2022

Social Media & Facial Recognition: A Nudge in the Right Direction

Rachel Danielle Beeman

Social Media & Facial Recognition: A Nudge in the Right Direction

Rachel Danielle Beeman*

Introduction

When one uses a retinal, fingerprint, or face-scan to unlock your smartphone, your phone has now stored this biometric data. When you set up your phone, you choose to provide this information to the phone and know, even if not explicitly, that the phone is storing this data.[1] Social media companies like Facebook and TikTok can scan the photos and videos you upload to create and store facial templates. Most users did not, but when Illinois passed the first-ever regulation on biometric data, the battle for privacy and social media began. Illinois' Biometric Information Privacy Act ("BIPA") enacted in 2008, sparked a group of Facebook users to file a class-action suit against Facebook.[2] The users allege Facebook collected and stored their biometric data "in the form of face scans without [ ] prior notice or consent" and harvested the scans for its "Tag Suggestions" program to encourage user tagging.[3] What is even more frightening about this is that this litigation involved algorithms from 2008; today, these facial scanning algorithms are becoming increasingly accurate.[4]

---

* Rachel Danielle Beeman, Seton Hall Law J.D. Candidate, 2022; Honors College and B.A. in Political Science and Philosophy, Seton Hall University, 2018; M.P.A. concentrating in Non-Profit Management, Seton Hall University, 2019. I would like to thank my fiance who has supported me during this process while deployed and serving his country in Iraq.

[1] *See* Jason Cipriani, *iPhone Face ID Is Pretty Cool. Here's How it Works and How to Use It*, C|NET, (Feb. 5, 2020 6:00 AM) https://www.cnet.com/how-to/the-iphone-and-ipads-face-id-tech-is-pretty-darn-cool-heres-how-it-works-and-how-to-use-it/ (stating that during the initial setup of Face ID, the phone "converts your face map to a 2D image that it uses as a master key," and every time after initial set up compares your face "with the master key it created.").

[2] *In re* Facebook Biometric Information Privacy Litigation, No. 15-cv-03747-JD, 2020 U.S. Dist. LEXIS 151269, at *3 (N.D. Cal. Aug. 19, 2020)

[3] *Id.*

[4] *See* Olivia Solon, *Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped without Consent*, NBC NEWS (Mar. 12, 2019) https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921 (in order for these algorithms to improve, they must be "fed hundreds of thousands of images of diverse array of faces" and what is more concerning is that "these people's faces are being used without their consent, in order to power technology that could eventually be used to surveil them").

Recently, California passed and began to enforce new privacy protections with the California Consumer Privacy Act ("CCPA") in 2018, which became effective in January of 2020.[5] With the additional legislation, a group of parents filed a class action against TikTok under both BIPA and CCPA, alleging unauthorized use of their minor child's biometric data.[6] As litigation begins to increase against social media companies, users appear to be rallying their legislatures to act to protect their biometric data. Some scholars refer to this time as a "constitutional moment for the United States," arguing that the increased litigation should be a call to action for Congress to pass a federal statute.[7] This Comment argues, however, that state legislatures should lead the way. State legislatures can offer citizens a private right of action against companies that use and store biometric data without notifying users or receiving express consent. Though the federal government arguably can offer similar relief, state legislatures face fewer procedural stalling and hurdles in comparison to those Congress faces.[8]

There are currently four states that have biometric data-specific statutes: Texas, Washington, California and Illinois. Illinois enacted the first biometric statute on the books and offers the most comprehensive private right of action.[9] California's statute has a private right of

[5] California Consumer Privacy Act of 2018, CAL. CIV. CODE tit. 1.81.5 § 1798.100-199 (2018) [hereinafter *CCPA*] http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (amended Sept. 25, 2020).
[6] *See* Compl. G.R. v. TikTok, Inc.; Compl. P.S. v. TikTok, Inc.
[7] Woodrow Hartzog and Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection,* 61 Boston College L.R. 1687, 1688 (2020).
[8] *See e.g.* Bill Keating, U.S. Representative 9th Distr. of Mass., *The Legislative Process*, (last visited Nov. 11, 2020) https://keating.house.gov/policy-work/legislative-process ("After a bill is introduced and referred to the committee of jurisdiction, the committee will often send the measure to its specialized subcommittee(s) for study, hearings, revisions, and approval."). This is only one step in the long procedure to getting a federal bill passed, which includes holding a public hearing for input. Part IV of this Comment will discuss the flaws of this process in more depth.
[9] *See* Jeffrey N. Rosenthal and David J. Oberly, *Biometric Privacy in 2020: The Current Legal Landscape*, LAW 360, (Feb. 3, 2020) https://www.law360.com/articles/1239794/biometric-privacy-in-2020-the-current-legal-landscape (noting that BIPA "is generally considered the most stringent of all state laws because it is the only biometric privacy law to provide a private right of action."). The Rosenthal article was written prior to the enactment of the CCPA, which also provides for a private right of action, albeit less comprehensive than BIPA.

action, but it is limited and only available under specific breach scenarios.[10] This Comment focuses on the California and Illinois statutes but takes note that Texas, Washington, New York, and Arkansas have either announced new legislation or have altered their current laws to encompass biometric data privacy.[11]

This comment proposes that states should pass a specific and comprehensive biometric data privacy law that (1) allows for a private right of action with statutory damages similar to those seen in BIPA, and (2) details the notice requirements of private corporations to users, prior to their use and collection of the data and services. The legislation, passed in each state would ideally allow plaintiffs to bring claims against social media companies who collect, use and store their biometric data without their express and informed consent. Part I discusses what facial recognition technology is and how it is used both generally and by social media companies. Part II discusses the important privacy implications of biometric data, specifically facial recognition, and why the public should care about this kind of regulation. Part III presents the current legal landscape for biometric privacy at both the federal and state levels, noting that no federal law exists explicitly regulating or protecting biometric data. Part IV discusses the theories underlying opting in versus opting out settings, and the language of notice and consent forms. Part V argues for state legislation as the solution over federal legislation given the inefficiency of the federal legislative process' and the ability for state legislation to provide a more targeted

[10] *See* Mark S. Melodia et al., *Litigating the CCPA in Court*, HOLLAND & KNIGHT LLP (July 22, 2020), https://www.hklaw.com/en/insights/publications/2020/07/litigating-the-ccpa-in-court ("[T]he law expressly provides that a private right of action is available only for certain data breach incidents 'and shall not be based on violations of any other section of' the CCPA."); *see also CCPA*, *supra* note 5, at § 1798.150(c) ("The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title.").

[11] Natalie Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, MINTZ, P.C., (Jan. 15, 2020) https://www.mintz.com/insights-center/viewpoints/2826/2020-01-15-anatomy-biometric-laws-what-us-companies-need-know-2020 ("[F]ive other states (Texas, Washington, California, New York and Arkansas) have now passed their own biometric statutes or expanded existing laws to include biometric identifiers.").

approach for consumers. Further, this part briefly outlines the template that state legislatures should follow based on the current state legislative landscape regarding facial recognition. Finally, Part VI provides a conclusion and discusses how the European biometric data law may also provide some insight into how state legislators should respond.

I. Facial Recognition Technology Today

First, this section will introduce how facial recognition technology works generally. Then, it will move into how social media companies utilize this technology. Specifically, this section will focus on how Facebook and TikTok deploy increasingly accurate and complex algorithms that scan users' uploaded images without users' express consent.

A. How Does Facial Recognition Technology Work Overall?

The typical association with facial recognition technology is likely law enforcement agencies. Generally this technology is defined as a method of identifying or verifying the identity of an individual using their face and can be used to identify people in photos, videos, or in real-time.[12] One method law enforcement may employ is to use their mobile devices during a stop.[13] For example, the application allows officers to put in photos of individuals suspected of a crime and search for other potential images of that face on the web.[14] This power and the criticism the platform has received is likely why the company itself has begun to institute new compliance measures including, requiring the officer to input a specific case number.[15] Clearview AI and its connection to facial recognition and social media will be discussed in more

[12] Electronic Frontier Foundation, *Street-Level Surveillance* (last updated Oct. 24, 2017) [hereinafter *EFF*] https://www.eff.org/pages/face-recognition.
[13] *Id*.
[14] *See* Heather Somerville, *Facial-Recognition Startup Clearview Moves to Limit Risk of Police Abuse*, THE WALL STREET JOURNAL, (Oct. 20, 2020, 3:56 PM) https://www.wsj.com/articles/facial-recognition-startup-clearview-moves-to-prevent-possible-police-abuse-11603217327.
[15] *Id*.

depth later in this Comment.[16] Facial recognition technology is rapidly advancing not only among law enforcement but, more importantly, in connection with social media companies that are improving algorithms and deploying facial recognition for multiple uses.[17]

In general, facial recognition systems "use computer algorithms to pick out specific, distinctive details . . . [like] distance between the eyes or shape of the chin, [ ] then convert [these measurements] into [ ] mathematical representation[s]" where the data collected is a face template.[18] A face template is unique, and "distinct from a photograph because it's designed to only include certain details that can be used to distinguish one face from another."[19] For example, the image below is from a United States Department of Commerce short question and answer, which "reverse engineered" face templates to facial scans with 93% accuracy.[20]

Reconstructed Images (illustration), in Michelle Chibba and Alex Stoianov, *On Uniqueness of Facial Recognition Templates*, NTIA U.S. DEPT. OF COMMERCE, Info. Privacy Comm'r.'s Office of Ontario, Canada (March 2014).

[16] *See infra* Section II C.
[17] *See generally* Thales Group, *Facial Recognition: Top 7 Trends (Tech, Vendors, Markets, Use Cases and Latest News)*, THALES GROUP, (last visited Nov. 12, 2020) (updated Sept. 12, 2020) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition, (discussing how various companies, including Facebook, use algorithms for facial recognition that are increasingly accurate). The article specifically discussed Facebooks DeepFace Program, which was launched in 2014, and can "determine whether two photographed faces belong to the same person, with an accuracy rate of 97.25%." *Id*. This is especially impressive because humans correctly answer this same question in 97.53% of cases. *Id*.
[18] *EFF*, *supra* note 12.
[19] *Id*.
[20] Michelle Chibba and Alex Stoianov, *On Uniqueness of Facial Recognition Templates*, NTIA U.S. DEPT. OF COMMERCE, Info. Privacy Comm'r.'s Office of Ontario, Canada (March 2014) https://www.ntia.doc.gov/files/ntia/publications/uniqueness_of_face_recognition_templates_-_ipc_march-2014.pdf.

