A Taxonomy of Legislative Approaches to Face Recognition in the United States

Jameson Spivack (Georgetown Center on Privacy and Technology)
Clare Garvie (Georgetown Center on Privacy and Technology)

INTRODUCTION: POLICE FACE RECOGNITION IN THE UNITED STATES

On December 25, 2015, Florida resident Willie Allen Lynch was arrested for selling fifty dollars' worth of crack cocaine to two undercover Jacksonville sheriffs three months earlier. The only thing tying Mr. Lynch to the crime was a face recognition search comparing photographs the officers had taken of the drug sale to the county's mugshot database. The search returned five possible matches—Mr. Lynch and four other suspects. Mr. Lynch and his defense attorney were given no information about the use of face recognition: its accuracy, potential biases, or even a list of the other possible suspects. Despite this, Mr. Lynch, who maintains his innocence, was sentenced to eight years in prison.[1]

1 *See* Lynch v. State, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018). For an overview of how face recognition was used in the case, *see* Lynch v. State, No. SC2019-0298 (Fla. Sup. Ct. 2019), *Amici Curiae Brief in Support of Petitioner*, *available at* https://www.aclu.org/sites/default/files/field_document/florida_face_recognition_amici_brief.pdf. The lower court's decision was affirmed on appeal, and the State Supreme Court determined it did not have jurisdiction to hear the case. Lynch v. State, SC2019-0298 (Fla. Sup. Ct. 2019).

Police use of face recognition is pervasive, affects most Americans, and, until very recently, has persisted under a widespread lack of transparency, oversight, and rules governing its use.[2] Police departments across the United States have deployed face recognition technology in thousands of criminal investigations since as early as 2001.[3] At least one agency has also used face recognition to identify protesters,[4] and by 2016, one quarter of the nearly eighteen thousand agencies across the country had access to a face recognition system.[5] Because thirty-one states allow police searches of DMV databases, more than half of all American adults can be identified through police face recognition simply by having a driver's license.[6] Many police departments have also used Clearview AI's face recognition service, which has amassed a database of an additional three billion images scraped from Facebook, Instagram, Twitter, Venmo, YouTube, and elsewhere.[7]

In 2016, the Government Accountability Office (GAO) published an extensive report on the use of face recognition by the FBI.[8] It made recommendations to increase transparency, enhance privacy protections, and better test the accuracy of their systems to guard against misidentification. This and many other reports have highlighted unique risks posed by police face recognition use:

- **Face recognition poses a threat to privacy.** Under the Fourth Amendment of the US Constitution, the right to privacy extends beyond the home, protecting "reasonable expectations of privacy" in some public settings and activities.[9] Face recognition gives police the power to conduct identity-based surveillance and the ability to scan and identify groups of people in secret, as well as to track someone's whereabouts through a network of security cameras. Without a warrant, this power may violate the Fourth Amendment, interpreted in the Supreme Court's 2018 decision in Carpenter v. United States as including a right to privacy in our movements across time and space.[10] The enrollment of most American adults into biometric databases used in criminal investigations represents an unprecedented expansion of law enforcement access to personal data, to which the American public did not consent.[11]

---

2 For an overview of the state of face recognition and laws governing its use, see Clare Garvie, Alvaro M. Bedoya, and Jonathan Frankle, "The Perpetual Line-Up: Unregulated Face Recognition in America," Georgetown Law Center on Privacy & Technology, (October 18, 2016): 25, 35, https://www.perpetuallineup.org/report.

3 *See* Pinellas County Sheriff 's Office, *Florida's Facial Recognition Network* (Mar. 26, 2014), *available at* https://drive.google.com/file/d/0B-MxWJP0ZmePX1QwTjltQkdVX0U/view?usp=sharing (indicating 2001 as the start date for the Sheriff Office's system).

4 Geofeedia, *Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots* (obtained by ACLU Northern California Oct. 11, 2016), *available at* https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

5 *See supra* note 2, at 25. This is a conservative estimate—the actual number is likely much higher. Prior to being terminated by the Attorney General's Office, all law enforcement agencies in the country were able to request searches of the Vermont driver's license face recognition system. *See ACLU Demands Immediate End to DMV Facial Recognition Program*, ACLU-VT (May 24, 2017), www.acluvt.org/en/press-releases/aclu-demands-immediate-end-dmv-facial-recognition-program.

