consequences of unregulated usage. A principal concern is that certain FRT models have been shown to have racial bias ingrained in them, either because of the homogeneity of their data sets[14] or the locations in which the technology is prominently used.[15] Additional concerns stem from the sheer amount of data collected for FRT models, including sensitive personal information.

Trust Stamp . . . . The same month [the] agency purchased a contract with Clearview AI starting at $500,000 with the potential to go up to $1.5 million dollars.").

[11] *Id.*

[12] Kelley M. Sayler, *Biometric Technologies and Global Security,* CONG. RSCH. SERV. (Aug. 22, 2024).

[13] *Id.*

[14] Perkowitz, *supra* note 7, at 4 ("One reason for the racial disparities in the performance of facial recognition technologies is the relative lack of nonwhite faces in the sample data sets that have been used to develop the algorithms. The poor representation of people of color from around the world, and their range of facial features and skin shades, creates what researchers call a 'demographic bias' built into the technology.").

[15] Complaint at 12, FTC v. Rite Aid Corp., No. 2:23-cv-5023 (E.D. Pa. Dec. 19, 2023).

One example of the discriminatory dangers that result from minimal regulation is the story of Mr. Robert Williams.[16] Mr. Williams was wrongfully arrested due to the inaccuracy of the FRT model used by the Detroit Police Department. In the settlement agreement that arose from this traumatic event, the Detroit Police Department agreed to introduce audit requirements for all cases that used FRT.[17] Mr. Williams and the American Civil Liberties Union (ACLU) saw the necessity of having policies in place to guide the use of this technology. This Note argues the same. Uniform regulations would guide entities such as the Detroit Police Department to ensure situations such as Mr. Williams's do not occur in the future. Mr. Williams's story is discussed in greater detail in Section VI.

Moreover, the overwhelming use of FRT across many industries can only intensify its potential impact on society and our daily lives. Unfortunately, the federal legislature has yet to catch up with the widespread use of FRT—evidenced by the fact that there are currently *zero* federal regulations in place to limit or supervise the usage of FRT. As of 2024, only a portion of states have taken charge and implemented state regulations for FRT. Illinois was the first state to do so, implementing the Biometric Information Privacy Act (BIPA).[18] BIPA's goal is to regulate how private entities collect, use, and share biometric information, including "retina or iris scan[s], fingerprint[s], voiceprint[s], or scan[s] of hand or face geometry."[19] Although BIPA has been regarded highly by the plaintiffs' bar, it has gaps in protections for consumers, too. Following Illinois's lead, about a dozen other states have enacted their own FRT regulations. Yet there is still much left to do to protect consumers equally across the states and to provide a foundation of protections relating to biometric information.

II. A BRIEF OVERVIEW OF FRT

A. The Beginning of FRT

Woodrow Wilson Bledsoe was one of the first to develop automated facial recognition in the 1960s. He developed a system that trained computers to recognize human faces.[20] Bledsoe was an American

---

[16] Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/Z6NV-EQZF].

[17] *See* Settlement Agreement at 2*,* Williams v. City of Detroit, No. 21-10827 (E.D. Mich. June 28, 2024).

[18] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10 (2008).

[19] *Id.*

[20] Thorin Klosowski, *Facial Recognition Is Everywhere. Here's What We Can Do About It*, N.Y. TIMES: WIRECUTTER (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-

mathematician and computer scientist who developed a hybrid model—using both a machine and a human operator—that could recognize faces pulled from the stored facial measurement dataset it had been given.[21] This initial form of FRT was not without its difficulties—the process required human operators to measure the facial characteristics and then enter that information into the computer for storage.[22] Initially, the computer itself had difficulties differentiating between faces. In the beginning, these difficulties became barriers to automatic facial recognition.[23] Using humans to "teach" the computer how to differentiate between faces raises concerns about inherent bias being introduced into the system.

Once Bledsoe understood how to limit technical barriers, he was able to fully automate the program "with software that measured eyes, ears, and so on in a photo of a face without human intervention."[24] From there, FRT's slow evolution continued through the 1990s until its first large-scale use by law enforcement at the 2001 Super Bowl.[25] Fast forward to the mid-2010s, when technological giants in the private sector, Apple and Google's Android, began using facial recognition and introduced FRT as a security feature on their phones.[26] In turn, FRT has experienced rapid growth over the past two decades.

Unlike with Bledsoe's initial creation, human operators are no longer needed to run FRT today. As technology evolves, society is shifting to include AI and machine learning in everyday activities, often integrating these technologies with FRT to increase efficiency and scale. The exponential growth of FRT use in our day-to-day lives provides positives and negatives for different uses and populations. The pervasive nature of FRT exacerbates discriminatory consequences. This is especially apparent for Black and Brown populations, who are already surveilled more than other populations.[27]

works/ [https://perma.cc/5C5G-NPKQ]; *see also* Perkowitz, *supra* note 7, at 4–5 (for his discussion of Bledsoe's "pioneering efforts in facial recognition").

[21] Perkowitz, *supra* note 7, at 5.

[22] *Id.*

[23] *Id.* One main barrier for the computer was the fact that photographs can change the appearance of the same face depending on lighting, angles, facial positioning, and facial expressions.

[24] *Id.*

[25] Klosowski, *supra* note 20.

[26] *Id.*

[27] *See Privacy & Racial Justice*, ELEC. PRIV. INFO. CTR., at 3, https://epic.org/issues/democracy-free-speech/privacy-and-racial-justice/ [https://perma.cc/M5JT-RKCZ] ("People of color are disproportionately subjected to surveillance and tracking. These systems of surveillance erode personal privacy and marginalize[] people of color."); *see also* Nicol Turner Lee & Caitlin Chin-Rothmann, *Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color*, BROOKINGS INST. (Apr. 12, 2022), https://www.brookings.edu/articles/police-surveillance-and-facial-

B. How Today's FRT Works: Bird's Eye View

According to the Center for Strategic and International Studies, FRT is a computer-generated filter that transforms images into "numerical expressions that can be compared to determine their similarity."[28] These filters are usually deep convolutional neural networks (DCNNs),[29] which are multiple layers of convolutional neural networks (CNNs). CNNs are algorithms useful for detecting and recognizing patterns within data.[30] DCNNs work by comparing matrices of pixels and finding matches[31] for face recognition, through the numerical expressions generated from facial images. With each layer of the CNN, larger portions of an image are analyzed for patterns, focusing on finer and finer details.[32] For example, a CNN will separate portions of the image it is fed and continuously, layer by layer, create and store data on each facial image—starting first with simple features such as the colors and edges of the image.[33] A CNN holds on to the data created from the images and is able to mathematically recognize the same face when fed an alternative photograph later on. It has been said that when a CNN is working for the purpose of facial recognition, the CNN acts similarly to the human brain.[34]

It is important to note that a CNN is only as good as the dataset that it learns from and uses. Thankfully, today, FRT algorithms view the diversity of datasets as an important requirement for their models,[35] unlike Bledsoe's original dataset which was fed only homogenous images.[36] When something is created with biased origins, the question becomes whether it is possible to overcome them. It is clear that some in the industry have worked hard to improve their models by introducing diversity to their datasets. However, it remains unclear how much work is required for a system to recognize faces

recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [https://perma.cc/U2FU-SMH7] (providing a discussion on the history of race surveillance and its deadly consequences, specifically, how "racial biases in policing [] disproportionately lead to unwarranted deaths, improper arrests, and the excessive use of force against Black individuals").

[28] James Andrew Lewis & William Crumpler, *How Does Facial Recognition Work?*, CTR. FOR STRATEGIC & INT'L STUD. (June 10, 2021), https://www.csis.org/analysis/how-does-facial-recognition-work [https://perma.cc/QM35-RT7B].

[29] *Id.*; *see also* Perkowitz, *supra* note 7, at 6–7.

[30] *What are Convolutional Neural Networks?*, IBM, https://www.ibm.com/think/topics/convolutional-neural-networks [https://perma.cc/R972-U9L8].

[31] Shesh Narayan Gupta, *Deep Convolutional Neural Networks (DCNN) Explained*, BUILTIN (June 11, 2024), https://builtin.com/articles/dcnn [https://perma.cc/4G2Y-DGD9].

[32] IBM, *supra* note 30.

[33] *Id.*; *see also* Gupta, *supra* note 31.

[34] *See* Lewis & Crumpler, *supra* note 28; *see also* Perkowitz, *supra* note 7, at 6–7.

[35] Perkowitz, *supra* note 7, at 7.

[36] *Id.* at 4.

of all races and genders. When CNNs are introduced to more diverse faces within the dataset, the matching confidence increases, providing better recognition statistics overall.[37] Inversely, when models lack diverse data to pull from, this leads to worse recognition confidence for underrepresented demographic groups compared to groups that oversaturate the dataset.[38] Thus, it is evident that when methods lack diversity training, poor societal impacts may result.[39]

From the beginning of FRT, the models have been riddled with systemic bias due to the lack of data diversity, but with inclusion and diversification, research shows that outcomes can improve. In a research paper by Anubhav Jain et al., the researchers show that it is possible to convert a previously highly biased model into a less biased model by increasing the amount of diverse data it is given.[40] The proposed method included a diverse dataset of 13.5 million images, including "50,000 distinct synthetic identities for six different racial groups."[41] The study concluded that their method of pretraining a model with a balanced dataset mitigates bias in the model and helps achieve fairer outcomes across various demographic groups in identification and photo generation.[42] As datasets become more diversified, matching confidence scores should increase. As confidence scores increase, the fairness of the models used in analyzing and categorizing people by gender and ethnicity will increase as well.[43]

C. Where is FRT Being Used Today?

FRT has applications across a multitude of industries, including security, healthcare, law enforcement, and marketing.[44] Some examples of use include surveillance videos, user authentication, border monitoring, identification screening (licenses and passports), photo and video analytics,

---

[37] *Id.* at 6–7; *see also* Xiaobo Qi et al., *A Convolutional Neural Network Face Recognition Method Based on BiLSTM and Attention Mechanism*, 2023 COMPUTATIONAL INTEL. & NEUROSCIENCE 2501022 (2023), where the authors increased sample diversity through randomly adjusting the brightness and contrast of images from five different datasets. With this alteration, they concluded that their model improved the accuracy of face recognition.