Although one can see that these reconstructions are not exact replicas in the way that a photograph would portray, these reconstructed images from the face templates should still create unease if in the wrong hands.

As with every advancement in technology, this too comes with common problems that are worth noting. Some computer systems "are designed to calculate a probability match score between the unknown person and specific face templates stored in the database."[21] The differences between most databases and algorithms are that each "vary in their ability to identify people under challenging conditions such as poor lighting, low quality image resolution, and suboptimal angle of view (such as in a photograph taken from above[,] looking down on an unknown person)."[22] That means that some of these programs are advanced enough to identify someone in low-lighting scenarios, while others cannot. The question then becomes, do those who deploy this technology, like law enforcement, know what minimum bar to set?

The most common errors are known as "false positives" or "false negatives."[23] A "false positive" is "when the face recognition system [matches] a person's face to an image in a database," but is not accurate.[24] For example, "a police officer submits an image of 'Joe,' but the system erroneously tells the officer that the photo is of 'Jack.'"[25] Though this is only a hypothetical, these errors seem to demonstrate important liberty and privacy implications for the "system error" that could harm Jack. Alternatively, a false negative occurs when a face recognition system fails to match a person's face to a face template that is already in the

[21] *EFF*, *supra* note 12.
[22] *Id*.
[23] *Id*.
[24] *Id*.
[25] *Id*.

database.[26] Put simply, the system will return zero results when the database may contain at least one positive match.[27]

B. Facial Recognition Technology and Social Media

Understanding the scale of how facial recognition technology relates to photos uploaded to social media may be difficult. In a 2013 white paper, Facebook reported its users had "uploaded more than 250 billion photos," and in 2017 estimated "that the total number of digital photos stored in [its] electronic database was around 5 trillion."[28] While this does not tell users what the social media giant does with this information, it does demonstrate the sheer number of potential face templates available for "scraping."[29] One way to find out how Facebook uses this information is by looking at its Privacy Policy. In Facebook's Privacy Policy, it advises its users to "consider who you choose to share with, because people who can see your activity on our products can choose to share it with others on and off our products, including people and business[es] outside the audience you shared with."[30] This policy appears to be Facebook's attempt to warn users that it cannot control how or when other users upload pictures of another user.

Another social media application has faced recent scrutiny with its use of facial geometric scans. TikTok, according to a recent class action, "scans a user's facial geometry

[26] *See EFF*, *supra* note 12.
[27] *Id*.
[28] Matthew T. Hays, *Technology Defendants Continue to Test Whether the Illinois BIPA Law Can Cope with Modern Facial Recognition Technology*, DYKEMA GOSSETT PLLC: THE FIREWALL (Dec. 6, 2019), https://www.thefirewall-blog.com/2019/12/technology-defendants-continue-to-test-whether-the-illinois-bipa-law-can-cope-with-modern-facial-recognition-technology/.
[29] For a definition of scraping see *What is Data Scraping?*, THE SCIENCE TIMES (May 29, 2020 11:07 PM) https://www.sciencetimes.com/articles/25874/20200529/what-is-data-scraping.htm, (defining scraping as "an automated technique of gathering data from the web using a scraper," which is a technology that is programed "to extract specific data from targeted websites").
[30] Facebook Privacy Policies, *How is This Information Shared?*, FACEBOOK, (last visited Sept. 22, 2020) https://www.facebook.com/policy.php.

before running an algorithm to determine the user's age . . . [and] uses facial scans to allow users to superimpose animated facial filters onto the moving faces of video subjects."[31] In the Summer of 2020 TikTok announced that for the "first time ever" it would be sharing the number of videos that have been removed for violating platform guidelines.[32] This report, titled "Transparency Report," includes: how the platform handles requests for information, protects minors, and responds to intellectual property infringement, among other things[33]; however, it does not contain the word "biometric" anywhere and does not address the proverbial elephant in the room. Despite this apparent transparency, it does not appear to address the recent allegations against them.

TikTok's alleged facial scans can have an array of uses, and looking to its privacy policy for information reveals that the company is not explicit with how it uses this data. According to their Privacy Policy there is certain information that they collect "automatically," including: "IP address, geolocation-related data (as described below), unique device identifiers, browsing and search history (including content you have viewed in the Platform), and Cookies."[34] The Privacy Policy does not address the recent allegations. The Plaintiffs state that TikTok uses a "proprietary facial recognition technology [to] scan[] every video uploaded . . . for faces, extracts geometric data relating to the unique points and contours (i.e., biometric identifiers) of each face, and then uses the data to create and store a template . . . without" notice.[35] Infringement on a individual's right to privacy, and their ability to know when and how their personally identifying information is being used should not go unnoticed.

---

[31] Compl. at 1, G.R. v. TikTok, Inc., No. 2:20-cv-04537 (C.D. Cal. May 20, 2020).
[32] Michael Beckerman, VP and Head of US Public Policy and Eric Han, Head of Safety, US, *Our H2 2019 Transparency Report*, TIKTOK, (July 9, 2020) https://newsroom.tiktok.com/en-us/our-h-2-2019-transparency-report.
[33] *See id*.
[34] TikTok, *Information We Collect*, (last visited Nov. 11, 2020) https://www.tiktok.com/legal/privacy-policy?lang=en.
[35] Compl. G.R. v. TikTok, at 4.

What exactly are TikTok and Facebook doing with all this data that they collect on our faces? According to TikTok's Privacy Policy, it uses the information it collects to "infer additional information about you, such as your age, gender, and interests," concluding with a catch-all phrasing "for any other purposes disclosed to you at the time we collect your information pursuant to your consent."[36] Is TikTok referring to the mandatory "I Agree" button presented to a user as they put in their name and contact information to register for a profile? If a user is not presented with adequate notice regarding facial scans, social media companies like TikTok should not be allowed to collect and store this information. Further down this page filled with verbose legal jargon, TikTok alerts its users that they "share categories of personal information *listed above* with service providers and business partners to help us perform business operations and for business purposes, including research, payment processing and transaction fulfillment, . . . data storage and hosting."[37] The personal information that TikTok purports to list above appears purposefully vague, and arguably provides them with a wide range of discretion.

II. Why We Care: Threats to Privacy

The pervasiveness of social media creates the potential that individuals will have unwanted photos unknowingly taken of them then posted to a *friend's* profile. This fear transfer into individuals' employment prospects and will be discussed in detail below. Finally, individuals should concern themselves with the prevalence of facial recognition as it has potential ominous governmental uses through law enforcement branches.

---

[36] *See* the TikTok, *Privacy Policy*, (last visited Sept. 23, 2020) https://www.tiktok.com/legal/privacy-policy?lang=en (allowing users to click the appropriate Privacy Policy depending on their location). It is especially interesting that TikTok provides a general privacy policy for all of the United States. *Id*. It is curious that the company does not reflect each of the individual state privacy regulatory standards, especially those which are require increased consumer protections like the CCPA and BIPA.

[37] *Id*. at *How We Share Your Information* (emphasis added).

A. The Threat to User's Image Uploads

Posting photos is more dangerous than writing a blog post or a status update because images are arguably less in our control. Some individuals agonize over the vocabulary they use or their word choices to ensure they do not present a negative connotation or present themselves in a negative light. Yet photos, unlike words, can be taken at any time or place and be posted with or without our knowledge. Then, as this Comment and other news articles have highlighted, social media companies can scan and create facial templates of these unwanted photos.[38] With the evolution of technology and smartphones, photos taken at your friend's BBQ or wedding are uploaded onto Facebook or Instagram, or used as the background of a TikTok and have become not fully within a user's control. Social media users and their friends—regardless of whether or not they have a profile—unknowingly give "up a part of [their] privacy, through [their] social media activities."[39] It is even worse that job applicants are opening themselves up to an "all-out investigation of [their] online persona."[40] Instagram and other social media sites have been described as "a playground for sharing snapshots with friends and a jungle of fierce competition among marketers relying on the expressive power of photography."[41] This new "playground" creates potential negative job implications as the next section will discuss.[42]

---

[38] *See* Aaron Holmes, *Instagram Could Face Up to $500Billion in Fines in Class-Action Lawsuit Alleging it Illegally Harvested Biometric Data*, BUSINESS INSIDER, (Aug. 12, 2020 10:48 AM) https://www.businessinsider.com/instagram-facing-500-billion-in-fines-in-facial-recognition-lawsuit-2020-8 ("Under the law, Facebook could be faced to pay up to $5,000 per violation for as many as 100 million Instagram users, totaling half a trillion dollars at most."). It is important to note that Instagram is owned by Facebook, which is why the article mentions Facebook. Facebook Inc., Annual Report (Form 10-K), at 7 (Jan. 30, 2020).

[39] *See* Dr. Saby Ghoshray, *The Emerging Reality of Social Media: Erosion of Individual Privacy Through Cyber-Vetting and Law's Inability to Catch Up*, 12 J. MARSHALL REV. INTELL. PROP. L. 551, 556 (2013).

[40] *Id*.

[41] Jessica Silbey, et al., *Existential Copyright and Professional Photography*, 95 NOTRE DAME L. REV. 263, 264 (2019).

[42] *See* Stella Liang, *How Social Media Affects Your Chance of Getting Hired*, SIMON FRASER UNIV., (Oct. 7, 2015) http://www.sfu.ca/olc/blog/csi-blog/how-social-media-affects-your-chance-getting-hired.

B. Employers and Social Media Investigations

As part of the hiring process, it is now common for employers to search a potential employee's social media profiles and platforms. Though conducted in 2015, a survey from CareerBuilder found that over fifty-two percent of employers utilize social media profiles and conducted searches of their candidates to determine job eligibility.[43] Further, things such as religious beliefs or marital status, not usually disclosed in an interview, get pushed from the interview room to a simple google search.[44] Social media companies give employers the potential ability to access facial scans that it collects and stores without a candidate ever receiving notice or giving consent. At times companies may employ background check companies. These third-party companies "[w]idespread access to [an] individual's online activit[y] has changed the employment screening landscape as the search for the right candidate . . . has transmogrified into an exercise in seeking a desirable behavioral profile."[45] Scholars posit that social media has become the core for many employment decisions.[46] Further, the more concerning aspect of this is that while "individuals may be more reluctant" to freely express themselves in the form of posts as employers increase their internet investigation,[47] users who do not have social media profiles may still have images uploaded of them.