6 *See Statement of Clare Garvie, Senior Associate, Center on Privacy & Technology at Georgetown Law before the U.S. House of Representatives Committee on Oversight and Reform* (May 22, 2019), 5, *available at* https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-GarvieC-20190522.pdf.

7 See Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *New York Times*, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. Former Center technologist Jonathan Frankle cautioned against just such a tool in 2016. See Jonathan Frankle, "How Russia's New Facial Recognition App Could End Anonymity," Atlantic, May 23, 2016, https://www.theatlantic.com/technology/archive/2016/05/find-face/483962/.

8 Government Accountability Office (GAO), "Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy," May 2016, https://www.gao.gov/assets/680/677098.pdf.

9 U.S. Const. Amend. IV; Katz v. United States, 389 U.S. 347 (1967).

10 Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

11 *See supra* note 6, at 5–7.

- **Face recognition risks having a chilling effect on free speech.** The First Amendment of the US Constitution protects the right to free speech, assembly, and association.[12] As law enforcement agencies themselves have cautioned, face recognition surveillance has the potential to "make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition"—chilling our ability to participate in constitutionally protected activities.[13]
- **Searches may lead to misidentifications.** While the algorithms behind face recognition have improved significantly since 2001, misidentification is still a major issue. Low-quality images, edited photos, and unreliable inputs such as forensic sketches and "celebrity lookalikes" increase the odds that the wrong person will be investigated, arrested, and charged with a crime they did not commit.[14]
- **Face recognition may have a disparate impact on communities of color.** Communities of color are disproportionately enrolled in face recognition databases and targeted by surveillance.[15] In San Diego, for example, police have used face recognition technology and license-plate readers up to two and a half times more on people of color than expected by population statistics.[16] The technology performs less accurately on people of color, meaning the risks of the face recognition police use, and the mistakes it may make, will not be distributed equally.
- **The failure to disclose a face recognition search may deprive a defendant of due process.** The risks of misidentification and bias are not mitigated by a fair, transparent court process. Face recognition searches produce evidence that speaks directly to a defendant's guilt or innocence. Per the constitutional right to due process and the Supreme Court's decision in *Brady v. Maryland*, evidence must be turned over to the defense.[17] Yet as in Mr. Lynch's case, and indeed the vast majority of cases involving a face recognition search, this information is not disclosed.[18]

In response to growing concern over the risks that the use of unregulated police face recognition poses to our civil rights and liberties, legislators have begun introducing—and passing—face recognition bans, moratoria, and regulatory bills.[19]

---

12 U.S. Const. Amend. I.

13 International Justice and Public Safety Network (Nlets), "Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field," June 30, 2011, 2, https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf.

14 For a discussion of how face recognition is used in practice and its associated risks, *see* Clare Garvie, "Garbage In, Garbage Out: Face Recognition on Flawed Data," Georgetown Law Center on Privacy & Technology, May 16, 2019, https://www.flawedfacedata.com.

15 *See supra* note 2 at 56 (describing disproportionately high arrest rates of black Americans); *see* Grother, Ngan, & Hanoaka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, Nat'l Institute of Standards and Technology (NIST) (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf ("We found empirical evidence for the existence of demographic differentials in the majority of contemporary face recognition algorithms that we evaluated.").

16 *See, e.g.*, Automated Regional Justice Information System, *San Diego's Privacy Policy Development: Efforts & Lessons Learned*, 11, *available at* https://drive.google.com/file/d/1ZR2jjiLcBMUKnHTRk1ZC248NbFUqNRww/view?us p=sharing (indicating that black Americans were 1.5–2.5 times more likely to be the targets of police use of licence-plate readers and face recognition technology).

17 Brady v. Maryland, 373 U.S. 83, 87 (1963) (holding that the suppression of evidence that is material to the guilt or innocence of the accused violates his due process rights under the Fourteenth Amendment).

18 Most law enforcement agencies consider face recognition searches to produce "investigative leads" only, not probable cause to make an arrest. But in practice, face recognition matches are often not independently corroborated through additional investigative steps before an arrest is made. See sup. note 14.