[38] Anubhav Jain et al., *Zero-Shot Demographically Unbiased Image Generation from an Existing Biased StyleGAN*, TECHRXIV (Dec. 2, 2023), at 1.

[39] Perkowitz, *supra* note 7, at 6–7 (discussing CNN-based algorithms and how the degree of diversity in training a data set can affect the racial performance of the CNN).

[40] Jain et al., *supra* note 38.

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] Murat Taskiran et al., *Face Recognition: Past, Present, and Future (A Review)*, 106 DIGIT. SIGNAL PROCESSING 1 (2020).

and social media user engagement and analysis.[45] Perhaps one of the more surprising private sector instances of use is grocery stores employing it to track customers' shopping behavior.[46]

As of August 2021, among the twenty-four government agencies surveyed, eighteen reported using FRT for either digital access or cybersecurity, domestic law enforcement, and/or physical security measures.[47] Of the agencies that answered the survey, six reported using FRT to generate leads in criminal investigations.[48] In some instances, FRT was used to identify suspects from mugshot databases, and in others, it was used to identify crime victims, such as vulnerable children, from publicly available images.[49] Additionally, five of the agencies reported using FRT for physical security reasons, including determining whether someone from a watchlist was present and/or controlling access to buildings and facilities.[50] In the private sector, Clearview AI is one of the main providers of FRT to law enforcement agencies.[51] As of 2021, Clearview AI had partnered with over 3,100 federal and local law enforcement agencies to identify individuals using images from nongovernmental sources.[52] Since 2021, Clearview AI has accumulated more than 60 billion facial images, nearly quintupling the size of its dataset.[53]

Across both the private and public sectors, there is variation in the security of facial recognition data. A November 2023 Department of Defense (DOD) Inspector General report mentions that some DOD biometric technologies "'do not have data encryption capabilities' and do not require the 'certification of destruction or sanitation of biometric data' when biometric devices are disposed [of]."[54] The DOD Inspector General report notes that "this could jeopardize force protection by providing adversaries

---

[45] *Id.*

[46] Lena Geraghty, *Facial Recognition Guide for Cities: Executive Summary*, NAT'L LEAGUE OF CITIES (2021), https://www.nlc.org/wp-content/uploads/2021/04/FacialRecognitionSummary_NLC.pdf [https://perma.cc/BYP4-NFK4].

[47] U.S. GOV'T ACCOUNTABILITY OFF., *Facial Recognition Technology: Current and Planned Uses by Federal Agencies* (GAO-21-526, Aug. 2021), at 15, https://www.gao.gov/assets/gao-21-526.pdf [https://perma.cc/W5GR-U8T8].

[48] *Id.* at 13.

[49] *Id.*

[50] *Id.*

[51] *See* Turner Lee & Chin-Rothmann, *supra* note 27.

[52] *Id.*

[53] *See Accelerate Your Investigations*, CLEARVIEW AI, https://www.clearview.ai/clearview-2-0, [https://perma.cc/7753-J92P] (Clearview notes that their platform "includes the largest known database of 60+ billion facial images sourced from public-only web sources, including news media, mugshot websites, public social media, and many other open sources").

[54] Sayler, *supra* note 12.

with the biometric information . . . ."[55] This lack of security within a major national governmental agency is alarming and unsettling. If the U.S. government is not protecting the biometric data it uses, who is? And how?

III. A LOOK AT THE CURRENT ILLINOIS STATE REGULATION

Illinois was the first state to enact a biometric data privacy law in 2008: the Biometric Information Privacy Act (BIPA). Section 15 of BIPA governs biometric data regulations for private entities and regulates the retention, collection, disclosure, and destruction of individual's biometric identifiers.[56] First, under BIPA, private companies and individuals in the private sector cannot collect, use, share, or store the public's biometric information, unless they get specific, knowing, and voluntary opt-in consent.[57] Notably, a private entity does not include a State or local government agency, court of Illinois, or court personnel.[58] Section 15 mandates private entities in possession of biometric identifiers to develop a written policy which establishes a retention schedule and guidelines for destruction.[59] Further, § 15 orders the destruction of said information to occur either when the initial purpose for collecting or obtaining is satisfied or within three years of the individual's last interaction with the private entity, whichever occurs first.[60]

Second, in addition to imposing obligations on private entities, BIPA empowers aggrieved individuals to seek damages through a private right of action for any individual who has had their information misappropriated (wrongfully collected, utilized, shared, etc.).[61] According to Adam Schwartz, the Privacy Litigation Director at Electronic Frontier Foundation, this is what makes BIPA the "gold standard" of biometric privacy legislation for plaintiffs.[62] Though controversial, other states have attempted to sign into law legislation similar to BIPA. For example, Vermont's legislature passed the Vermont Data Privacy Act (VDPA) in 2024, which, in addition to creating many rights, would have empowered consumers with private right of action against entities that misappropriate their personal data, including biometric data.[63] Ultimately, the Vermont Governor vetoed the bill, citing

---

[55] *Id.*

[56] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15 (2024).

[57] 740 ILL. COMP. STAT. 14 *et seq.*

[58] 740 ILL. COMP. STAT. 14/10.

[59] 740 ILL. COMP. STAT. 14/15(a).

[60] *Id.*

[61] 740 ILL. COMP. STAT. 14 *et seq.*

[62] Talking Liberties with the ACLU of Illinois, *Protecting Your Biometric Information,* ACLU ILL., Episode 16 at 8:19 (Oct. 17, 2019), https://www.aclu-il.org/en/protecting-your-biometric-information [https://perma.cc/DD5C-FMV4].

[63] Vermont Data Privacy Act, H.121, 2023–2024 Gen. Assemb., Reg. Sess. (Vt. 2024).

concerns over the state becoming "more hostile than any other state to many businesses and non-profits."[64] A solution to quell states' fears of being singled out as "hostile" to businesses is providing this private right of action to all consumers across all states through federal regulations similar to those proposed in VDPA and in BIPA. This shift would ensure no single state would be singled out as "hostile."

Turning back to Illinois, this "gold standard" is not set in stone.[65] As courts and legislatures continue to work through enforcing these novel protections, the rights afforded by BIPA may ebb and flow. In the Illinois Supreme Court's February 2023 ruling in *Tims v. Black Horse Carriers, Inc.*, the Court explained that BIPA claims are subject to a five-year statute of limitations under Illinois's "catch-all" period, rather than the one-year statute of limitations for privacy and defamation claims.[66] The reason for this change was mainly driven by policy and the judiciary's desire for "certainty, predictability, and uniformity"[67] for all related claims. This is an example of judicial involvement that has the chance to impact BIPA's protections—at least until the legislature responds.

In the past few years, several bills have been introduced, and some enacted, by the Illinois General Assembly that have the potential to alter the rights afforded by BIPA. As of August 2024, BIPA's broad rights have been modified slightly to limit potential damages for duplicative violations caused by the misappropriation of the same piece of information by the same company.[68] One recent amendment to BIPA's protections, SB 2979, was a reaction by the legislation after the Illinois Supreme Court's holding in *Cothron v. White Castle*. In *Cothron v. White Castle*, the court held that individual scans themselves are each a violation, creating the potential for numerous duplicative violations and limitless amounts in damages.[69] Section

---

[64] Press Release, *Action Taken by Governor Phil Scott on Legislation - June 13, 2024,* OFFICE OF THE GOVERNOR OF VT. (June 13, 2024), https://governor.vermont.gov/press-release/action-taken-governor-phil-scott-legislation-june-13-2024 [https://perma.cc/77SG-3GSG].

[65] ACLU ILL., *supra* note 62 (characterizing BIPA as the "gold standard").

[66] Tims v. Black Horse Carriers, Inc., 216 N.E.3d 845, 853 (Ill. 2023).

[67] *Id.*

[68] Brett M. Doran et al., *BIPA Update: Illinois Limits Liability and Clarifies Electronic Consent for Biometric Data Collection*, GREENBERG TRAURIG (Aug. 14, 2024), https://www.gtlaw.com/en/insights/2024/8/bipa-update-illinois-limits-liability-and-clarifies-electronic-consent-for-biometric-data-collection [https://perma.cc/QQ4W-8JQ8].

[69] Cothron v. White Castle Sys., Inc., 79 F.4th 894, 895 (7th Cir. 2023) (noting that "[t]he state supreme court accepted the certification and has now answered the question, holding that 'a separate claim accrues under the Act each time a private entity scans or transmits an individual's biometric identifier or information in violation of Section 15(b) or 15(d)' of the Act.") (quoting Cothron v. White Castle Sys., Inc., 216 N.E.3d 918, 920 (Ill. 2023) *as modified on denial of reh'g* (July 18, 2023)); Doran et al., *supra* note 68.

IV discusses *Cothron v. White Castle* in more detail. In addition to the change in the potential number of violations, SB 2979 amends what the Act defines as an electronic signature, or a "written release."[70] Now, individuals can provide electronic approval for private entities to collect or disclose their biometric information through methods like an "electronic sound [or] symbol,"[71] such as a voice recording.