---

[43] *Id*.
[44] *Id*. ("When it comes to sensitive topics, such as religion and marital status, the interviewers are not supposed to ask during the interview, they will ask Google instead.").
[45] *See Ghoshray, supra* note 40, at 553.
[46] *See Ghoshray, supra* note 40, at 555 ("At the core, the scenarios represent how the societal landscape is being shaped by individuals' immersion in social media.").
[47] *See Ghoshray, supra* note 40, at 576 ("If a potential employee recognizes a priori that anything he or she expresses in a public forum could be found in a future search as part of digital data mining for distilling patterns for a 'suitable' employee, the individual will be more inclined to suppress her thoughts than to express them."). Though this article explores the constitutional implications and infringements on the democratic process employment investigations pose, these implications raise awareness of the need for privacy protections overall. *See id*. at 556 ("[J]udges and administrators will be thrust into the unenviable role of making significant decisions regarding people's lives and livelihoods, with only scarce legislative guidance.").

As the saying goes, a picture says a thousand words. With the ability for large social networking sites to scan and retain biometric data and our lack of control over who posts pictures of us, negative employment decisions may pose serious problems in the near future.[48] Despite the important implications unwanted facial recognition and social media searches can play in one's career, an even eerier threat lurks within government's potential uses.

C. Government Access and Use of this Data

This year we have seen increased scrutiny over a phone application that law enforcement agencies use to assist with finding suspects. As of January 2020, the New Jersey Attorney General announced an investigation into Clearview AI and banned all law enforcement officers from using the technology.[49] This announcement came in light of a New York Times article, which alleged "Clearview had amassed a database of more than three billion photos across the web" from scraping data from "sites like Facebook, YouTube, Twitter and Venmo."[50] Given the potential for this type of data to be taken from social media profiles without notifying users or asking for their consent, and law enforcements potential uses, stricter regulation requiring user consent is something that everyone should be talking about.

Some law enforcement agencies have been using facial recognition technology long before the release of Clearview AI. The oldest and largest facial recognition system in the country is based out of Pinellas County, Florida, and has been in place for over twenty years.[51]

---

[48] *See* Michael J. Tews et al., *The Effects of Negative Content in Social Networking Profiles on Perceptions of Employment Suitability*, 28 INT. J. SELECT ASSESS. 17, 17 (2019) ("Given the ease of access to information and its low cost, employers are increasingly making use of social networking sites in the context of employee selection."). This article continues to say that about sixty percent of employers will eliminate candidates because of perceived negative social media profiles. *Id*. at 17–18.

[49] Kashmir Hill, *New Jersey Bans Police from Using Clearview Facial Recognition App*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/technology/clearview-ai-new-jersey.html.

[50] *Id*.

[51] *See* Jennifer Valentino-DeVries, *How The Police Use Facial Recognition, and Where it Falls Short*, N.Y. TIMES (Jan. 12, 2020), https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.

The officials in Florida stated that they use the system 4,600 times per month, but it is only effective with clear images such as photos from anonymous social media accounts.[52] Despite this database containing access to over thirty million images some law enforcement agents argue that the law does not require them to tell the court or the defendant's attorney about any use of facial recognition during an investigation.[53] The most concerning part of this exposé is that a 2016 Georgetown Law study showed one in two Americans were in a law enforcement facial recognition program,[54] given Clearview AI's recent contracts with law enforcement that number has likely increased. Further, this is not simply a local issue, but as the study shows, the Federal Bureau of Investigation ("FBI") uses individuals 'driver's license photos to compare the faces of suspected perpetrators.[55] Though this is a demonstration of how the FBI was using driver's license photos, Clearview AI was founded in 2017, and with the attack on the U.S. Capital building in early 2021 speculation abounds as to the use of facial recognition technologies.[56]

Though Clearview AI and its connection to American law enforcement is a modern issue, the government using social media to find individuals is not new. In 2009 Iran used photos to target and identify potential protest sites.[57] The government "posted photos from protests on a website and invited citizens to identify individual faces that were singled out."[58] If the government had wanted, perhaps they could have uploaded the photos to Facebook, and once the

---

[52] *Id*.
[53] *Id*.
[54] *See* Clare Garvie, Alvaro Bedoya and Jonathan Frankle, "The Perpetual Line-Up: Unregulated Police Face Recognition in America," Georgetown Law: *Center on Privacy & Technology* (Oct. 18, 2016) https://www.perpetuallineup.org.
[55] *See id*.
[56] *See* Rae Hodge, *Capital Attacks: FBI Mum on Facial Recongition, Clearview AI Searches Spike*, C|NET (Jan. 12, 2021 1:36 PM) https://www.cnet.com/news/capitol-attack-fbi-mum-on-facial-recognition-clearview-ai-searches-spike/ (Though the FBI has not responded to questions as to whether or not they are using facial recognition to identify suspects, "Clearview AI has confirmed a spiek in searches of its database used by law enforcement").
[57] Yana Welinder, *A Face Tells More than A Thousand Posts: Developing Face Recognition Privacy In Social Networks*, 26 HARV. J. L. & TECH. 165, 167 (2012).
[58] *Id*. at 166.

"tagging" feature was in use, they may have had suggestions for who those potential suspects were. Though facial recognition technology in 2009 was not sophisticated enough to identify these protestors, imagine if "the government could simply match these faces against the hundreds of billions of photos available on Facebook,"[59] or Instagram, or TikTok available today.

Facebook and Instagram used their ability to access and use our photos to "expand facial recognition algorithms and optimize age progression technology."[60] Therefore, our data is accessed without our permission or knowledge, and large social media companies are profiting off users' image and likeness without consent or knowledge.

III. Current Legislation Regulating Biometric Data

Part III focuses on the lack of federal regulation and evaluates the current state regulation. Specifically, this Comment focuses on the comprehensive biometric data law in Illinois and California, and only briefly outlines both Washington and Texas laws.

A. Federal Legislation

In light of news articles circulating about facial recognition harms in association with law enforcement in 2020, Senators Markey and Merkley, along with Congresswomen Jayapal and Pressley, introduced the Facial Recognition and Biometric Technology Moratorium Act of 2020.[61] Likely, the ACLU litigation pressured Congress with its allegations that Clearview AI committed an "extraordinary and unprecedented violation of Illinois residents' privacy rights . . . seeking to profit off its use of 'face recognition technology.'"[62] Though the proposed federal bill

[59] *Welinder, supra* note 57, at 167.
[60] Logan Wayn and Jake Linford, *Contracting for Fourth Amendment Privacy Online*, 104 MINN. L. REV. 101, 102 (2019).
[61] Press Release, *Senators Markey And Merkley, And Reps. Jayapal, Pressley To Introduce Legislation To Ban Government Use Of Facial Recognition, Other Biometric Technology*, (June 25, 2020) https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology.
[62] Compl. at 1–2, American Civil Liberties Union v. Clearview AI, Inc., No. 2020CH04353 9337839 (May 28, 2020).

does not implicate private companies, it demonstrates that citizens' pressure through distrust and uproar can force Congress to act. This bill is important in the context of this Comment not because of the bill itself as most federal bills do not become law, but rather the bill acts as a clear demonstration of the lack of speed and efficiency with which Congress can act. Prior to this federal move, states responded more quickly, took measures into their own hands, and banned law enforcement agencies from using facial recognition applications.[63] Within the time it took to propose the Congressional Bill, this phone application under investigation and accused of BIPA violations received a federal contract. The Department of Homeland security and ICE announced their partnership with this controversial app.[64] The Moratorium demonstrates litigation groups such as the ACLU's ability to pressure legislators, but this bill would only cover federal law enforcement agencies and a few limited state agencies. Therefore, in regard to facial recognition and biometric data usage, private companies are still in the clear from even potential federal regulation within the United States at this time. If citizens have the power to encourage representatives to propose sweeping and novel legislation, the public should further demand that social media platforms be required to provide users with notice and require affirmative consent.

B. State Legislation

A few states have passed biometric data-specific privacy laws. The trend of passing legislation in this field as well as the constant change in the legal landscape, warrants an argument that social media companies should merely create the most comprehensive privacy policy to avoid having to make future changes.[65] This section, however, focuses on the current

[63] *See Hill, supra* note 49.
[64] Taylor Hatmaker, *Clearview AI landed new facial recognition contract with ICE*, TECHCRUNCH, (Aug. 14, 2020, 6:34 PM) https://techcrunch.com/2020/08/14/clearview-ai-ice-hsi-contract-2020/.
[65] *See generally* Natalie Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020*, MINTZ P.C. (Jan. 15, 2020) https://www.mintz.com/insights-center/viewpoints/2826/2020-01-15-anatomy-biometric-laws-what-us-companies-need-know-2020.

array of statutes that exist in Illinois, California, Texas, and Washington. The Illinois and California sections discuss recent cases against social media companies Facebook and TikTok, and the Texas and Washington subsections will focus on the statutes themselves.