19 This represents the general trend currently; some states introduced bills earlier. See, e.g., MD H.B. 1148 (2017).

PROPOSED AND ENACTED LEGISLATION

Generally, there have been three legislative approaches to regulating face recognition in the United States: complete bans, moratoria, and regulatory bills. Moratoria can be further broken down into two types: *time-bound moratoria*, which "pause" face recognition use for a set amount of time; and *directive moratoria*, which "pause" face recognition use and require legislative action—such as a task force or express statutory authorization—to supersede the moratoria. Most of these bills have covered all government use of face recognition, with particular attention given to limits placed on police use. This section focuses on police use as well.

Type of legislation	What it does	Examples
Ban	Complete shutdown of all face recognition use	**Enacted:** San Francisco, CA;[20] Cambridge, MA[21] **Proposed:** Nebraska[22]
Moratorium: time-bound	Face recognition use paused for a set amount of time	**Enacted:** Springfield, MA[23] **Proposed:** Maryland[24]
Moratorium: directive	Face recognition use paused, requires legislative action to supersede	**Proposed:** Massachusetts[25]
Regulatory bill	Regulates specific elements of face recognition, along a spectrum from narrowly focused to broader	**Enacted:** *California:* prohibited in conjunction with police body-worn cameras[26] (narrower) *Washington:* regulates numerous elements[27] (broader)

20 *See* Kate Conger, Richard Fausset, and Serge F. Kovaleski, "San Francisco Bans Facial Recognition Technology," *New York Times*, May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

21 *See* Jackson Cote, "Cambridge Bans Facial Recognition Technology, Becoming Fourth Community in Massachusetts to Do So," MassLive, February 27, 2020, https://www.masslive.com/news/2020/01/cambridge-bans-facial-recognition-technology-becoming-fourth-community-in-massachusetts-to-do-so.html.

22 *See* LB1091, "Adopt the Face Surveillance Privacy Act," Nebraska Unicameral Legislature, *available at* https://www.nebraskalegislature.gov/bills/view_bill.php?DocumentID=41387.

23 *See* Jackson Cote, "Springfield City Council Passes Facial Recognition Moratorium," *MassLive*, February 25, 2020, https://www.masslive.com/springfield/2020/02/springfield-city-council-passes-facial-recognition-moratorium.html.

24 MD S.B.857 (2020), *available at* http://mgaleg.maryland.gov/2020RS/bills/sb/sb0857F.pdf.

25 MA S.B. 1385 (2019), *available at* https://malegislature.gov/Bills/191/S1385.

26 CA A.B. 1215 (2019) (prohibited only until Jan. 1, 2023), *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215.

27 WA Engrossed. Subst. S.B. 6280 (2020), *available at* http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf.

A. Bans

The strongest legislative response is to ban the use and acquisition of the technology completely. Bans can focus on state use of face recognition, commercial or private sector use, or both. To date, only local municipal governments have implemented bans, concentrated in towns and cities in California and Massachusetts. As of July 2020, the following municipalities had banned face recognition: Alameda, California; Berkeley, California; Boston, Massachusetts; Brookline, Massachusetts; Cambridge, Massachusetts; Easthampton, Massachusetts; Northampton, Massachusetts; Oakland, California; San Francisco, California; and Somerville, Massachusetts.[28] A number of states proposed bans on face recognition during the 2019–2020 legislative session: Nebraska, New Hampshire, New York, and Vermont.[29]

City governments have passed bans following robust public dialogue about the risks and benefits of face recognition technology. They represent what is possible with a transparent, democratic process, and the power of proactive localities. In the words of the San Francisco city supervisor who sponsored the ban: "We have an outsize responsibility to regulate the excesses of technology precisely because they are headquartered here."[30] It is unclear at this point, however, whether face recognition bans will take hold at the local, state, or federal level. Some jurisdictions may also find the bans to be unintentionally overbroad, restricting uses of the technology deemed to be necessary or uncontroversial.[31]

B. Moratoria

Another strong measure that a legislature can take is to place a moratorium on the technology,[32] which has two forms: *time-bound* and *directive*.