In addition to amendments that have been implemented, additional bills have been introduced but are not yet adopted. For instance, an Illinois House Bill *BIPA-SECURITY PURPOSES* seeks to amend the definition for "security purposes" for biometric data usage under BIPA.[72] This amendment would exclude data being collected for *security purposes* from the current three-year retention limitation for private entities.[73] In addition to the change in retention period, the amendment seeks to allow increased disclosure of information to third parties for "security purposes."[74] If enacted, the amendment's vague description of "security purposes" could cause concern. Hardline rules like this make it easy for bad actors to act around them, such as by expanding their definition of what a security purpose is to include more biometric information under the exception than necessary. Originally, there had been a prohibition against all disclosures under BIPA, and now, this purposed exception creates a loophole for private entities to share users' biometric information with others for "security purposes."

Additionally, similar bills have been introduced and have failed. For example, one Illinois Senate bill aimed to alter the scope of "private entity" to include only those who employ more than five individuals.[75] This amendment had the potential to deregulate at least 1 million small businesses from mandated BIPA compliance.[76] Moreover, there is concern for consumers that bills will continue to be introduced that systematically chip away at BIPA's broad protections. This concern is evident from the ACLU of Illinois's devotion to educating and advocating for privacy rights under BIPA.[77]

---

[70] Doran et al., *supra* note 68; Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10 (2024).

[71] *See* 740 ILL. COMP. STAT. 14/10.

[72] BIPA-Security Purposes, H.B. 4102, 103rd Gen. Assemb. (Ill. 2023).

[73] *Id.*

[74] *Biometric Information Privacy Act (BIPA*), ACLU ILL. (May 8, 2024), https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa [https://perma.cc/9GPX-3DL4].

[75] BIPA-Entity Definition, S.B. 3319, 103rd Gen. Assemb. (Ill. 2024).

[76] *See* U.S. SBA OFF. OF ADVOC., *2023 Small Business Profile* (2023) (reporting that 1,007,294 small businesses operate without employees and 220,684 operate with 1–19 employees).

[77] *See* ACLU ILL., *supra* note 74, at *Bills that Weaken BIPA*.

IV. EXAMPLES OF FRT LITIGATION

Examples of recent Illinois FRT litigation will provide context on how courts are interpreting and implementing the current BIPA regulations. First, *Cothron v. White Castle* is important because it shows how the Illinois Supreme Court interpreted certain sections of BIPA and sought to enforce their statutory interpretation. Second, *ACLU v. Clearview AI* is important because of the groundbreaking settlement that came out of the case. By homing in on Illinois-based cases, the likelihood that other cases would be interpreted differently or settled differently is high. This uncertainty is the reason this Note asserts the need for federal regulations. Instead of fifty state supreme courts interpreting their states' regulations, there would be one statute to interpret. This consistency would benefit both businesses and consumers. Moreover, federal protections would help ensure vulnerable populations, especially in states without current regulations, would be protected from the misappropriation of their biometric data.

A. A Deeper Look at Cothron v. White Castle (2023)

Court decisions can alter statutory definitions and greatly influence legislation's impact on parties. Courts often interpret statutes, but in *Cothron v. White Castle*, the court's decision highlighted the importance of legislation having clear statutory intent. The Illinois Supreme Court's holding in *Cothron* prompted the enactment of SB 2979, which amended BIPA to allow an electronic signature to constitute a "written release" under the Act's definition, as well as to allow any electronic sound or symbol used to consent to the collection or disclosure of biometric information.[78] These modifications to individuals' rights under BIPA may not be the last as more legislators are pushing for more constraints on BIPA's applicability. On one hand, it is important to look at BIPA's potential negative impacts on businesses, such as White Castle, which faced a *$17 billion payout*.[79] It is fair that businesses are concerned about understanding BIPA to understand their responsibilities and liabilities. But, like the Illinois Supreme Court emphasizes, it is up to the legislature to consider "policy concerns and make clear its intent regarding the assessment of damages . . . ."[80] Without clear statutory intent, the threat of inconsistency in enforcement cases looms. On

[78] Doran et al., *supra* note 68; Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10 (2024).

[79] John T. Wolak & William C. Martinez, *That's a Super-Sized Sack of Sliders: Illinois Supreme Court Finds White Castle Could Face up to $17 Billion in Damages*, ABA BUS. L. TODAY (May 15, 2023), https://businesslawtoday.org/2023/05/illinois-supreme-court-finds-white-castle-could-face-17-billion-damages-bipa/ [https://perma.cc/T2FW-4DTJ].

[80] Cothron v. White Castle Sys., Inc., 216 N.E.3d 918, 929 (Ill. 2023).

the other hand, any amendments to BIPA, present and future, in response to BIPA-related litigation have the power to take away BIPA's "gold standard" seal of approval for individual plaintiffs' protections. Finding a balance in reading for the legislation's statutory intent and protecting both business and consumers going forward is vital.

In *Cothron v. White Castle*, the controversy arose out of a proposed class action filed by Cothron, on behalf of 9,500 current and former Illinois employees of White Castle.[81] Cothron had been employed at White Castle since 2004 and was working as a manager at the time the suit was filed. The technology at issue was a fingerprint scanner, which was required for access to employees' paystubs and computers. Cothron alleged that White Castle did not seek her consent to acquire her biometric information until 2018, ten years *after* BIPA became effective. Thus, the complaint alleges over ten years of unconsented biometric data collection from Cothron and other employees by White Castle.

The plaintiff in this case originally filed in Cook County Circuit Court. However, the third-party defendant removed to federal court under the Class Action Fairness Act of 2005. Shortly thereafter, the plaintiff dismissed the third party but continued suit in the United States Northern District of Illinois. The District Court certified the case up to the Seventh Circuit. After accepting the certification, the Seventh Circuit found both parties' interpretation of the Act reasonable under Illinois law. Due to the novelty of the question, and the outcome of the case resting on the proper interpretation of the Act, the case was then re-certified to the Illinois Supreme Court.

The main sections of BIPA the courts analyzed included § 15(b) and (d). Section 15(b) states a private entity may not "collect, capture, purchase, receive through trade, or otherwise obtain" a person's biometric data without first providing notice to, and receiving consent from, the person.[82] Further, under § 15(d), private entities may not "disclose, redisclose, or otherwise disseminate" biometric data without consent.[83] Thus, Cothron alleged that White Castle unlawfully collected and disclosed employees' biometric information through distribution to their third-party vendor for fingerprint readers for over ten years.

The certified question presented to the Illinois Supreme Court was whether § 15 claims accrue every time a private entity scans a person's biometric identifier and then disseminates that information to a third party, or if the violation occurs only at the first scan. In the end, the Illinois Supreme Court agreed with the plaintiff. For § 15(b) claims, the court found the plain

[81] *Id.*

[82] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/15(b) (2008).

[83] 740 ILL. COMP. STAT. 14/15(d).

language of the Act to support the conclusion that violations accrue every time a private entity collects or disseminates biometrics without prior informed consent.[84] This conclusion was in line with both the federal district court and Illinois appellate court's views on § 15(b) language. As for § 15(d) claims, the Illinois Supreme Court came to the same conclusion: the Act applies to every transmission of information to a third party. The main arguments for a new violation at every disclosure were that the plain meaning of "disclose" implies a new dissemination,[85] and the fact that "redisclosure" simply means to disclose again, which, under the Act, is another violation.[86] In sum, the court said, "We believe that the plain language of §§ 15(b) and 15(d) demonstrates that such violations occur with every scan or transmission."[87] The court finalized its opinion, noting that policy-based concerns with the potential for excessive damage awards from the Act in place currently are to be left to the legislature to analyze and amend.[88] After the court's decision, SB 2979 is the Illinois legislature's response to this call for action.

According to critics of SB 2979, like the ACLU, the amendment takes away individuals' rights to be compensated for violations of individual rights provided by BIPA. However, from an economic policy perspective, acknowledged by the Illinois Supreme Court, the amendment protects businesses from being liable for damage amounts in the billions while still offering something to individual claimants through their private right to action.[89] The cost-benefit analysis produces different outcomes for each side. On one hand, allowing a company to pay less than the court found them to be liable for creates incentives for companies to continue to collect and disseminate mass amounts of data, largely unscathed. However, on the other hand, it seems unrealistic for companies across the country to be on the brink of bankruptcy as a result of these allegations.

As of September 2024, these recent amendments to BIPA are affecting how biometric data is collected and shared. The amendments to BIPA emphasize the need for companies to review their contracts with third-party providers of biometric devices and information storage.[90] Ultimately, these

---

[84] *Cothron*, 216 N.E.3d at 923–25.

[85] *See* Cothron v. White Castle Sys., Inc., 20 F.4th 1156, 1163–64 (7th Cir. 2021).

[86] *See* Cothron v. White Castle Sys., Inc., 477 F. Supp. 3d 723, 733 (N.D. Ill. 2020), *aff'd*, 79 F.4th 894 (7th Cir. 2023).

[87] *Cothron*, 216 N.E.3d at 926.

[88] *Id.* at 929.

[89] *See* Wolak & Martinez, *supra* note 79.

[90] *See* Alan S. Wernick, *How Will the Recent Amendments to Illinois's BIPA Affect the Use of Biometric Data?*, ABA BUS. L. TODAY (Sep. 4, 2024), https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-june/how-will-

lawsuits highlight the real-world ambiguities that come from novel statutory protections and their interpretations. Because BIPA solely protects Illinois residents, similar circumstances could continue to occur across the fifty states. Instead of re-inventing the wheel for each new state, creating a federal statute to lay a foundation of regulations nationwide is beneficial for all.