1. Illinois' Biometric Protection

Illinois was the first state legislature to specifically address biometric data when it passed BIPA in 2008,[66] and citizens did not take long to put this bill to use. First, looking at the statute it is important to note the extensive private right of action the language of the statute gives to aggrieved citizens. This is demonstrated through looking at BIPA in action in the settlement and case against Facebook from 2020.

i. The Biometric Information Privacy Act of Illinois

BIPA, in its relevant provision states that any person aggrieved by a violation of this Act shall have a right of action and recover against any private entity that violates this Act with increasing minimum liquidated or actual damages as the scienter requirement increases. [67] Further, a plaintiff may get reasonable attorneys' fees and costs, as well as injunctive relief depending on what the court deems appropriate. [68] The statute provides for a private right of action. A private right of action allows any individual who meets the statute criteria has a right to bring a claim to court on their own.[69] Illinois is the only state law to allow such a broad private right of action. Specifically, the statute provides for **X** REMEDY. The other state

[66] Molly McGinley et al., *New Jersey Eyes Regulation of Biometric Data*, N.J.L.J. (June 27, 2019), https://www.law.com/njlawjournal/2019/06/27/new-jersey-eyes-regulation-of-biometric-data/.
[67] Biometric Information Privacy Act of 2008, 740 ILL. COMP. STAT. ANN. 14/20 https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 [hereinafter BIPA].
[68] *Id*.
[69] Michael D. Hays, et. al, *Overview of Recent Decisions Interpreting the Illinois Biometric Information Privacy Act*, HUSCH BLACKWELL LLP (Oct. 15, 2019) https://www.huschblackwell.com/newsandinsights/overview-of-recent-decisions-interpreting-the-illinois-biometric-information-privacy-act#:~:text=The%20Illinois%20BIPA%20is%20the,up%20to%20%245%2C000%20per%20violation ("[Illinois] is the only biometrics privacy statute in the country with a private right of action that provides for liquidated damages for 'aggrieved' parties of up to $5,000 per violation.").

statutes named herein do not provide for a private right of action, other than California, which limits the extent of the private action to a specific subset of issues.

ii. Facebook and BIPA

Recently, the 2008 litigation against Facebook settled. Illinois residents brought claims against Facebook under the Illinois law yet agreed to transfer the case from the United States District Court for the Northern District of Illinois to the Northern District of California.[70] The users claimed that their biometric data was used and stored without their permission or knowledge for the suggested tag tool.[71]

First, the court analyzed the plaintiff's standing in the case. Under federal law, a plaintiff has standing to bring suit if they can show: "(1) they suffered an actual, concrete injury in fact; (2) a causal connection between the injury and the conduct complained of; and (3) a likelihood that injury will be redressed by a favorable decisions."[72] In this case, the court concluded the plaintiffs "alleged a concrete and actual injury in fact under BIPA that was sufficient to confer standing."[73] The Ninth Circuit reached a decision interpreting BIPA in a favorable light to plaintiffs.[74]

The court in *In re Facebook Biometric Infor. Priv. Litig.* approved to an amended settlement agreement, [75] which it entered in August of 2020.[76] The settlement prior settlement in

[70] *See In re Facebook Biometric Information Privacy Litigation*, 185 F. Supp. 3d 1155, 1158. (N.D. Cal. 2016).
[71] *See In re Facebook*, at *5.
[72] Karen Borg and Al Fowerbaugh, *BIPA Suits Against 3rd-Party Vendors Face Numerous Hurdles*, LAW 360, (Aug. 20, 2020) https://www.law360.com/articles/1300064/bipa-suits-against-3rd-party-vendors-face-numerous-hurdles.
[73] *See In re Facebook*, at *5.
[74] *Id.* at *6 (citing Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 28 (Ill 2019) (holding that "a person need not have sustained an actual damage beyond violation of his or her rights under the Act in order to bring an action under it."). This interpretation is especially important because it arguably provided plaintiffs with the broadest private right of action available. The bar is high for plaintiffs to prove harm and damages, and with the courts limited interpretation of harm as any violation of the statute, a true victory for privacy occurred in 2019.
[75] The court rejected the initial proposal partially due to a concerns for an unfair and "steep discount" on statutory damages under the BIPA, an overly broad release from liability and lack of sufficiency of notice. *Id.* at *6–*7.
[76] *Id.* at *7.

June received criticism from U.S. District Judge James Donato, charged with overseeing the case, as "woefully inadequate" and "too little in the long run."[77] This criticism is important to emphasize within this Comment because it demonstrates that while a remedy through the judiciary may be a good way to "scold" a multi-billion-dollar company, it is likely not enough. Therefore, instituting new regulatory requirements on a state-by-state basis would like to have more impact.

The specifics of the settlement agreement demonstrates that the judicial action in these matters is merely a slap on the wrist. The original settlement proposed to create fund that amounted to a mere 3% of Facebook's total net income of $18,485,000,000 in 2019.[78] While this was a good start, the final amended settlement takes the penalties one step further, requiring Facebook to create an opt-in setting[79] and pay an additional $100 million.[80] This settlement furthers the argument that state legislation is better because this agreement is limited to only members of the class.[81] Settlements, unlike a court ruling or decision are not binding as precedent on potential future litigants. Although the settlement agreement states that Facebook must set the Face Recognition default to off and "delete all existing face templates for class members unless Facebook obtains a class member's express consent."[82] To receive this kind of consent, Facebook would have to expressly disclose its uses and possession of the face templates, an unlikely scenario.[83] It is not clear whether or not Facebook has followed through,

---

[77] Bobby Allyn, *Judge: Facebook's $550 Million Settlement In Facial Recognition Case is Not Enough*, NATIONAL PUBLIC RADIO, (July 17, 2020, 11:36 PM), https://www.npr.org/2020/07/17/892433132/judge-facebooks-550-million-settlement-in-facial-recognition-case-is-not-enough.
[78] Facebook Inc., Annual Report (Form 10-K), at 42 (Jan. 30, 2020).
[79] An opt-in setting is one that requires users to explicating agree to have the respective company collect their data, rather than the company automatically collecting it.
[80] *See In re Facebook*, at *7.
[81] Keep in mind that settlements are not binding, therefore, despite this case seeming like a victory it does not bind future courts that will likely see this issue again.
[82] *See In re Facebook*, at *8.
[83] *Id*.

though if they had, this settlement arguably would only be applicable to Illinois residents, and no other state residents would be required to receive notice of Facebook's facial template collection, nor the users express consent to use these facial scans.

The most important aspect of this settlement is that Facebook is required to interpret "silence or inaction by the user" as the "withholding of consent, and the Face Recognition function [must] be set on "off" and [the relevant] face templates deleted."[84] This is similar to the opt-in measure that this Comment will propose, but the judiciary does not have a specific enforcement branch. The court can issue fines or bench warrants, but this is not enough considering the judge themselves cannot directly ensure that the settlement is followed. State legislative measures should be created to form these private rights of action and create a legally enforceable measure against social media companies that requires notification of collection, use, and storage of this data, along with what purposes they are using the data for.

Beyond Facebook, TikTok users have attempted to voice their concerns about the app tracking and using their facial geometrics for profit without users' consent.[85] It is difficult to know how much TikTok profits from users' data because they are a private company that does not have to legally disclose its financial data in the same way Facebook does to its public investors. A recent news article shows that "[a] class-action lawsuit accuses TikTok of collecting and storing users' biometric data without consent."[86] This suit was "[f]iled in the U.S. District Court for [the Northern District of California] by guardians for two Illinois [minors] who used the app."[87] The complaint states that "TikTok violated Illinois' Biometric Information

[84] *Id.*
[85] *See generally* Compl. P.S. v. Tiktok, Inc., No. 3:20-cv-02992-WHO, April 30, 2020.
[86] Sara Merken, *TikTok Faces Privacy Lawsuit Over Biometric Data Collection*, WL (May 1, 2020), https://www.reuters.com/article/dataprivacy-tiktok/tiktok-faces-privacy-lawsuit-over-biometric-data-collection-idUSL1N2CJ22P.
[87] *Id.*

Privacy Act by not informing users that it collected face scans or disclosing its reasons for doing so."[88] The plaintiffs seek to represent a class of individuals who, when living in Illinois, "used face filters, face stickers, or the face tracker lens on an image or video of that user's own face or whose face appeared in a video" on the TikTok app or the musical.ly app, which merged with TikTok in 2018.[89]

With the recent settlement against Facebook, the tidal wave of litigation is growing against social media companies. As of July 2020, "[t]here are now close to twenty similar class actions in which Illinois TikTok users have sued under BIPA, with other cases in the Northern District of Illinois and in the Northern and Central District of California (all such actions collectively, "TikTok Actions")." [90] Facebook is not the only social media company coming under scrutiny by its users demanding reparations for privacy harms they suffered without proper notice. Further, these users are using both the CCPA and BIPA to attempt to get the courts to intervene.

2. California's Privacy Act

In 2018, California followed Illinois' lead and passed the CCPA. The CCPA gave consumers more control over data that businesses can collect from them, and the legislation did not go into effect until January 1, 2020.[91] Despite its infancy, over fifty lawsuits have already been filed.[92] The statute requires "companies that sell consumer data to disclose that practice and give consumers the ability to opt-out of the sale by supplying a link titled 'Do Not Sell My

[88] *Id*.
[89] *Id*.
[90] A.S. v. Tiktok, Inc., No. 3:20-CV-00457-NJR, 2020 U.S. Dist. LEXIS 114991, July 1, 2020, at *3.
[91] Mark S. Melodia et al., *Litigating the CCPA in Court*, HOLLAND & KNIGHT LLP (July 22, 2020), https://www.hklaw.com/en/insights/publications/2020/07/litigating-the-ccpa-in-court.
[92] *Id*.

Personal Information' on the business's home page . . . known as the right to opt-out," but for consumers under the age of 16 parents or guardians must opt-in.[93]

Facebook has responded to the CCPA with what is known as limited data usage.[94] Facebook introduced this adjustment to its platform in July as a response to California's announcement that it would implement strict enforcement starting July 31, 2020.[95] Facebook added this "feature require[ing] simple modification[s] to the existing Facebook PageView pixel so that Facebook can automatically detect whether or not a user is in California."[96] Specifically, Facebook's developers "will need to include a string within the Facebook pixel for 'dataProcessingOptions' [ ] allow[ing] business[es] to specify its degree of CCPA compliance."[97] It appears that the amount of effort to ensure compliance is mounting against social media companies. Continuously updating algorithmic additions must at some point begin to outweigh the diminishing benefit of avoiding compliance, and it is only a matter of time until this point is reached.