---

28 *See* Peter Hegarty, "East Bay City Becomes Latest to Ban Use of Facial Recognition Technology," *East Bay Times*, December 18, 2019, https://www.eastbaytimes.com/2019/12/18/east-bay-city-becomes-latest-to-ban-use-of-facial-recognition-technology; *see* Tom McKay, "Berkeley Becomes Fourth U.S. City to Ban Face Recognition in Unanimous Vote," *Gizmodo*, October 16, 2019, https://gizmodo.com/berkeley-becomes-fourth-u-s-city-to-ban-face-recogniti-1839087651; see Nik DeCosta-Klipa, "Boston City Council Unanimously Passes Ban on Facial Recognition Technology," *Boston.com*, June 24, 2020, https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban; see ACLU of Massachusetts, "Brookline Bans Municipal Use of Face Surveillance," December 11, 2019, https://www.aclum.org/en/news/brookline-bans-municipal-use-face-surveillance; see sup. note 20; *see* Michael Connors, "Easthampton Bans Facial Recognition Technology," *Daily Hampshire Gazette*, July 3, 2020, https://www.gazettenet.com/Easthampton-City-Council-passes-ordinance-banning-facial-recognition-survaillance-technology-35048140; see Jackson Cote, "Northampton Bans Facial Recognition Technology, Becoming Third Community in Massachusetts to Do So," *MassLive*, February 27, 2020, https://www.masslive.com/news/2019/12/northampton-bans-facial-recognition-technology-becoming-third-community-in-massachusetts-to-do-so.html; *see* CBS SF, "Oakland Officials Take Steps Towards Banning City Use of Facial Recognition Tech," July 16, 2019, https://sanfrancisco.cbslocal.com/2019/07/16/oakland-officials-take-step-towards-banning-city-use-of-facial-recognition-tech; see sup. note 20; *see* Alex Newman, "Somerville Bans Facial Recognition Technology," *Patch*, June 28, 2019, https://patch.com/massachusetts/somerville/somerville-bans-facial-recognition-technology.

29 NE L.B. 1091 (2020), *available at* https://www.nebraskalegislature.gov/FloorDocs/106/PDF/Intro/LB1091.pdf; NH H.B. 1642 (2020), *available at* http://gencourt.state.nh.us/bill_status/billText.aspx?sy=2020&id=1202&txtFormat=pdf&v=current; NY S.B. 7572 (2020), *available at* https://legislation.nysenate.gov/pdf/bills/2019/S7572; VT H. 929 (2020), *available at* https://legislature.vermont.gov/Documents/2020/Docs/BILLS/H-0929/H-0929%20As%20Introduced.pdf.

30 See sup. note 20.

31 *See* Tim Cushing, "San Francisco Amends Facial Recognition Ban after Realizing City Employees Could No Longer Use Smartphones," *Techdirt*, December 20, 2019, https://www.techdirt.com/articles/20191219/18253743605/san-francisco-amends-facial-recognition-ban-after-realizing-city-employees-could-no-longer-use-smartphones.shtml. The article describes amendments to San Francisco's ban to permit employees to use the biometric lock feature on city-issued cell phones.

32 Moratoria have been used in surveillance policymaking in the past. For example, in 2013, Virginia placed a two-year moratorium on government use of drones. The purpose was to give lawmakers time "to work with law enforcement and other stakeholders to adopt reasonable regulations limiting the use of drones and assuring public participation in the oversight of their use." See ACLU, "Virginia House of Delegates and Senate Approve Two Year Moratorium on Drones," February 6, 2013, https://www.aclu.org/press-releases/virginia-house-delegates-and-senate-approve-two-year-moratorium-drones.

1. Time-bound moratoria

Time-bound moratoria stop virtually all use of face recognition for a predetermined amount of time.[33] The purpose of this pause is to give elected officials and the public time to learn about face recognition, reconvening later once the moratorium expires. At this point, legislators can decide if, and how, to regulate face recognition.

At the municipal level, in early 2020, Springfield, Massachusetts, placed a moratorium on face recognition until 2025.[34] At the state level, a 2020 bill introduced in the Maryland legislature would prohibit all public and private use of face recognition for one year.[35] The bill does not include any other provisions or directions, but rather states the moratorium "shall remain effective for a period of one year from the date it is enacted and, at the end of the one–year period, this Act, with no further action required by the General Assembly, shall be abrogated and of no further force and effect."[36]

Time-bound moratoria raise the possibility for public engagement and the future implementation of either a permanent ban or strong regulation. These bills prompt discussion within legislative committees—the members of which are often unfamiliar with face recognition—about the technology, including its potential harms. There is a risk, however, that if the legislature fails to act once the moratorium period is over, use of face recognition will recommence with no safeguards in place.