B. ACLU v. Clearview AI (2020)

The ACLU of Illinois, while not financially benefitting from BIPA litigation, is one of the plaintiff-side leaders bringing FRT cases on behalf of Illinois residents. Its support is key for plaintiffs, especially as the legislation continues to be amended and as massive amounts of biometric information are collected and shared daily.

ACLU v. Clearview AI illustrates the potential dangers that unregulated Big Tech and FRT can bring to consumers. In May 2020, the ACLU of Illinois filed a lawsuit against Clearview AI. Clearview AI is a privately owned, U.S.-based company developing intelligence platforms, mainly facial recognition.[91] According to its website, it "help[s] generate high-quality investigative leads" for law enforcement.[92] Clearview AI's technology is fed from a database of over 60 *billion* facial images sourced from public sources, including the news, mugshot websites, public social media accounts, and other publicly available sources.[93] Clearview AI previously served more than 200 non-governmental customers, such as Walmart, Bank of America, and the Chicago Cubs, but it has since discontinued its contracts with non-governmental groups.[94] Clearview AI asserts that it is not a real-time surveillance tool; instead, its technology acts *reactively* when a crime has been committed.[95] Therefore, according to Clearview AI, it is not designed to provide live surveillance and is not a threat to individuals' privacy concerns.

In its complaint, the ACLU alleged numerous violations of Illinois residents' privacy rights protected under BIPA. Many of the accompanying plaintiffs in the case were community groups that focus on protecting privacy, with some groups working specifically to ensure the safety of domestic violence and sexual assault survivors. The ACLU asserted that

proposed-amendments-to-illinois-bipa-affect-the-use-of-biometric-data/ [https://perma.cc/G6XQ-U2CW].

[91] *Company Overview*, CLEARVIEW AI, https://www.clearview.ai/overview [https://perma.cc/XJ5E-WNEC].

[92] *Id.*

[93] *Id.*

[94] Complaint at 30, ACLU v. Clearview AI, Inc., No. 20-CH-4353, 2021 Ill. Cir. LEXIS 292 (Ill. Cir. Ct. May 28, 2020); *see also* CLEARVIEW AI, *supra* note 91.

[95] CLEARVIEW AI, *supra* note 91.

before the lawsuit was filed, Clearview AI "ignored the fact that biometric information can be misused to create dangerous situations and threat[en] . . . lives."[96] The main allegation against Clearview AI is that its technology systematically collected and stored faceprints of non-consenting Illinois residents since the company's inception.[97] In addition, the ACLU alleges that Clearview AI has failed to abide by BIPA's publicly available retention schedule policy and also alleges that Clearview has no guidelines for permanently destroying the faceprints that it collects.[98] Additionally, the ACLU argued that other private companies have refused to create technology similar to Clearview AI's because it is a "radical erosion of privacy."[99] Apple went as far as to block Clearview AI from its App Store and from its developer program for violating its terms.[100] Apple's decision suggests that if other large technology companies are refusing to develop technology such as this, it may be worthwhile to assess the privacy and ethical considerations posed by similar technology.

At the time the complaint was submitted, Clearview AI had captured over 3 billion faceprints from images online without the knowledge or consent of depicted Illinois residents.[101] In filing the complaint, the ACLU sought a declaratory judgment stating that Clearview AI's conduct violated BIPA and requiring the unlawful conduct to be ceased. In response to the complaint, Clearview AI offered a few voluntary measures to avoid capturing faceprints of Illinois residents: avoiding utilizing photos online whose metadata included geolocation information within Illinois, avoiding utilizing photos from IP addresses within Illinois, as well as avoiding photos from websites with URLs that contain Chicago or Illinois in the name.[102] For

---

[96] ACLU, *In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law* (May 9, 2022, at 11:45 CT), https://aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois [https://perma.cc/766T-MBQY] (quoting Linda Xóchitl Tortolero, president and CEO of Mujeres Latinas en Acción, a Chicago-based non-profit that fights to empower Latinas through service and advocacy, especially survivors of domestic violence and sexual assault). Here, Ms. Linda Xóchitl Tortolero is referring to the misuse of biometric data in the context of domestic violence and sexual assault survivors, a group uniquely vulnerable to facial recognition surveillance.

[97] Complaint at 27, ACLU v. Clearview AI, Inc., No. 20-CH-4353, 2021 Ill. Cir. LEXIS 292 (Ill. Cir. Ct. May 28, 2020).

[98] *Id.*

[99] *Id.* at 19.

[100] *Id.*; *see also* Rishi Iyengar, *Apple Suspends Controversial Facial Recognition App Clearview AI From Its Developer Program*, CNN (Feb. 28, 2020, at 19:50 EST), https://www.cnn.com/2020/02/28/tech/clearview-ai-apple-account-disabled/index.html [https://perma.cc/76F8-5FJV].

[101] Complaint at 3, ACLU v. Clearview AI, Inc., No. 20-CH-4353, 2021 Ill. Cir. LEXIS 292. (Ill. Cir. Ct. May 28, 2020).

[102] *Id.* at 24–25.

the ACLU, the voluntary measures offered by Clearview AI were a drop in the bucket and would be nearly irrelevant in real applications for protecting individuals' privacy.

After almost two years of litigation, the ACLU and Clearview AI settled on May 9, 2022.[103] The ACLU heralded this settlement as a big win. The settlement agreement called for Clearview AI to comply with BIPA wholeheartedly and stated that Clearview AI was "permanently banned, nationwide, from making its faceprint database available to most businesses and other private entities."[104] In addition to the permanent ban for private actors, Clearview AI was banned from selling access to its database to *any entity* in Illinois, including the state and local police who had been using the services for five years.[105] This settlement agreement made waves and made clear that Clearview AI's unrestricted profits off of unknowing and non-consenting individuals' faceprints was unacceptable. This lawsuit has been one of many in the push for accountability and regulations that will shield individuals from the effects that may stem from biometric data collection and dissemination, especially in the wrong hands.

The *ACLU v. Clearview AI* litigation showcases how BIPA can be used to enforce consumer protections against tech giants, like Clearview AI. By banning Clearview AI from selling its datasets to companies within Illinois, all Illinois residents are protected from their biometric data being scraped and retained without their consent. Further, the suit may show other states why it is important to implement similar legislation. Or, even better, it provides the federal government with a blueprint to enact federal regulations that could eventually protect all American citizens' privacy rights.

V. PREVIOUS FEDERAL INVOLVEMENT

The examples of Illinois-based FRT litigation discussed in Section IV illustrate how the private right of action is working and how the courts have interpreted BIPA's statutory language. Under BIPA, Illinois residents benefit from additional protections and enforcement opportunities as compared to states without similar acts. Section V looks at the current federal enforcer, the FTC, who acts on *behalf* of all consumers under consumer protection laws at the federal level.[106]

---

[103] ACLU, *supra* note 96.

[104] *Id.*

[105] *Id.*

[106] Alfred Ng, *Washington Takes Aim at Facial Recognition*, POLITICO (Jan. 19, 2024, at 8:00 CT), https://www.politico.com/news/2024/01/19/washington-takes-aim-at-facial-recognition-00136498 [https://perma.cc/TU3G-6S7W].

The latest enforcement action from the FTC was in December 2023, when it banned Rite Aid's facial recognition system after alleging that Rite Aid's system had disproportionately misidentified people of color and women as shoplifters.[107] As of September 2025, there have not been any successful attempts for federal legislation implementation to regulate FRT. Although there have been numerous federal actions suggested, including bills and portions of acts that call for specific commission activity, there has been no enacted legislation specific to FRT. Below are a few examples of the federal government's past involvement with FRT-related legislation.

A. National Defense Authorization Act (NDAA)

First, Congress has clearly been thinking about facial recognition and biometric technology, as evidenced by numerous sections of the 2020 and 2021 National Defense Authorization Act (NDAA). According to a Congressional Research Service (CRS) report, in the 2020 NDAA, § 5708 expresses Congress's view that the discriminatory use of facial recognition technologies "is contrary to the values of the United States" and that "the United States Government should not engage in the sale or transfer of facial recognition technology to any country that is using such technology for the suppression of human rights."[108] Moreover, § 5708 tasks the Director of National Intelligence with submitting to the Congressional Intelligence Committee a report on the intelligence community's use of facial recognition technologies, according to the CRS.[109] Similarly, § 5104 in the 2021 NDAA "tasks the National AI Advisory Committee with advising the President on 'whether the use of facial recognition by government authorities . . . is taking into account ethical considerations and . . . whether such use should be subject to additional oversight, controls, and limitations.'"[110] These authorizations of action and power show that Congress is thinking about FRT. The failure of Congress to act and create federal regulations to protect against the misappropriations that are "contrary to the values of the United States" shows the complexity of regulating this kind of technology.[111] It also highlights the need for federal regulations to ensure FRT and other biometric surveillance are not used to the detriment of society.

---

[107] *Id.*

[108] *See* National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 5708(a)(1)–(2), 133 Stat. 1198, 2166–67 (2019).

[109] Sayler, *supra* note 12.

[110] *Id.*; *see also* National Defense Authorization Act for Fiscal Year 2020, 133 Stat. at 2167.

[111] *Id.*; *see also* 15 U.S.C. § 9414(c)–(d).