Most notably, California passed a modification to the CCPA at the end of the same year that it became effective, 2020.[98] The amendment is known as the California Privacy Rights Act ("CPRA"), which "greatly expand[s] the CCPA and impose[s] novel obligations on businesses," including "grant[ing] consumers new rights, and modify[ing] the CCPA's enforcement

---

[93] Kristen J. Matthews and Bourtney M. Bowman, *The California Consumer Privacy Act of 2018*, *Privacy Law Blog*: PROSKAUER ROSE LLP, (July 13, 2018) https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/.
[94] Simon Poulton, *Facebook CCPA Compliance Challenges: Limited Data Use*, SEARCH ENGINE LAND (July 2, 2020), https://searchengineland.com/facebook-ccpa-compliance-challenges-limited-data-use-337170.
[95] *Id*.
[96] *Id*.
[97] *Id*.
[98] Matthew A. Diaz and Kurt R. Hunt, *California Approves the CPRA: a Major Shift in U.S. Privacy Regulation*, 11 NAT. L. REV. (Nov. 17, 2020) https://www.natlawreview.com/article/california-approves-cpra-major-shift-us-privacy-regulation ("[A] major expansion of the existing California Consumer Privacy Act (CCPA), which many businesses continue to grapple with since becoming effective in January 2020.").

provisions."[99] Further, the CPRA expands the exemptions related to the Health Insurance Portability and Accountability Act ("HIPAA") and what is known as de-identified information.[100] Bloomberg Law provides suggestions for how businesses should address the shifting legal field surrounding increased consumers' concerns for their privacy.[101] Though Illinois and California have passed expansive legislation, there are two other states with approaches worth noting.

iii. Texas' Biometric Privacy Statute

Following Illinois' lead, Texas enacted legislation in 2009, which specifically prohibits private companies' use of certain biometric identifiers.[102] This statute does not include a private right of action, meaning that anyone who is aggrieved may not bring an individual suit. Instead, aggrieved individuals must show that the "the civil penalty is $25,000" for the state attorney general consider bringing an action.[103] The high-bar for damages demonstrates a significant hurdle for individuals able to bring their claims to the Texas Attorney General's office. The Texas' statute specifically identifies what a biometric identifier is and limits a person's ability to capture a biometric identifier "of an individual for a commercial purpose unless the person: (1) informs the individual before capturing the biometric identifier; and (2) receives the individual['s] consent to capture the biometric identifier."[104]

---

[99] Mark Brennan et al., *Insight: California Privacy Rights Act – Key Takeaways for Businesses*, BL, (July 15, 2020, 4:01 AM) https://news.bloomberglaw.com/class-action/insight-california-privacy-rights-act-key-takeaways-for-businesses?context=search&index=8.
[100] *See* Diaz, *supra* note 98.
[101] Some strategies include: re-evaluating data inventories and data maps to determine their sufficiency measured against CCPA requirements, monitor privacy developments both at the California state legislature level and the federal-level, and keep in mind that exceptions grants to "employee and business-to-business information" are expiring in January of 2021. *Id*.
[102] TEX. BUS. & COM. CODE ANN. tit. 11 (2009), https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm.
[103] *Id*. § 503.001(d).
[104] *Id*. § 503.001(b)(1-2).

Despite this law being on the books since 2009, only recently the Texas Attorney General announced an investigation into Facebook's use of biometric identifiers.[105] A private right of action is more effective because it takes the pressure off of public officials who may be distracted by re-election and the public's perception of their leadership. Further, a private right of actions takes the pressure off of taxpayers given that State Attorney General offices are public functions, which are funded through state funds. Attorney General's offices, funded through taxes, do not have to worry about over consumption of taxpayer funds if a private right of action is available for citizens to seek remedy. Private individuals who want to bring actions against private companies like Facebook or TikTok may do so under both the Illinois and California legislation.

iv. Washington States Biometric Law

Washington enacted a business regulation in 2017 that included what a business may not do with a biometric identifier as it is described within the statute.[106] The law does not provide a private right of action, however. The statute places exclusive enforcement in the Attorney General of the State of Washington.[107] This statute differs from both Texas and Illinois law in that it does not regulate "the capture of biometric data and instead focuses on the 'enrolled' – 'unenrolled' dichotomy . . . if an entity does not enroll biometric data in the method proscribed . . . the act will not impose its notice and consent requirements."[108] This language indicates that the business must follow the specific method described in the language to fall under the notice and

[105] Hunton, Andrews Kurth LLP, *Texas AG investigates Facebook's Use of Biometric Identifiers*, (July 29, 2020), https://www.huntonprivacyblog.com/2020/07/29/texas-ag-investigates-facebooks-use-of-biometric-identifiers/.
[106] WASH. REV. CODE ANN. tit. 19 § 19.375.020, https://app.leg.wa.gov/RCW/default.aspx?cite=19.375.
[107] *Id*. at § 19.375.030(2).
[108] Niya T. McCray, *The Evolution of U.S. Biometric Privacy Laws*, INSURANCE LAW: SENSITIVE TO THE TOUCH, at 79 (May 2018) https://www.bradley.com/-/media/files/insights/publications/2018/05/ftd1805mccray.pdf.

consent requirements. Therefore, it is fair to reason that businesses can evade this type of regulation by simply enrolling biometric data in a manner that is not proscribed by the statute.[109]

Washington has recently attempted to amend its law and allow for a "broad private right of action," but this amendment failed.[110] Despite this failure, the mandate remains that a "person may not enroll a biometric identifier in a database for commercial purpose, without first providing notice, obtaining consent or providing a mechanism to prevent the subsequent use of biometric identifier for commercial purpose."[111]

The Washington law as it stands appears weak on its face and not likely to be truly enforceable against private corporations. This is especially true when one looks at the "broad security exception," that allows for "entities that collect and store biometric data in relation to a 'security purpose'" to be exempted from prosecution under the law.[112] This exception includes excluding stores tha have video surveillance, but it is not yet clear how broadly this security exception will go.[113] Specifically with regard to mobile devices that store fingerprints or facial recognition technology for payment methods stored on a device, it is unclear whether this method would fall under "security purpose."[114]

IV. Theories Underlying Default Settings and the Relevance of Nudging

[109] *See* Divya Taneja, *Washington Enacts a Biometric Privacy Statute in a Departure from the Existing Standard*, Proskauer Rose LLP (June 13, 2017) https://newmedialaw.proskauer.com/2017/06/13/washington-enacts-a-biometric-privacy-statute-in-a-departure-from-the-existing-standard/ ("If an entity does not enroll biometric information for a commercial purpose in the precise way described in this definition – collection, conversion into a reference template, and storage in a database – the entity is not subject to the Statute's requirements.").
[110] Christopher J. Buontempo and Cynthia J. Larose, *Update: It's Déjà vu all over again: Washington Privacy Act Fials to Pass*, NAT.'L. L. REV., (Feb. 4, 2020) https://www.natlawreview.com/article/updated-it-s-d-j-vu-all-over-again-washington-privacy-act-fails-to-pass.
[111] *See Washington*, *supra* note 107, § 19.375.020.
[112] *McCray*, *supra* note 108.
[113] *See Taneja*, *supra* note 109.
[114] *Id*.

Below is a description of default settings, in which the author posits that opt-in default settings are best for facial recognition data collection. The section will describe some social theories behind "nudging" and why it is important for legislatures and even social media companies who write these privacy policies to consider the kind of language they contain.

A. Default Settings

The difference between an opt-in and opt-out setting is quite nuanced but creates drastic differences in the privacy implications for users. An opt-in setting occurs when a company or entity notifies the user that they would like to collect or use data, and essentially asks if one agrees. This differs from an opt-out setting, which by default allows the company or entity to collect data or information from the individual unless they go to their settings and select the option to not allow this type of collection.

According to the FTC, opting-out means the user may limit the extent that the company can provide their personal information, and if a user neglects to opt-out the first time he or she receives a privacy notice, it is never too late.[115] Despite this particular article referring to financial data and privacy that citizens are afforded under the Fair Credit Reporting Act ("FCRA") and the Gramm-Leach-Bliley Act ("GLBA"), the definition is still applicable in this instance because biometric data is still personal information[116] to which a user should have the right to protect.

[115] Federal Trade Commission, *Privacy Choices for Your Personal Financial Information*, (last visited Sept. 22, 2020), https://www.consumer.ftc.gov/articles/0222-privacy-choices-your-personal-financial-information.
[116] *See* the CAL. CIV. CODE § 1798.100 (2018) (defining Biometric information that includes "any data that contains identifying information"); *see also* DANIEL J. SOLOVE AND PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 794 (Wolters Kluwer eds., 6th ed. 2018) (noting that personally identifiable information ("PII") is the basis for all privacy law, which regulates "the collection, use and disclosure of PII and leaves non-PII unregulated").

Protection "by default [would] require ensuring mechanisms are in place within the organization to ensure that, by default, only personal data [ ] that is necessary for"[117] a prior, specifically identified purposes, is collected and remains within the organizations system for a limited period. This type of limited data collection and storage mirrors the international standards proposed within the European Union's privacy legislation.[118] Today companies collecting and tracking users' personal data such as emails, phone numbers, search bars, and website history as part of target ad-marketing campaigns is common place.[119] There is a stark difference, however, between collecting the aforementioned data and facial or other biometric identifiers. The difficulty in attempting to permanently unsubscribe from an email list should be an indication of the concerns users should have regarding unsubscribing or opting-out of biometric collection. Creating a new email or putting a phone number on the 'do not call 'list is possible; however, creating a new face or altering biometric identifiers is almost impossible. Biometric data poses heightened risks because of its uniqueness to the individual and the fact that the full ramifications of biometric technology are not yet known,[120] which provides support for state legislators to initiate and pass protective measures for citizens' data now.

B. The Relevance of Nudging to Opt-in Versus Opt-out Settings

The key to understanding the relevance of opt-in versus opt-out settings comes with the term known as "nudging." Nudging is something that has come to be "understood as approaches

[117] Michael Monajemi, *Privacy Regulation in the Age of Biometrics That Deal with a New World Order of Information*, 25 U. MIAMI INT'L & COMP. L. REV. 371, 389 (2018).
[118] *See id.*, at 388.
[119] *See* Leslie K. et al., *Ads That Don't Overstep*, HARV. BUS. R. (Jan.-Feb. 2018) https://hbr.org/2018/01/ads-that-dont-overstep ("[U]sers regularly shar[e] personal data online and web cookies track[] every click, marketers have been able to gain unprecedented insight into consumers . . . " allowing targeted ads to become the future of marketing). The article highlights the eeriness of companies targeting their costumers searches including an expose where target sent maternity coupons to a teenage girl whose family was unaware of her predicatment. *Id*.
[120] *See BIPA, supra* note 67, § 14/5 (c), (f).

that steer people in certain directions while maintaining their freedom of choice."[121] Further, nudging is "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives."[122] The term "choice architecture" generally refers to strategically formulating choices that cause individuals to make specific decisions.[123] There are several different types of nudges, but in this context, we will refer to the proposed default rule as a nudge. The state legislature would have to be conscious of the potential bias it may impose on social media users through the idea of choice architecture. Despite this risk of bias, however, requiring social media websites to explain why users should grant them access to their face templates seems like it would be worth the risk.