2. Directive moratoria

Directive moratoria temporarily stop face recognition use while explicitly instructing the legislature or other government officials to take additional steps. Often this entails the creation of a task force, working group, or commission organized by either the legislature or attorney general to study face recognition and recommend policy responses.[37]

A bill introduced in Washington state in 2019 proposed a moratorium on government use of face recognition technology while setting up a task force to study the technology. The task force would be composed of members of historically oversurveilled communities, and would deliver a report to the legislature about potential effects. The bill would also require the attorney general to provide a report certifying the tools in use did not contain accuracy or bias issues, as tested by an independent third party.[38]

---

33 Time-bound moratoria often have carve-out provisions for face recognition use during emergencies or exigent circumstances and in the case of missing children. Some also have carveouts for use in fraud detection by state driver's licensing departments.

34 Sup. note 23.

35 MA S.B. 0857 (2020), *available at* http://mgaleg.maryland.gov/mgawebsite/Legislation/Details/sb0857. Note: the original bill would prohibit government and private use of face recognition for one year. An amendment, discussed at a hearing for the bill, would eliminate the moratorium on private use.

36 Ibid.

37 Provisions creating working groups are often part of non-moratorium regulatory bills, which allow continued use of face recognition until the working group makes further recommendations.

38 WA S.B. 5528 (2019-2020), *available at* https://app.leg.wa.gov/billsummary?BillNumber=5528&Initiative=false&Year=2019. (Note that this bill is no longer under consideration.)

Directive moratoria can also pause face recognition use *until* the legislature passes certain laws. In contrast to the above example, in which decisions about future policy are left to the working group, this kind of moratorium sets minimum thresholds that future legislation must achieve.

For example, a bill introduced in Massachusetts in 2019 would place a moratorium on government use of biometric surveillance, including face recognition, "[a]bsent express statutory authorization." That authorization must provide guidance on who is able to use biometric surveillance systems, their purposes, and prohibited uses; standards for data use and management; auditing requirements; and rigorous protections for civil rights and liberties, including compliance mechanisms.[39]

At the federal level, the *Facial Recognition and Biometric Technology Moratorium Act of 2020* prohibits federal use of certain biometric technologies such as face recognition until Congress explicitly allows their use, with certain limitations. It also conditions federal grant funding to state and local agencies on their adoption of moratoria similar to that proposed in the federal bill.[40]

These bills encourage jurisdictions to research the full implications of face recognition use and engage with members of the public before enacting a more permanent law. Moratoria also limit the risk of reverting to status quo use once the time period is over. However, there is a risk that a task force or commission may not be representative of affected communities; may lack authority; or may be inadequately funded, restricting its effectiveness.[41]

C. Regulatory Bills

Regulatory bills seek to place restrictions on face recognition's use, rather than stop it altogether. Regulatory bills range along a spectrum from more narrowly focused (regulating only specific uses or other elements of face recognition) to broader (regulating more of these elements).

1. Common elements of regulatory bills

Face recognition bills propose a wide range of measures, including:

- **Task force or working group:** groups must study face recognition and make policy recommendations.
- **Requirements on companies:** face recognition vendors must open up their software to accuracy and bias testing; commercial users must get consent or provide notice of use, as well as allow data access, correction, and removal.

---

39 MA S.B. 1385 (2019), *available at* https://malegislature.gov/Bills/191/S1385.

40 *See* Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology (June 25, 2020), available at 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.

41 *See*, e.g., Governor Jay Inslee, *Letter To the Honorable President and Members, The Senate of the State of Washington* (Mar. 31, 2020), available at https://crmpublicwebservice.des.wa.gov/bats/attachment/vetomessage/559a6f89-9b73-ea11-8168-005056ba278b (vetoing a section of WA S.B. 620 (regulatory bill) that established a face recognition task force on the grounds that it was not funded in the budget).