B. H.R.8152: American Data Privacy and Protection Act (ADPPA)

The American Data Privacy and Protection Act (ADPPA) was introduced in the House of Representatives in June of 2022.[112] When the Act was suggested, it passed the House Committee on Energy and Commerce but failed to advance any further. This was the closest form of legislation that would have provided nationwide protection similar to BIPA. The Committee on Energy and Commerce filed a report in December 2022 recommending the bill to pass with its amendments, including consumer-based foundational privacy rights and enforcement measures for violations of the Act. The Act's purpose was to establish a "preemptive national consumer privacy and data security framework built around limitations for collecting, processing, and transferring individuals' information . . . and providing individuals with control with respect to their personal information."[113] The amended Act suggested that it would have protected biometric information, including "facial . . . mapping, geometry, or templates,"[114] but not including "digital or physical photograph[s]" or "audio or video recording[s]."[115] It is important to note that the ADPPA would not have preempted current state laws, including BIPA, which was an important feature for states who currently have strong protections.[116]

As for enforcement of the Act, ADPPA called for the FTC to continue being the federal regulator, including holding the role of primary enforcement. The Supreme Court in April 2021 held that the FTC may not "obtain monetary relief for consumers who have been harmed solely by using the agency's authority" under the FTC Act.[117] However, under § 402 of ADPPA, the Attorney General or State Privacy Authority may have brought a civil action on behalf of an aggrieved individual to recover damages and civil penalties, enforce compliance, or enjoin the violating practice.[118] Additionally, the amended Act would have given the FTC authority to step into proceedings brought by states when appropriate. Also, private citizens may have brought their own actions for violations as well to recover compensatory damages, injunctive relief, declaratory relief,

---

[112] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

[113] American Data Privacy and Protection Act, H.R. DOC. NO. 117-669, at 36 (2022).

[114] *Id.* § 2(3)(A)(iv), at 3.

[115] *Id.* § 2(3)(B)(i-ii), at 3.

[116] *Id.* § 404(b)(2)(M), at 35; *see generally* H.R. DOC. NO. 117-669 § 404(b)(2) (A-S) for the full list of state laws to be protected under the American Data Privacy and Protection Act.

[117] AMG Capital Mgmt., LLC v. FTC, 593 U.S. 67 (2021); *see also* H.R. DOC. NO. 117-669, at 38.

[118] H.R. DOC. NO. 117-669 § 402, at 31.

reasonable attorneys' fees, and litigation costs. However, individuals may not have brought their suits until two years after the Act were to take effect.[119]

The American Data Privacy and Protection Act aimed to offer a lot of similar protections to BIPA, just on a national scale. Unfortunately, the Act has been left behind, even after the House of Representatives Committee on Energy and Commerce approved it 53-2. Though a similar bill was reintroduced in Congress in 2024—the American Privacy Rights Act of 2024[120]—as of September 2025, both the American Data Privacy and Protection Act and the American Privacy Rights Act of 2024 have not moved further in the House, nor are there related bills listed by Congress. The cycle of proposing these bills suggests that Congress is still thinking about implementing federal regulations for FRT and biometric technology.

C. S.681/H.R. 1404—Facial Recognition and Biometric Technology Moratorium Act of 2023(FRBTMA)

The Facial Recognition and Biometric Technology Moratorium Act of 2023, or S.681, was introduced in the Senate on March 7, 2023. On the same day, it was introduced to the House as H.R. 1404. A review of the Act was referred to the Committee on the Judiciary and the Committee on Oversight and Accountability. The goal was to "prohibit surveillance by the Federal Government without explicit statutory authorization and to withhold certain Federal public safety grants from State and local governments that engage in biometric surveillance."[121] This Act would be a limitation on the ability of governmental entities to utilize FRT, limiting law enforcement's usage of FRT. Comparing FRBTMA with BIPA, the former would offer similar opportunities to bring a civil action for awards of actual and punitive damages, attorneys' fees and costs, and any other relief that would be appropriate under the circumstances. Notably, however, this relief would be targeted at violating governmental entities, not private actors. Due to FRT's usage by a majority of federal agencies,[122] as well as other local and state governmental entities, this Act is unlikely to become legislation. However, it would be an important gap filler for acts such as BIPA, which do not protect against governmental entities and focus solely on private entities.

---

[119] *Id.* § 402, at 61–62.

[120] *See* discussion *infra* Section V.D.

[121] Facial Recognition and Biometric Technology Moratorium Act of 2023, S.681, 118th Cong. (2023).

[122] U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 47, at 9 ("Most of the federal agencies we surveyed—19 of 24—reported one or more FRT-related activities in fiscal year 2020, with digital access and domestic law enforcement as the most common.").

D. H.R.8818: American Privacy Rights Act of 2024 (APRA)

The American Privacy Rights Act of 2024 (APRA) was a new bill reintroduced in the 118th Congress in June 2024 that was based on a bill originally introduced in 2022. In the updated version, there are a few key differences from the original. First, § 117(a)(2)(B), "Enforcement by Persons," mentions BIPA for violations occurring "primarily and substantially in Illinois."[123] The proposed bill would match the relief granted under BIPA for APRA actions. Second, the APRA would preempt some state laws that are not listed as exceptions under § 118(a)(3) "State Law Preservation."[124] The exceptions of laws that are not to be "preempt[ed], displace[d], or [supplant[ed]," include provisions of laws "that address the use of encryption as a means of providing data security,"[125] "that protect the privacy of health information,"[126] that address electronic surveillance,[127] and "[p]ublic safety or sector-specific laws unrelated to privacy or data security . . . ."[128] Notably, this long list of state laws does not include biometric information laws. The exclusion of state biometric information regulations from the exceptions list currently leaves these regulations open to preemption. Right now, should a state law be preempted, this could result in a state's *stronger* protections being taken away. This would be the case for Illinois and BIPA. Preemption would not be of concern, however, if instead Congress explicitly stated that more expansive protections were excluded from preemption.

Other states with strong regulations, such as California, have taken action to oppose enactment of this bill. The California Privacy Protection Agency (Privacy Agency) wrote Congress an opposition letter on June 26, 2024, outlining its objections to the new bill. The letter noted that it "would support a federal privacy law that sets a floor on protections and allows states to continue to adopt stronger safeguards, consistent with most federal privacy laws. Instead, APRA seeks to preempt nearly every provision in groundbreaking state laws . . . ."[129] Further, the Privacy Agency went on to explain how other federal privacy laws typically allow states to adopt stronger protections, such as the Health Insurance Portability and

---

[123] American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. § 117(a)(2)(B) (2024).

[124] *Id.* § 118(a)(3).

[125] *Id.* § 118(a)(3)(P).

[126] *Id.* § 118(a)(3)(N).

[127] *Id.* § 118(a)(3)(L).

[128] *Id.* § 118(a)(3)(I).

[129] Letter from Ashkan Soltani to California Priv. Prot. Agency, *Re: H.R. 8818, The American Privacy Rights Act of 2024 – Opposed* (June 26, 2024), https://cppa.ca.gov/pdf/cppa_letter_opposing_apra.pdf [https://perma.cc/VHE7-85Z2].

Accountability Act (HIPAA) and the Fair Credit Reporting Act (FCRA).[130] Finally, the Privacy Agency pointed out that the APRA sought to weaken independent watchdogs who currently audit and bring administrative actions against businesses for privacy violations, limiting state enforcement actions.[131]

These arguments highlight the issues with the APRA from a consumer protection standpoint. Congress should seek to provide the baseline for privacy protections for all Americans while allowing states to individually add on safeguards for their citizens. Finally, the APRA has not shown any progress in Congress as of late 2024. Therefore, the jury is still out on what this bill will look like in the future, or if it will even pass at all.

These past federal attempts of passing regulations for biometric and FRT-specific usage show that Congress has been thinking about this gap in legislation. This Note suggests the gap-filler is federal regulation which balances the concerns for business and consumer protections and mitigates the threat of discrimination at the hands of face surveillance and biometric technology.

VI. THE SOCIETAL IMPACT

Finally, Section VI analyzes the culmination of modern FRT usage, the current regulatory scheme, and the discriminatory impact of face surveillance on minority communities.

A. FTC v. Rite Aid

A pioneering moment in FRT regulations occurred in late 2023 with the FTC's first enforcement action against a company for their use of AI and FRT in an allegedly biased and unfair manner.[132] This case stands as a warning to other retailers and private entities utilizing FRT, including companies that use FRT to identify and make automatic decisions about consumers.[133] The FTC's action against Rite Aid is the first of its kind. The action is the blueprint to enforce the agency's policies about the misuse of biometric information and consumer protection measures. Further, this action articulates the need for companies to participate in bias mitigation

[130] *Id.*

[131] *Id.*

[132] Kirk Nahra et al., *FTC Announces Groundbreaking Action Against Rite Aid for Unfair Use of AI*, WILMERHALE (Jan. 11, 2024), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240111-ftc-announces-groundbreaking-action-against-rite-aid-for-unfair-use-of-ai [https://perma.cc/L7TN-CEUH].

[133] *Id.*

strategizing and training, and to require routine verification of their program's efficacy.

To summarize the FTC enforcement action against Rite Aid, the FTC alleged that Rite Aid had failed to take reasonable measures to prevent harm to consumers from its use of FRT.[134] The FTC alleged that Rite Aid installed an FRT surveillance system in a subset of its locations, primarily in urban stores, "along public transportation routes," and in locations that would disproportionately impact racial and ethnic minority populations.[135] Further, the complaint alleged that Rite Aid's technology's accuracy varied depending on the demographics of the image subjects and that Rite Aid made no attempt to assess its FRT's reliability, including the likelihood of false positive generation.[136] These false positives caused Rite Aid employees to take action against individuals by subjecting them to increased surveillance, banning them from the store, publicly accusing them of past criminal activity, detaining them, and calling the police to report criminal activity.[137] Rite Aid's failure to take reasonable steps to prevent harm likely caused "substantial injury to consumers, and especially to Black, Asian, Latino, and women consumers."[138]

These allegations can be validated by studies that show AI and FRT are more likely to mislabel faces from these demographic groups. For example, a study done by MIT Media Lab, Gender Shades, found that "[d]arker females have the highest error rates for all gender classifiers ranging from 20.8–34.7%."[139] This is just one study that exemplifies the drastic differences in recognition rates between different races and genders.