Technology is everywhere and it arguably "organizes the world for us – subtly shaping the ways that we make sense of it."[124] Social media companies should be required to have default settings that give users the ability to have true freedom of choice—a nudge in the right direction. Lauren Willis argues that "the use of a default scheme from which consumers can opt out is premised on three key assumptions."[125] The paper discusses the problem that any "default will be "sticky," that "consumers with a true preference for the opt-out position. . . will opt-out," and "where a firm opposes the default position . . . [it] will be forced to explain it in the course of trying to convince consumers to opt-out, resulting in well-informed decisions by consumers."[126] It is important to understand the differences between the ideas of language being too sticky or slippery.

---

[121] Cass. R. Sunstein, *Do People Like Nudges?*, 68 AMIN. L. REV. 177, 177-78 (2016).
[122] Michal Lavi, *Evil Nudges*, 21 VAND. J. ENT. & TECH. L. 1, 4 (2018) (quoting RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH AND HAPPINESS 6 (2008)).
[123] *See* Anuj C. Desi, *Review Essay: Libertarian Paternalism, Externalities, and the "Spirit of Liberty,"* 36 LAW & SOC. INQUIRY 263, 268 (2011) ("Choice architecture is premised on the notion that for many decisions, context matter. . . framing choices should be made consciously to help people maximize their own interests.").
[124] *Lavi*, *supra* note 122, at 5.
[125] Lauren E. Willis, *Why Not Privacy by Default?*, 29 BERKELEY TECH L.J. 61, 66 (2014).
[126] *Id.* at 66–67.

The concept of a setting being "too sticky," refers to a situation where "consumers stick with the default even though they would opt out were they well-informed,"[127] and comes down to a lack of information. To avoid a setting that is too sticky, state legislation should require companies to include details on what information is being used, if it is being stored, the benefit to the user of having the setting on, and whether the company has the right to sell this data to a third-party. The goal for this kind of information would be that it is presented in a straightforward, easy to understand manner, rather than with nuanced and difficult language of which Willis warns against.[128]

The concept of a setting being too slippery means that "consumers opt out even though they would prefer the default position were they well-informed."[129] Again, this theoretical idea about default settings comes down to the level of information provided to the consumer when they have the option to allow the company to collect the data or not. Further, Willis argues that default settings are pointless without "robust competition over protect[ing] consumers['] privacy develops in the marketplace—a doubtful prospect—firms will generally prefer for consumers to be in the"[130] position, which best suits the companies' interests. This verbiage creates an opt-out setting but provides only minimal information. Even if companies are required to create these default settings, it is likely that consumers will not "necessarily be making well-informed decisions."[131] This idea comes down to what kind of language policymakers use to create these laws.

[127] *Id.* at 67.
[128] *Id.* at 66 ("Privacy law scholars have been skeptical of the idea that a notice-and-choice regime could produce robust individual decision making about personal data privacy.").
[129] *Id.* at 67.
[130] *Id.* at 67–68.
[131] *Willis*, *supra* note 125, at 68.

Policymakers at the federal as oppose to state level, typically will not address the full scope of default settings necessary to enable citizens to be well-informed and will likely not address the "granularity of opt-out choices."[132] Federal laws tend to be watered down and may be incapable of requiring the kind of specificity with which companies must inform their users.[133] In essence, it appears that policy makers do not have the capacity to address the nuances necessary to create default settings through law that would create the best privacy possible for their citizens. This is one reason why that this Comment proposes state legislation, which can provide the most comprehensive legislation without the red-tape posed by federal legislation.[134]

It is important to understand the users' economic behavior when it comes to our online presence. In particular, one survey found that 84% would rather receive targeted advertising in exchange for content than to pay for that content with money, but 93% of participants said "they would opt-in to a Don't-Track-Me position if given the choice."[135] This survey shows that a large majority of consumers will opt-in, if given the option, which will benefit companies. This does not, however, diminish the need to give them informed consent or adequacy of

---

[132] *Willis, supra* note 125, at 69.

[133] *See Hartzog, supra* note 7, at 1692; *see also* Stephanie Condon, *House Passes Watered Down NSA Reform*, CBS News (May 22, 2014 at 11:56 AM) https://www.cbsnews.com/news/house-passes-watered-down-nsa-reform-bill/; *see also* Kristi Pullen Fedinick et al., *Watered Down Justice*, NAT. RESOURCES DEFENSE COUNCIL 22 (Sept. 2019) https://www.nrdc.org/sites/default/files/watered-down-justice-report.pdf (a report discussing the federal bill on clean water that is not specific enough, making it arguably ineffective).

[134] For example, looking at a comprehensive federal bill that was passed in 2008 about Genomes this red-tape is evident. *See* National Human Genome Research Institute, *How a Bill Becomes Law*, (last updated May of 2020) https://www.genome.gov/about-genomics/policy-issues/How-Bill-Becomes-Law. The bill (1) is drafted, (2) introduced by the bill's representative in either the House or the Senate, (3) is submitted to committee, (4) the committee either has hearings or does nothing and the bill dies; (5) if the bill survives committee, a subcommittee will review the bill, conduct hearings and propose changes; (6) after hearings both the subcommittee and main committees will meet to discuss the marked up bill, and (7) with the amendments the committee must then report the bill to the floor of the full Congresssional chamber for voting; (8) the bill is then passed or not in that chamer of congress; (9) if passed the bill moves to the next chamber for voting and that chamber may form a conference committee and commit a report. *See id*. The final stage of the bill after the conference report is approved with recommendations for the final bill, the president must sign the bill into law or veto it. *See id*.

[135] *Willis, supra* note 125, at 80.

understanding the choices they have. Consumers deserve privacy, and though Willis's article is not specific to biometric data, it shows that data overall requires user consent and understanding.

Turning the attention back to social media companies, Facebook made a recent announcement about its policy of transparency that begins to track the kind of disclosures social media companies should regularly make. Facebook announced in September of 2019 that they would require all settings for new and existing users to be automatically turned off, requiring each user to "opt-in."[136] Despite this announcement, there appears to be confusion surrounding what kind of setting is actually in place. For example, ABC 6 News reported the default setting as an ability for users to opt-out of the facial recognition program within Facebook.[137] Opting-out versus opting-in is a crucial difference, as one indicates that the company may use the information unless the user tells them not to, versus the company having to ask permission to gather information in the first place.[138] The ABC 6 report and the recent court settlement highlight the confusion.

The current settlement "requires Facebook to automatically turn class members' facial recognition settings to 'off' and delete any face templates it may have . . . unless that individual affirmatively opts in . . . after receiving BIPA-complaint disclosures in a standalone document."[139] This settlement was reached in 2020 and Facebook's 2019 announcement that it

---

[136] Kate O'Flaherty, *Facebook Confirms 2 Billion Users Will Now Need to Opt In to Facial Recognition*, FORBES, (Sept. 4, 2019) https://www.forbes.com/sites/daveywinder/2020/09/13/these-120-mph-electric-flying-cars-to-get-virtual-force-field-security-acronis-teknov8-evtol-airspeeder-racing/#7d90fdde65f9.

[137] *See* Rodney Dunigan, *Facebook Allowing Users to Opt-Out of Face Recognition*, ABC6, (Sept. 4, 2019) https://abc6onyourside.com/on-your-side/facebook-allowing-users-to-opt-out-of-face-recognition (stating that "[t]he social media site is now allowing users to opt-out of the facial recognition feature.").

[138] See *Willis*, *supra* note 125, at 72 (stating the costs on consumers for opting out is much higher than the costs on the company). "Consumers must find the opt-out procedure, if one exists, and execute the steps for opting out, such as installing a program, changing settings, or completing an online form [and] [e]ven when [it] . . . is not onerous, [these steps] must be completed for each device." *Id*. The difficulty with finding how to unsubscribe through opting out is among the reasons for why this Comment argues that opt-in should be the required default.

[139] Allison Grande, *Facebook Users Share Details of Historic $550M Privacy Deal*, LAW 360 (May 11, 2020), https://www.law360.com/articles/1272036/facebook-users-share-details-of-historic-550m-privacy-deal.

will take measures towards opting-in and consent were yet to be realized. Facebook's reaction in light of pending litigation pressures from a single piece of state legislation demonstrates the benefit of creating legally cognizable harm surrounding biometric data for which the judiciary can provide relief. Judicial enforcement of one settlement is not enough, and action on behalf of several state legislatures in key market states is necessary to create much needed protections.

In conclusion, rather than giving companies an incentive to facilitate consumer exercise of informed choice, current default settings leave firms with opportunities to play on consumer biases or confuse consumers into sticking with or opting-out of the default. Opt-in default settings for biometric information are better because it allows users to control the information that companies collect about them in an ideal data protection regimes.[140] These kinds of regimes though, are essentially impossible where there are, what is called a "constructed environment."[141] This kind of environment is one where choices are constrained because they are specifically engineered to create feelings of being overwhelmed by options and forced into defaulted complacency.[142] This Comment argues that an opt-in setting for biometric data is ideal because of the literature surrounding the choice architecture and the virtual impossibility of creating an actual choice.

V. State Action Over Federal Inaction and Inefficiency

This section will argue that federal legislation is too slow, and the current oversight by federal agencies like the FTC is ineffective in preventing the misuse of users' biometric data. In particular the focus is on Facebook and its most recent FTC order. Next a discussion of how past

[140] Woodrow Hartzog and Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 BOSTON COLLEGE L. REV. 1687, 1695 (2020).
[141] *Id*.
[142] *Id*.

federal biometric bills have failed ensues. Finally, Part V concludes with a proposed outline of what state legislatures should include in their bills based off of Illinois' BIPA and the CPRA.