Along with the complaint against Rite Aid, the FTC issued a Proposed Stipulated Order for Permanent Injunction and Other Relief. According to the FTC, the Proposed Order "will require Rite Aid to implement comprehensive safeguards to prevent these types of harm to consumers when deploying automated systems that use biometric information to track them or flag them as security risks. It will also require Rite Aid to discontinue using any such technology if it cannot control potential risks to consumers."[140]

---

[134] Complaint at 10, FTC v. Rite Aid Corp., No. 2:23-cv-5023 (E.D. Pa. Dec. 19, 2023).

[135] *Id.* at 12.

[136] *Id.*

[137] *Id.* at 2.

[138] *Id.*

[139] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 87 (2018).

[140] *Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards*, FTC (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-

On February 26, 2024, a Stipulated Order was filed, including stipulations that Rite Aid had to agree to in order to settle the suit.[141] Of those, the most interesting include prohibiting Rite Aid from using the technology for five years and requiring that Rite Aid delete covered biometric information, destroy all methods derived from that information, create a retention policy, post clear notices online and at the retail locations where the technology is to be used, and create a security and monitoring program.[142] These stipulations outline what an ideal FRT program would look like for complete fairness. They also emphasize the fact that companies need to be thinking about discrimination before installing new technology. In the 2023 Joint Statement from the FTC and other regulators including the Consumer Financial Protection Bureau, Justice Department's Civil Rights Division, and Equal Employment Opportunity Commission, the government warned companies that discrimination laws would continue to apply to new technology like AI and FRT, and enforcement would follow any violations of such.[143]

In sum, *FTC v. Rite Aid* highlights what enforcement actions from the FTC will look like going forward for discrimination and bias in AI and FRT utilized by private entities. It also solidifies the fact that some companies are currently utilizing FRT in a discriminatory way. Rite Aid is just one example of private actors using FRT without clear federal guidelines in place. With the FTC taking on enforcement actions on a case-by-case basis, this prolonged timeline between usage and enforcement will likely extend private entities' misguided use of FRT and exacerbate the discriminatory consequences of their actions.

B. Disproportionate Consequences

Numerous sources have reported on the discrimination that stems from racial and gender bias inherent in FRT. For example, Gender Shades, a project active between January 2017 and August 2020, piloted an

releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without [https://perma.cc/8XVT-4F9Z].

[141] Stipulated Order for Permanent Inj. and Other Relief, FTC v. Rite Aid Corp., No. 2:23-cv-5023 (E.D. Pa. Feb. 26, 2024).

[142] *Id.* at 13.

[143] Rohit Chopra et al., *Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems*, FTC (Apr. 25, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf [https://perma.cc/PHE3-CWUQ].

intersectional[144] approach to inclusive product testing for AI.[145] Researcher Joy Buolamwini tested her TED speaker photo on facial analysis technologies from leading companies at the time. She found that some of these technologies could not detect her face at all, while others labeled her face as male.[146] A method's ability to differentiate between genders is essential for high confidence matching between photos and real people. Higher confidence in matching improves fairness in FRT utilization because of the reduced number of false matches. Gender Shades' research found the products that it tested were unfair. After analyzing results on 1270 unique faces, the Gender Shades authors uncovered severe gender and skin-type bias in gender classification.[147] The methodology of Gender Shades included measuring the accuracy of commercial gender classification algorithms that balanced gender and skin type.[148] Of the technologies studied, all performed more accurately on male faces than female faces, more accurately on faces with lighter skin tones than those with darker skin tones, and least accurately on dark-skinned female faces.[149]

Notably, "commercial gender classification algorithms" are not the same FRT methods that we have been discussing, although gender classification technology does automatically determine a person's gender based on their facial features, similar to automated FRT. Critics of Ms. Buolamwini's research harp on this point, noting that the research centered on demographic-labeling algorithms, not facial recognition technology. However, this assertion may be weak. While demographic-labeling algorithms and facial recognition technology are different, both technologies

---

[144] Kimberlé Crenshaw coined the term "intersectionality" in *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics*, 1989 U. CHI. LEGAL F. 139 (1989). There, she used the term to highlight the multidimensionality of Black women's experience as both Black and women, contrasting against the "single-axis analysis that distorts these experiences." *Id.* at 139; *see also Kimberlé Crenshaw on Intersectionality, More than Two Decades Later*, COLUM. L. SCH. (June 8, 2017), https://www.law.columbia.edu/news/archive/kimberle-crenshaw-intersectionality-more-two-decades-later [https://perma.cc/5KB9-HQDT] (In an interview with Columbia Law School, Ms. Crenshaw described intersectionality as "a lens through which you can see where power comes and collides, where it interlocks and intersects. It's not simply that there's a race problem here, a gender problem here, and a class or LBGTQ problem there. Many times that framework erases what happens to people who are subject to all of these things." Intersectionality is a way to see a person's identity such as race, gender, class, etc. through a multidimensional lens acknowledging how each identity creates a unique experience.).

[145] Buolamwini et al., *Gender Shades*, MIT MEDIA LAB, http://gendershades.org/index.html [https://perma.cc/NMT8-HL4F].

[146] Buolamwini & Gebru, *supra* note 139.

[147] *Id.*

[148] *Id.* at 12.

[149] *Id.* at 8 (finding that there was an 8.1–20.6% difference in error rate across all technologies for male to female performance, an 11.8–19.2% difference in error rate for lighter to darker skinned performance, and 20.8–34.7% error rate for darker female face performance).

use machine learning to extract facial features from an image. Classification algorithms learn from data just as a classic FRT does. The main difference is that classification algorithms use their knowledge to predict the person's gender based on other people in the dataset after extracting the features, while FRT matches any given photograph with other similar photographs in the data set based on the data attached to each face.[150]

Additionally, others argue that Gender Shades is an older study and the associated data is outdated, given how fast technology advances.[151] These same critics from the Security Industry Association argue that now, a large number of leading technologies shows much more accurate data. They state that technologies used in commercial and government settings today are "well over 99% accurate overall and more than 97.5% accurate across more than 70 different demographic variables."[152] They argue that FRT today has an accuracy that is better than "fingerprint technologies generally viewed as the gold standard of identification."[153] However, other studies have shown racial bias in FRT, many of which were conducted by federal agencies, such as the National Institute of Standards and Technology (NIST).

In 2011, researchers at the NIST used an image database to compare the accuracy between photographs of individuals of East Asian and Caucasian descent.[154] This study found that the accuracy of the algorithm varied based on where the method was developed. Essentially, if East Asian developers created the method, the method was more accurate in identifying those of East Asian descent compared to other groups, and vice versa.[155] This suggests that whatever gender and racial identity the developer holds, the method will be skewed. As the Center on Privacy & Technology at Georgetown Law points out, this is concerning because "software engineers in the [U.S.] are predominately Caucasian males."[156]

Further, another study that the Center on Privacy & Technology discusses in its study is an FBI-co-authored study from 2012. The study examined three commercially available facial recognition methods and

---

[150] Cunjian Chen, *Gender Classification from Facial Images*, WEST VIRGINIA UNIVERSITY GRADUATE THESES, DISSERTATIONS, AND PROBLEM REPORTS (2011), at 8–15.

[151] Jake Parker & David Ray, *What Science Really Says about Facial Recognition Accuracy and Bias Concerns*, SEC. INDUS. ASS'N (July 23, 2022), https://www.securityindustry.org/2022/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/ [https://perma.cc/B7ML-LWQR].

[152] *Id.*

[153] *Id.*

[154] Clare Garvie et al., *The Perpetual Line-Up*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), Part E, https://www.perpetuallineup.org/findings/racial-bias [https://perma.cc/NTS8-SCF4].

[155] *Id.*

[156] *Id.*

found that all three were 5–10% less accurate in identifying African Americans compared to Caucasians. The study also found similarly skewed accuracy when comparing females to males and younger to older individuals.[157] These studies show the inherent biases and inaccuracies relating to race and gender, which can lead to misidentification. These inaccuracies and misidentification can then lead to law enforcement subjecting persons to wrongful arrests, interrogations, and more.

A key example of this misuse and abuse of FRT is the powerful story of Robert Julian-Borchak Williams. Mr. Williams was wrongfully arrested due to the inaccuracy of the FRT used by the Detroit Police Department. He was arrested on his front lawn in front of his wife and two daughters, without being told by law enforcement why he was being arrested.[158] Mr. Williams was taken to a detention center where his mugshot, fingerprints, and DNA were taken, and he was held overnight.[159] The following day, Detroit detectives showed him still photos from an upscale boutique's surveillance video and accused him of shoplifting.[160] In response, Mr. Williams asked, "[y]ou think all Black men look alike?"[161] Although the detectives acknowledged they got it wrong, this was not the end of Mr. Williams's false-arrest story.[162] After being held in custody for thirty hours, he was released on a $1,000 personal bond. He later had to take time off work to attend his arraignment and deal with various related matters, even though it was clear from the photos he was not the shoplifter.[163]

In response to the wrongful arrest, Mr. Williams, along with the ACLU of Michigan, filed a civil rights lawsuit in April 2021 (and later amended the complaint in 2023), alleging violation of his Fourth Amendment right to be free from unlawful searches and seizures.[164] The Fourth Amendment guarantees the "right of the people to be secure in their persons . . . against unreasonable searches and seizures . . . and no Warrants shall issue, but upon probable cause . . . ."[165] In their complaint, the ACLU focused on the

---

[157] *Id.;* s*ee also* Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (2012) [https://perma.cc/9HH9-9CF7].

[158] Hill, *supra* note 16.

[159] *Id.*

[160] *Id.*

[161] *Id.*

[162] *Id.* ("In Mr. Williams's recollection, after he held the surveillance video still next to his face, the two detectives leaned back in their chairs and looked at one another. One detective, seeming chagrined, said to his partner: 'I guess the computer got it wrong.'").

[163] *Id.*

[164] Amended Complaint at 7, Williams v. City of Detroit, No. 2:21-cv-10827-LJM-DRG (E.D. Mich. June 23, 2023).

[165] U.S. CONST. amend. IV.

reasonably preventable errors of the Detroit Police Department and their consequences.[166] The ACLU further alleged that Mr. Williams's case, along with several other facial recognition-related false arrests in Detroit, proved that the "city lacked any policy for law enforcement use of face recognition technology at the time the technology was used in this case and that Detroit failed to train its police officers on the dangers of misusing face recognition technology in their investigations."[167]

As of June 28, 2024, the parties have formalized a "groundbreaking settlement agreement . . . achieving the nation's strongest police department policies constraining law enforcement's use of face recognition technology."[168] These policies include requiring police to reinforce face recognition results with other reliable evidence linking the matched individual to the crime before making an arrest, train on FRT and its dangers, and audit all cases in which the Detroit Police Department used FRT since 2017.[169] This settlement is a step towards ensuring law enforcement agencies are using FRT accurately and fairly. Further, this situation is not unique—Mr. Williams's case just received wider media coverage compared to other cases. The high error rates for minority groups with FRT plus the lack of FRT-use policies in law enforcement are a deadly combination for false arrests due to FRT's failures.

DataWorks was the FRT company utilized by the Detroit Police Department, which purchased the system in 2017.[170] NIST found DataWorks to be one of over 100 biased facial recognition systems.[171] The NIST Face Recognition Vendor Test (FRVT) "describes and quantifies demographic differentials for contemporary face recognition algorithms . . . ."[172] The FRVT used a data set of *more than 18 million images* from more than 8 million individuals to analyze the accuracy of nearly 200 face recognition algorithms for demographic groups.[173] NIST used this FRVT to generate an

---

[166] *Williams*, *supra* note 164, at 66–68.

[167] *Williams v. City of Detroit Summary,* ACLU (Jan. 29, 2024) https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest [https://perma.cc/2ZNG-AZHM].

[168] *Id.*

[169] *Id.*

[170] Clare Garvie and Laura M. Moy, *America Under Watch*, GEO. L. CTR. ON PRIV. & TECH. (May 16, 2019).

[171] NIST is currently the leading standardized observer of method accuracy. NIST describes and quantifies demographic differentials from FRT on the market today through their Face Recognition Vendor Test. *See* Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* NAT'L INST. OF STANDARDS AND TECH. (Dec. 2019), https://doi.org/10.6028/NIST.IR.8280 [perma.cc/A45P-KLDK]; *see also* Hill, *supra* note 16.

[172] NAT'L INST. OF STANDARDS AND TECH., *Face Recognition Vendor Test (FRVT),* https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt [perma.cc/E6EU-72HH].

[173] *Id.*

internal report that compared and analyzed false match rates within and across countries.[174] It reported nominal false match rates within Eastern European faces, even when the method was developed elsewhere.[175] On the contrary, NIST reported high false match rates for comparisons of darker-skinned individuals across many countries and regions.[176] This included all methods studied, the highest false match rate being for the comparison of Somali faces.[177] Also, NIST noted that it "is very common for algorithms to give high [false match rate] within East Asian countries and between them."[178] Interestingly, when the method was developed in China, some methods exhibited "much reduced" false match rates in the East Asian population.[179] The NIST report also had each algorithm conduct 3 million comparisons of eight demographics (two sexes, four races) within the U.S. mugshot database to analyze the false match rates by race and sex. From its research, it noted several observations including highest false match rates in American Indigenous peoples, higher false match rates for women, and high false match rates in Asian and Black women.[180]

The observations from NIST's FRVT show the varying accuracy among algorithms for matching based on demographic groups such as different countries of origin, race, ethnicity, and sex. These results also vary largely based on the method used. This information is key to informing FRT users to be aware of the inherent biases within their technology. In turn, the hope is to encourage FRT developers to work against these biases and to limit them, as well as train users on how to best use FRT to minimize bias. The data from NIST indicates that there is more to be done in eliminating bias in FRT before we have methods that recognize faces of all races and genders equally.

The inherent racial biases in the FRT methods are not the only cause for disproportionate outcomes—the lack of regulations is also to blame. For instance, the lack of internal testing, apparent in *FTC v. Rite Aid*, is not atypical, but systemic. Situations such as the Rite Aid case emphasize the need for early and continuous testing during both development and usage of FRT. According to The Perpetual Line-Up, a 2016 report by the Center on Privacy & Technology at Georgetown Law, major FRT companies have

174 *Id.*

175 Grother et al., *supra* note 171, at 38.

176 *Id.* (stating that the second highest FMR occurred for West Africa (Ghana, Liberia, Nigeria)).

177 *Id.*

178 *Id.* at 39.

179 *Id.* at 42.

180 *Id.* at 47.

admitted that they do not run internal tests relating to racial biases.[181] The Perpetual Line-Up reports that law enforcement agencies use too few protections to ensure accuracy in facial recognition.

Further, few agencies that use FRT have internal auditing or training programs.[182] The lack of police training in the use of FRT and the lack of policy for its use were apparent in *Williams v. City of Detroit*. Of the agencies who responded to the Center's requests, there were varying approaches for ensuring the methods and systems purchased were accurate. For instance, the Center reported that the Los Angeles County Sheriff's Department and Ohio Bureau of Criminal Investigation "did not require any demonstration or testing for face recognition accuracy."[183] This is quite concerning. In addition to the varying levels of care for baseline system accuracy, few participant agencies used "trained human reviewers" to review the recognition method's results for identification.[184] Without proper training, humans' inherent biases can play a role in inaccurate matches and can become "liabilities for police deployments of face recognition".[185] If untrained humans are such a liability, it seems clear that training is the bare minimum required for ensuring accuracy for FRT matching before subjecting individuals to arrest, detention, and more.

C. Potential for Biometric Autonomous Weaponry

The societal impacts of FRT are limitless. In addition to day-to-day discriminatory outcomes, there are other concerns. One of the most devastating possible outcomes was raised in August 2024, when a Congressional Research Service report (IF11783) suggested that biometric technologies can be integrated with lethal autonomous weapon systems (LAWS).[186] The report noted "[s]uch weapons could potentially feature a database containing the biometric identifiers of preapproved human targets; the weapons could then use the database to autonomously locate, select, and engage human targets."[187] It argued that FRT, combined with weaponry, could increase target precision, which could go in either direction: further in violation of international humanitarian law or further into adherence with international humanitarian law.[188] This potential technological advancement

[181] Garvie et al., *supra* note 154, at Part A: Key Findings.
[182] *Id.* at Part D: Accuracy.
[183] *Id.*
[184] *Id.*
[185] *Id.*
[186] Sayler, *supra* note 12.
[187] *Id.*
[188] *Id.*

could come with serious consequences if the database used has higher error rates for certain populations, such as ethnic, racial, and gender minority groups. This underscores serious ethical concerns, especially if these weapons are used abroad.

Congressional Report IF11783 illuminated that "researchers have repeatedly found that AI-trained facial recognition programs fail disproportionately when used for women and people of color due to both the models and the data on which the programs were trained."[189] Further, even if the data set utilized by the weaponry had equal failure rates, bad actors would continue to exist. An example of this is data poisoning, which is when a bad actor seeks to surreptitiously mis-train an opponent's AI. This "could present additional challenges for AI-trained biometric technologies."[190] Although at the time the Congressional report was written this technology was seen as futuristic, it carries significant ethical concerns that must be addressed before its operation.

VII. SUGGESTION FOR FEDERAL REGULATIONS

It is important to note that the following suggestions are idealized regulations that would be implemented in a perfect world. FTC enforcement actions are currently the primary federal regulatory scheme, which is reasonable. However, operating on a reactive, case-by-case basis is not the most efficient method.

Critics will argue that a federal overhaul of FRT regulations is overreaching. There is a valid concern that technological innovation may be suppressed in instances of regulation that exceeds statutory authority. However, here, federal involvement is proper.[191] Though this does not entirely negate innovation concerns, it is vital to remember that regulations do not exist in a vacuum. Regulations must balance and care for both businesses' interests of innovation, as well as consumer protection. This Note proposes the FTC as the primary enforcement mechanism that has the statutory authority to regulate.[192] Under the Commerce Clause, the FTC, as delegated by Congress, has the authority to do whatever it deems "necessary and proper" in the regulation of matters affecting commerce.[193] As evidence of the FTC acting under this grant of authority, as of January 2025, the FTC has proposed and finalized numerous rules to address AI-enabled consumer

[189] *Id.*

[190] *Id.*

[191] The Commerce Clause is one possible justification for federal regulation, among others.

[192] U.S. CONST. art. I, § 8.