A. The FTC's Battle with Facebook

The FTC, as of September 15, 2020, appears to be "gearing up to file a possible antitrust lawsuit against Facebook . . . challenging the company's dominant position in social media."[143] In light of this potential prosecutorial action, Facebook's sway through lobbying groups and other tactics may be waning.[144] Currently, the only means for the federal government to pursue private companies like Facebook and TikTok for non-consensual use of an individual's data is through the Consumer Protection Bureau. As it stands to the Federal Trade Commission ("FTC") under the Bureau of Consumer Protection does not specifically list biometric data privacy as part of its duties.[145] This is further evidence of state legislatures' need to stand up rather than looking to the federal regulatory arm.

Given that there is no federal statute or regulatory body to either force companies to protect or enforce this protection with regard to biometric data, and the rise of litigation there is an obvious void in the regulatory scheme. The FTC has attempted to step into this gap through civil suits against companies suspected of violating consumer privacy rights generally. Most recently, the FTC has issued its second round of orders against Facebook.[146] This new round

---

[143] Brent Kendall et al, *FTC Preparing Possible Antitrust Suit Against Facebook*, THE WALL STREET J., (Sept. 15, 2020), https://www.wsj.com/articles/ftc-preparing-possible-antitrust-suit-against-facebook-11600211840?mod=hp_lead_pos2.

[144] The news of this potential prosecution does not imply that biometric privacy regulatory standards will be enforced and introduced to regulate private companies use of users' biometric data without their consent or express knowledge. This is evidenced by the fact that Facebook is still "in the process of making its case to the commission." *Kendall, supra* note 143.

[145] Federal Trade Commission, *Division of Privacy and Identify Protection*, (last visited Nov. 10, 2020) https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity.

[146] Press Release, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, (July 24, 2019) [hereinafter *FTC Press Release*] https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

penalizes Facebook for violating the first order in 2012.[147] Further, it requires Facebook to implement a series of measures to strengthen privacy protections and a $5 billion fine.[148] This 2019 order and fine come as a result of Facebook failing to follow the FTC's 2012 settlement order and not in light of new information or wanting Facebook to heighten its protections for consumers.[149] In light of the fact that this is the second time that the FTC has attempted to rein in Facebook's social-media regime, perhaps Facebook will follow the stipulations order.

According to Facebook's third quarter earnings call, CEO Mark Zuckerberg formally announced that Facebook "entered into a settlement with the FTC to make structural changes and build a rigorous privacy program that will set a new standard for our industry."[150] Zuckerberg appears to be taking this second round of FTC stipulations into account as the company has put in place new privacy policies.[151] The FTC stipulations require Facebook to establish a compliance officer to oversee the new privacy program as well as "increases outside oversight."[152] This order will remain in effect for twenty years, which means that the FTC will 'monitor' Facebook's actions to ensure compliance.[153] This stipulation included a new demand for several documents to be turned over to the Department of Justice for review, which could indicate that this time could be different from the 2012 warning.[154] The FTC requirements in the 2019 order demonstrate that the organization is attempting to more strictly regulate Facebook's

[147] *Id*.
[148] *See* FTC Press Release, *supra* note 146.
[149] *See* FTC Press Release, *supra* note 146.
[150] FACEBOOK, INC., Third Quarter 2019 Earnings Conference Call Transcript (Oct. 20, 2019) at 2.
[151] *See generally* Facebook Business, *Facebook's Commitment to Data Protection and Privacy Compliance with the GDPR*, (Jan. 29, 2018) https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr.
[152] *FTC Press Release*, *supra* note 146
[153] *Id*.
[154] Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief at 4, U.S. v. Facebook, Inc., No. 19-cv-2184 (D. D.C. 2019).

actions.[155] Specifically, Facebook must "exercise greater oversight" with their third-party vendors and refrain from using data obtained for two-factor authentication for advertising.[156] Most notably, the FTC asked Facebook to provide "clear and conspicuous notice of its use of facial recognition technology, and obtain affirmative express user consent."[157]

The Federal regulatory process takes too long, and as the FTC's multiple attempts to require Facebook to change demonstrates, is inefficient.[158] The FTC is in charge of protecting consumer data, yet it had to issue multiple 'warnings' and fines in order for the largest social media company Facebook to initiate a change to their policy, finally. This further demonstrates the need for state legislation, as the recent BIPA settlement shows that the legislation was better able to protect its resident consumers than the FTC was at protecting citizens as a whole.

Looking beyond the individual federal enforcement branches, the federal legislative process itself takes too long.[159] In 2017 Congress attempted to pass the "Consumer Privacy Protection Act of 2017."[160] The two key measures of this bill included an "amend[ment] to the federal criminal code [making] it a crime to intentionally and willfully conceal knowledge of a [data] security breach" resulting in at least $1,000 harm to any individual, and required "certain commercial entities to implement a comprehensive consumer privacy and data security program."[161] While this bill may have been a step in the right direction, it was proposed in 2017, "read twice, and referred to the Committee on the Judiciary," where it has remained.[162] Further, based on the language of the first requirement, the bill merely highlighted the risk of data

[155] *FTC Press Release*, *supra* note 146.
[156] *Id*.
[157] *Id*.
[158] *See supra* text accompanying note 134.
[159] *Id*.
[160] The Consumer Privacy Protection Act of 2017, S. Res. 2124, 115th Cong. (2017) (read twice and referred to S. Comm. on the Judiciary Nov. 14, 2017).
[161] *Id*.
[162] *Id*.

security breaches, and did not necessarily advocate for private companies' potential misuse of that data internally. Federal legislation takes too long to pass and to satisfy the majority of Congressional representatives tends to be overly broad or vague. Though "[t]he broader the default scope, the more easily it can be understood," it is less likely that it will "satisfy most consumer preferences."[163] Looking at the ability to satisfy consumer preferences in relation to federal regulations, most industries that are heavily federally regulated advocate for federal regulations because they know that it will allow the most loop-holes.[164]

B. Concerns About Lack of Uniform Law

If the nation begins to see sweeping state legislation providing for a private right of action, as Illinois' BIPA does, then there may be an argument that this would create a lack of uniformity of law. This idea of uniform law throughout the United States dates back to the framers' intention that the Federal Government have the power to issue such "laws as to create unity."[165] This concern would not be relevant, however, if states like New York and New Jersey, with robust market places follow California and Illinois's lead with regard to biometric privacy. In theory, the populational representation of these states would place pressure on social media companies to create a national standard that is heightened to the state with the most robust laws.[166]

---

[163] Lauren E. Willis, *Why Not Privacy by Default?*, 29 BERKELEY TECH. L. J. 61, 87 (2014).

[164] *See* CHRISTOPHER CARRIGAN AND CARY COGLIANESE, *George J. Stigler, "The Theory of Economic Regulation"* IN THE OXFORD HANDBOOK OF CLASSICS IN PUBLIC POLICY AND ADMINISTRATION 286 (Martin Lodge et al. eds., Oxford Univ. Press. 2015) https://tspppa.gwu.edu/sites/g/files/zaxdzs2001/f/Carrigan%20Coglianese%202015%20George%20J.%20Stigler.pdf .

[165] *See* Martin v. Hunter's Lessee, 14 U.S. 304, 347–48 (1816) (reasoning that the motive behind federal appellate review over state court decisions is necessary to "uniformity of decisions throughout the whole United States, upon all subjects within the purview of the [C]onstitution"). Despite the Supreme Court emphasizing the importance of "uniformity of law," this has been understood to refer only to a single and coherent interpretation of the Federal constitution. *See* Cornell Law School, *Martin v. Hunter's Lessee (1816)*, LEGAL INFO. INST. (last updated July of 2020) https://www.law.cornell.edu/wex/martin_v._hunter%27s_lessee_%281816%29.

[166] *See* Future of Privacy Forum, *Privacy Principles for Facial Recognition Technology in Commercial Applications*, 2 (Sept. 2018) (last visited January 2021) https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-

The first instance of this happening can be seen through Facebook's reaction to the CCPA. For example, with the passage of the CCPA, Facebook updated their websites code to recognize when a user is a California resident.[167] Then updated their specified settings to include what is called Limited Data Usage ("LDU").[168] Facebook is able to tailor their policies to the geo-location of their user's states regulatory requirements.[169] This Comment poses the theory, however, that if enough states with as robust a market as California begin to pass regulation requiring increased biometric data protection and notification, at some point the costs of the company changing each individual setting should outweigh the small benefit of the continued use of data in other portions of the United States.[170] Continually having to change their user policies and code to adapt to individualized state legislation would eventually meet the economic tipping point and ideally cause Facebook and other social media companies like TikTok and Instagram to make company-wide shifts.[171]

Though some concerns about a lack of uniformity of law have been posed, some scholars agree that a federal bill would be too watered down to create effective change.[172] Looking at the current global landscape, scholars have begun to argue that the European Union's ("EU") recent comprehensive legislation might spur the United States into introducing increased biometric data protections. This speculative measure, however, if done through federal legislation "seems

---

1.pdf ("All such companies should therefore support these Principles with the goal that by following these principles to collect, use, and share facial recognition data, they will deserve and retain consumer trust."); *see also Brennan*, *supra* note 99 (Advising businesses to watch for potential legislation changes given that the CCPA is so extensive and may encourage other states to "enact privacy legislation with differing requirements").

[167] *See O'Flaherty*, *supra* note 136.

[168] *See O'Flaherty*, *supra* note 136.

[169] *See* Kimberly J. Gold, Michael Galibois, and Vincent James Barbuto, *The Facial scan that launched a thousand laws: Biometric Privacy Legislation Trend Continues to Grow Nationwide*, L. BUS. RESEARCH, (Aug. 26, 2019) https://www.lexology.com/library/detail.aspx?g=973b23e5-04e8-4372-8f35-bae223ba5d3c ("The time and resources allocated to a refresh of policies and procedures could be far less costly than reacting after the fact to litigation spawned from one of the many biometric privacy laws on the horizon.").

[170] *See supra* note 166 and accompanying text.

[171] *Id*.