[193] *Id.*

harms.[194] The policy concerns from allowing businesses to exponentially profit off of society without balancing with protections must be addressed. This Note suggests that one path forward is a foundational federal regulation.

This Note proposes fairness and equity to be the principal objectives for the proposed regulation. These principles are particularly appropriate in the case of FRT because of the proven and preventable discriminatory outcomes from unregulated FRT and biometrics usage. If the federal regulations are rooted in these principles and balanced with business necessities, commercial entities will be forced to adapt their auditing methods and implementation of FRT. This Note asserts that although national regulations may increase costs and uncertainty in the industry, the same regulations will incentivize the industry towards a more socially desirable direction. As discussed in Section VI, the current usage and auditing process of FRT results in socially *undesirable* outcomes, such as racial profiling, false arrests and imprisonment, and unfounded harassment.[195] Instead of the FTC enforcing case-by-case and only a few states working towards these objectives, a foundational federal regulation will produce fairer technology usage across the nation.

Additionally, in the past five years, there have been many cases where biometric surveillance companies and those using the technology have settled for large sums of money based on claims under state statutes.[196] A federal foundation would, at a minimum, provide some certainty for the industry to understand what actions are statutorily acceptable going forward. In turn, the assistance from federal involvement would also help streamline the adjudicatory process for these claims in the future.

The following proposal of federal regulations would create a foundation for national protections. It would allow all states to prosecute violating companies and individuals. The proposal is informed by the FTC response in *FTC v. Rite Aid*, BIPA, the 2022 American Data Privacy and Protection Act, and the Facial Recognition and Biometric Technology Moratorium Act of 2023. In the final proposal, keeping the FTC as a primary means of enforcement is not done in ignorance of the need to shift away from

---

[194] FTC, *The FTC is on the Front Lines of AI Innovation & Regulation* (June 2021–Jan. 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/ai-accomplishments-1.17.25.pdf [https://perma.cc/BHG4-Z6ZP].

[195] *See generally supra* Section VI.

[196] *See supra* Section IV.A; *see also* Troutman Pepper Locke State Attorneys General Team, *$51.75M Settlement in Clearview AI Biometric Privacy Litigation Illustrates Creative Resolution for Startups Facing Parallel Litigation and Enforcement Action*, TROUTMAN PEPPER LOCKE (Apr. 30, 2025), https://www.regulatoryoversight.com/2025/04/51-75m-settlement-in-clearview-ai-biometric-privacy-litigation-illustrates-creative-resolution-for-startups-facing-parallel-litigation-and-enforcement-action/ [https://perma.cc/S525-DEDH].

reactionary enforcement. Additionally, should there be a need, adding another option for enforcement, such as through state attorney generals, may provide parties more opportunities to file suit.

First, *FTC v. Rite Aid* assists in outlining the goals of the regulations. These goals include protecting consumers' biometric privacy by limiting retention of biometric data by companies, educating consumers when their data is being collected and used for monitoring, and holding FRT method users accountable when the technology is used in discriminatory ways. The FTC's March 8th Stipulated Order outlines some key highlights for what is important to the FTC moving forward with biometric information collection and utilization compliance. One key point is that companies will be held accountable for their third-party vendors' failure to audit the FRT methods for implicit discrimination and false positives. Commercial entities will need to ensure that the FRT methods they are utilizing have been properly audited to minimize the potential harm—through gender and racial bias, false positives, and actions taken in response—the technology they implement can cause to their customers and the community. Further, another key point is creating and publishing retention policies for the biometric data collected, as well as providing proper notice to customers that they have consented to be subject to biometric monitoring by being on the company's premises.

Additionally, because of its negative impact on the community, Rite Aid was ordered to discontinue its technology for five years. It could be argued that five years is unreasonable or excessive. If the proposal were to minimize impacts on private actors, such as minimizing the time during which the technology must be removed from private actors, the Act may be more likely to pass. Therefore, the final proposal would include a clause for when technologies are found to have false positive rates of 5% or more. The use of that technology must be discontinued *until* tangible improvements are made, without a defined timeframe.

Second, the proposal shall include key components of BIPA protections for consumers within the general framework of the 2022 American Data Privacy and Protection Act (H.R. 8152) to establish the foundational privacy rights and enforcement measures for violations by companies and private actors. Inspired by BIPA, the proposal would include a private right of action for violations of the Act. Currently, after *Cothron v. White Castle*, duplicative violations of the same biometric information are not allowed. The proposal echoes this because of the unreasonable damage awards that may come out of large, class-action suits.

Further, mirroring the BIPA damages amounts of $1,000 per negligent violation and $5,000 for intentional or reckless violations, along with reasonable attorneys' fees and costs, is reasonable for the national scale as

well. BIPA itself does not define "reckless". Imputing the definition of recklessness from Illinois criminal law, an intentional or reckless violator of BIPA would *consciously* disregard a substantial and unjustifiable risk (here, risk of violating the Act) constituting a *gross deviation* from the standard of care that a reasonable person would exercise.[197] This Note suggests any actor who acts intentionally or with wanton disregard for the Act has acted with the requisite culpability to be liable for the higher damages amount. In alignment with BIPA, damages amounts are different for negligence versus intentional or reckless violations because of the necessary culpability attached to an intentional or reckless act.

Additionally, BIPA claims are subject to the uniform five-year statute of limitations. This statute of limitations is reasonable and would allow consumers proper time to learn that their rights have been violated and to act. Therefore, it will be continued in the final proposal. Additionally, similar to the key points from *Rite Aid*, the right to know about the data being collected, how it is stored, and how long it will be kept are important takeaways from BIPA. As for the 2022 American Data Privacy and Protection Act, it mainly echoes BIPA's main points. The most important takeaway from ADPPA is the non-preemption of state laws by the federal statute. This is essential to meet the purpose of establishing a baseline of regulations federally and allowing states to regulate additionally as they see fit. Additionally, the ADPPA proposed that the FTC remains the primary enforcement authority while allowing the state attorney generals or state privacy authorities to bring civil actions on behalf of aggrieved individuals.

By creating a layer of available remedies for consumers, the proposal seeks to ensure that enforcement will be taken seriously by both companies and private actors. Ultimately, the key is safeguarding options for consumers to meet their individual needs.

Third, it is well known that the federal and local governments are some of the main users and collectors of biometric information. Therefore, a portion of the aforementioned regulations and protections should be enforceable against the misuse of biometric information by state actors. This stems from previously introduced congressional bills, such as the Facial Recognition and Biometric Technology Moratorium Act of 2021, which acknowledged the need for regulations for state actors using FRT or other biometric collection technologies. The Moratorium Act aimed to "prohibit surveillance by the Federal Government without explicit statutory authorization,"[198] among other things.

---

[197] 720 Ill. Comp. Stat. 5/4-6 (2025).

[198] Facial Recognition and Biometric Technology Moratorium Act of 2021, H.R. 3907, 117th Cong. (2021).

The proposal hopes to incorporate this goal by creating better steps for the federal government to receive clear authorization. It is unclear what exactly this would look like. However, it is important to regulate the government's use of FRT because of the sheer volume of biometric data it can access. As reports from the DOD suggest, some agencies may not be protecting biometric information at a level we expect of private actors, or at all.[199] The proposal to put up guardrails around the government's collection and use of biometric information may be seen as a limit to the government's ability to protect communities. However, the counterargument is that if the government were to require the use of biometric information for a legitimate purpose, it would still have the same access, but with checkpoints to minimize the threat of abuse or over-collection.

Finally, overall, the main goal of the proposal is to create an adequate baseline of federal protections to protect people equally throughout the U.S. Right now, with the states being the only line of defense for consumers, many Americans are left unprotected from the misuse of their biometric information. Further, regulating FRT with the societal impacts in mind assists in framing the proposal for equal and fair use of FRT for all people, irrespective of race or gender. This is why a unified front of key concepts combined with previous regulations or proposals may be more successful.

To sum up the main points of the proposal:

1. FRT designers, companies, and private actors utilizing FRT must internally audit the technology for accuracy and discontinue use when false positive rates go above 5%;
2. Companies and private actors should be required to post retention and use policies in publicly available spaces and inform consumers of the use of FRT on their premises;
3. Aggrieved individuals will have a private right of action for $1,000 per negligent violation and $5,000 for intentional or reckless violations, in addition to reasonable attorneys' fees and costs;
4. The private right of action will have a statute of limitations of five years and will not allow for duplicative recovery;
5. Individuals, the FTC, the state attorney generals, or the state privacy authorities may bring the civil action on behalf of the aggrieved;

[199] *See supra* Section II.C (". . . some DOD biometric technologies 'do not have data encryption capabilities' and do not require the 'certification of destruction or sanitation of biometric data' when biometric devices are disposed [of].").

6. The federal regulation will not preempt stronger state regulations;
7. There will be a new regulatory scheme specifically for federal and local government actors to create checkpoints to limit unauthorized or unnecessary biometric information collection and usage; and finally,
8. The threat of discriminatory use of FRT looms. Thus, if an actor is found to be intentionally using biometric information in a discriminatory way, punitive damages may be awarded and longer bans on FRT usage will be asserted.

The hope is that future federal regulations for FRT will be implemented to protect *all*. By allowing state-specific regulations to supplement federal regulations, this proposal empowers states to take responsibility and act on behalf of their citizens' specific needs and desires. Ultimately, the federal regulation must be centered on the goals of protecting everyone equally and be informed about the societal implications of unregulated FRT. Baseline federal protections are just the beginning for ensuring that the most sensitive information is protected from misuse and misappropriation by companies, private actors, and the government.