[172] *See Hartzog*, *supra* note 7, at 1692.

destined to be a watered-down version of the GDPR, [General Data Protection Regulation], given the trans-Atlantic differences in rights, cultures, commitments, and regulatory appetites" to have the faintest chance of passing.[173] This difficulty of passing comprehensive federal bills without watering down their potency further emphasizes the need for state legislation because states are better positioned to set the stringency that is best suitable for their respective constituents. A watered down, less effective and less specific version of biometric legislation at the federal level, though creating the "uniformity of law" the founders sought[174], is not what the states need to tackle reigning social media giants. These social media companies require specific and harsh legislation because these companies have gone largely unchecked until recently.[175] Further, the United States is now known globally for "accommodating the internet and digital technologies into [laws already in] existence and often poorly fitting legal structures."[176]

With the changes of both American's feelings towards privacy, where citizens are expressing increased levels of privacy concerns,[177] and rapid enhancement of facial recognition technology,[178] now is the time for legislators to step in. The new privacy norm is that about six

---

[173] *Id*.
[174] *See Martin*, 14 U.S. at 347.
[175] *But see* Cecilia Kang and Mike Issac, *U.S. and States Say Facebook Illegally Crushed Competition: Regulators Are Accusing the Company of Buying Up Rising Rrivals to Cement Its Dominance Over Social Media*, N.Y. TIMES (Dec. 9, 2020) https://www.nytimes.com/2020/12/09/technology/facebook-antitrust-monopoly.html ("Lawmakers and regulators have zeroed in on the grip that Facebook" maintain over social networking, "remaking the nation's economy").
[176] *Hartzog*, *supra* note 7, at 1693.
[177] Brooke Auxier ET AL., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH, (Nov. 15, 2019) https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (finding 62% of Americans believe that their "online and offline activities are being tracked and monitored by companies").
[178] *Facial Recognition: Top 7 Trends (Tech, Vendors, Markets, Use Cases & Latest News*), THALES GROUP https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition (Last updated: Feb. 20, 2021) ("All the software web giants now regularly publish their theoretical discoveries in artificial intelligence, image recognition, and face analysis to further our understanding as rapidly as possible."). This article also discusses interesting and beneficial uses of facial recognition technology; however, despite its benefits including assisting in finding missing children, this does not discount the argument to provide social media users with notice and require their express consent. *Id*.

in ten U.S. "adults say that they do not think it is possible to go through daily life without having data collected about them."[179] Despite this alarming number, this survey did not pose the specific question in regards to whether or not citizens are aware that their facial geometry is being scanned, tracked, and stored[180]—setting aside those users who have taken Facebook and Instagram to court. A citizen who lacks knowledge about how their data is used or even that it is being used, is not the same thing as providing passive consent, and social media companies should not continue unregulated in using and abusing users' biometric data.

Examples of specific acts that social media companies like Facebook, Instagram, and TikTok do without users' explicit knowledge includes tracking and creating user online profiles, and using those profiles to predict certain behaviors or attitudes, then selling this data compilation for profit.[181] The data is also being shared globally, not just within the specific state, or even region where that person is located. For example, "if Facebook places cookies on [an] EU citizens computer for tracking their usage history to provide personal advertisements to them," the General Data Protection Regulation passed in the European Union would protect that consumer.[182] This regulation likely would also extend to certain biometric identifiers that fall under these categories as well. A major component of this law "is meant to deter companies from overreaching their grasp on individual consumers."[183] The ultimate achievement of the EU's sweeping regulations, however, was likely not intended but may "force privacy standards all over the world to rise up to a set standard."[184]

---

[179] *Id*.
[180] *Id*.
[181] *See Monajemi*, *supra* note 117, at 391.
[182] *See Monajemi*, *supra* note 117, at 391.
[183] *Id*. at 391–92.
[184] *Id*. at 391–92.

While it is hopeful that this legislation will cause private companies to switch their United States privacy policies, it is not likely. Facebook and other social media companies, like TikTok, provide separate privacy policies dependent on what country you are in. It is much easier, however, to separate out privacy policies and practices by country, as opposed to on a state-by-state basis as the current United States landscape is transforming into. Companies now would not only have to provide separate privacy policies for each respective state, but coding within each sites algorithm that accounts for each user's geo-location, then the respective biometric data privacy statute. At what point does this become too much work? Alternatively, looking at this from a practical business perspective, at what point does the risk of litigation outweigh the potential profits that companies may gain from using these data points?[185]

C. Overview of Proposed Legislation

This Comment proposes state legislation, similar to both Illinois and California, that requires all social media companies to provide users with a simple, clear, outline of how their biometric data has been used, if it has been stored, how long it will be stored, the method for deleting and protecting this data, and allow each user the option of opting-in to the companies use after being fully informed. The legislation would not specifically name Facebook but would provide users with seeking a remedy for the conduct of Facebook within their given state of residency. Affirmative consent is important as opposed to passive consent, which is represented by merely clicking "I Agree" when a user first creates a profile. The idea of citizens working together to demand change from a company is known as market pressure. In theory, this could work, but in reality this is impractical. Arguments for market pressures to force transparency

[185] *See Prescott*, *supra* note 11.

and increase competition have been proposed,[186] but this Comment will focus on the state legislatures ability to protect citizens.

Specifically looking at the importance of statutory damanges it is important to highlight a hallmark privacy case *Clapper v. Amnesty International.*[187] The Court in this case held that the plaintiffs had no standing to sue because they lacked proof of an injury.[188] Given that proving the injury is such a high burden, this Comment proposes statutory damages to relieve some of the burden of proving the exact amount claimed and encourage attorneys with contingent fees to take these cases. Specifically, the class actions against Facebook and TikTok demonstrate the kind of high settlements that cause actions to be brought.[189] These class actions help to not only call to attention the wrongs of social media companies, but also should act as notice to state legislators in *other* states to allow private rights of actions for their citizens to seek relief.

Each of these state biometric data laws provides important details for state legislatures to keep in mind. First, that Illinois offers the best template for state legislatures to follow due to their expansive private right of action and statutory damage requirements.[190] Second, that as the Washington and Texas laws show a reliance on State Attorney Generals to bring cases will result in only the largest of violations being brought forward.[191] Third, though the CCPA provides a private right of action, it is limited in comparison to BIPA.[192] BIPA is the best template

---

[186] *See Welinder*, *supra* note 57, at 169 (arguing that "increased transparency of social networks . . . would empower users to demand that social networks conform to pre-existing privacy norms"). Though this author makes a valid point, this Comment argues that state regulation would be better than market pressures through the unlikelihood of increased competition.
[187] 568 U.S. 398, 410 (2013).
[188] *Id*.
[189] *See Holmes, supra* note 38; *see also In re Facebook* at *7.
[190] *See* §20 (1) – (4), 740 ILL. COMP. STAT. ANN. 14/20.
[191] *See Hunton, Andrews Kurth, LLP, supra* note 105; *see also McCray, supra* note 108 and the broad security exception permitted under Washington's biometric statute.
[192] *See* Moran Lewis, *Preparing For The CCPA Private Right Of Action For Certain Security Incidents - Morgan Lewis Practical Advice On Privacy: Guide To The CCPA*, J.D. SUPRA, LLC (Jan. 6, 2020) https://www.jdsupra.com/legalnews/preparing-for-the-ccpa-private-right-of-12835/ (The CCPA grants a "limited private right of action").

primarily due to the fact that it has demonstrated its strength in the recent settlement agreement against Facebook—the industry leader for social media companies.[193]

While the world watches to see what effect the European Union's data protection and "privacy law [has] in the next few years in countries such as the US and China because of the GDPR on their business[es]," [194] this article hopes to see pressure from increased state legislation push social media companies into compliance with a national, top-notch standard of notice and consent. Monajemi suggests that the increased privacy requirements will place pressure on companies to shift privacy practices but argues that this pressure will be felt by federal rather than state governments to meet the EU's muster.

VII. Conclusion

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society.[195]

Justice Brandeis's words are especially applicable today with the rapid changes and advancements in facial recognition technology and social media's use of it. We as a society

---

[193] *See generally* Nikole Davenport, *Smart Washers May Clean Your Clothes, But Hacks Can Clean Out Your Privacy, And Underdeveloped Regulations Could Leave You Hanging On A Line*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 259, 295 (Spring 2016) (the potential for civil liability should act as a deterrent to "manufacturers whose policies, or lack thereof, allow data breaches to occur [because they] will not only face the potential wrath of the FTC, but also from the plaintiffs' class action bar"). Though this journal article does not advocate for BIPA as a superior statute in regards to facial recognition technology, it advances the important opinion that threat of civil litagtion may cause adequate deterrence from lacks privacy regulation adherence by private companies. *Id*. Therefore, this proposition would lend support to the idea that private right of action, and more specifically, one as broad as BIPA would provide the most comprehensive protection for consumers. *See also* Lori Tripoli, *Resurgent BIPA More Than Second Fiddle To CCPA?*, COMPLIANCE WEEK (Feb. 21, 2020 11:36 AM) https://www.complianceweek.com/data-privacy/resurgent-bipa-more-than-second-fiddle-to-ccpa/28481.article ("law's reach has turned out to have been more extensive than some may have anticipated. 'Many companies—especially in the technology sector—have been targeted for allegedly violating Illinois' biometrics law even though they maintain no physical presence [or] operations within the state,' Rosenthal notes."). Further, the Tripoli article articulates that though the CCPA is broader in its applicability to more businesses, companies should be wary of disregarding the potency of BIPA. *Id*.

[194] *See Monajemi*, *supra* note 117, at 392.

[195] Warren and Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

must "define anew" the exact nature and extent of the extent of protections offered to U.S. citizens, and state legislatures are best positioned to strike.

Pressure continues to mount on social media companies. From the recent settlement with Facebook to the passage of the CCPA and flood of lawsuits that followed, the time for regulation is now. These judicial settlements and increased use of the judiciary shows that the regime of unrestricted, unauthorized access to our biometric data is ceding. State legislation is the best method for protecting citizens and social media users from unwanted biometric data scans and storage of this data because state legislatures do not face the same pressures from powerful lobbying groups nor campaign donations that Congress may face. State legislatures are also able to create more exacting laws with expediency in proposal, adoption and implementation.

Moving state-by-state appears to be working as evidenced by the flood of litigation California has seen with the CCPA coming into effect this year, and the increased pressure on the FTC to act against Facebook with the settlement from BIPA. Therefore, other states should adopt similar legislation to force social media companies to make national changes, rather than regional exceptions in their respective privacy policies and algorithms. Protection of biometric data is a new right, which demands recognition and protection by state legislators.