- **Accountability and transparency reports:** implementing agencies must provide details on the face recognition tools they use, including how and how often, to elected officials. Some require reports before implementation, and many require ongoing reports.[42]
- **Implementing officer process regulations:** officers must receive periodic trainings, conduct meaningful reviews of face recognition search results, and disclose to criminal defendants that face recognition was used in identifying them.
- **Explicit civil rights and liberties protections:** such as prohibiting the use of face recognition to surveil people based on characteristics including but not limited to race, immigration status, sexual orientation, religion, or political affiliation.
- **Data and access restrictions:** such as prohibiting the sharing of face recognition data with immigration enforcement authorities, limiting federal access to face recognition systems, and prohibiting use on state driver's license databases.
- **Targeted bans:** prohibiting specific uses, such as live facial recognition, or in conjunction with body-worn cameras or drones. Face recognition use can also be limited by type of crime—for example, only to investigate violent felonies.
- **Court order requirements:** law enforcement must obtain a court order backed by probable cause (or, in some instances, only reasonable suspicion[43]) to run face recognition searches. Some bills more narrowly apply this requirement to ongoing surveillance or real-time tracking only.[44] This can also apply narrowly to law enforcement seeking face recognition data from private entities that have collected it, rather than law enforcement searches themselves.

2. Examples of regulatory bills

A narrower bill proposed in Indiana calls for a "surveillance technology impact and use policy," but includes no other restrictions.[45] In New Jersey, a proposed bill requires the attorney general to arrange for third-party accuracy and bias testing.[46] In 2019, the California legislature passed a law prohibiting "a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera."[47]

At the other end of the spectrum, broader regulatory bills address multiple elements of face recognition development and use. Though they address a wider range of concerns, this does not mean they necessarily address *all* legitimate areas of concern related to face recognition, or that the proposed rules are substantive or enforceable.

---

42 Some of these provisions are modeled on the federal Wiretap Act. See 18 U.S.C. § 2519, reports concerning intercepted wire, oral, or electronic communications, https://www.law.cornell.edu/uscode/text/18/2519.

43 ID H.B. 492 (2020), *available at* https://legislature.idaho.gov/sessioninfo/2020/legislation/H0492/.

44 *See*, e.g., sup. note 22.

45 IN H.B. 1238 (2020), *available at* http://iga.in.gov/legislative/2020/bills/house/1238.

46 NJ A.B. 989 (2020), *available at* https://www.njleg.state.nj.us/2020/Bills/A1000/989_I1.PDF.

47 CA A.B. 1215 (2019), *available at* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1215.

For example, in March 2020, Washington state passed a law that regulates numerous elements of face recognition.[48] The bill includes provisions like these: a pre-implementation accountability report documenting use practices and data management policies for any new face recognition systems; "meaningful human review" when face recognition is used in legal decisions; testing in operational conditions; face recognition service APIs made available for independent accuracy and bias testing; periodic training for officers; mandatory disclosure to criminal defendants; warrants for ongoing, "real-time" or "near-real-time" use; civil rights and liberties protections; and prohibitions against image tampering in face recognition searches.[49]

Regulatory bills seek to strike a balance between the benefits and harms of face recognition use. For example, while a separate privacy bill introduced in Washington in 2019 garnered industry support for its light-touch approach to regulating face recognition, it elicited criticism from privacy advocates for containing loopholes and providing inadequate enforcement mechanisms.[50] Narrowly targeted bills have a greater likelihood of passing through support from well-resourced law enforcement and company stakeholders, yet often fail to meaningfully protect against the true scope of possible harms.[51] Some advocates are also critical of regulatory bills, particularly more limited ones, for using up available political capital and possibly eliminating the chance of stronger regulation in the future.

CONCLUSION

In the past year, the United States has turned a significant corner in its approach to face recognition. There is now widespread agreement that regulation is necessary, even as lawmakers, advocates, law enforcement, and other stakeholders may disagree on exactly what that looks like.[52] The status quo—expansive, unregulated, secret face recognition use—is no longer acceptable.

---

48 *See* Mariella Moon, "Washington State Approves Stronger Facial Recognition Regulations," *Engadget*, March 13, 2020, https://www.engadget.com/2020-03-13-washington-facial-recognition-regulations.html.

49 Sup. note 27.

50 *See* Lucas Ropek, "Why Did Washington State's Privacy Legislation Collapse?," *Govtech*.com, April 19, 2019, https://www.govtech.com/policy/Why-Did-Washington-States-Privacy-Legislation-Collapse.html.

51 *See*, e.g., Ban Facial Recognition (https://www.banfacialrecognition.com), a widely supported petition site calling for a complete ban on police face recognition use.

52 This includes both Republican and Democratic lawmakers, as well as face recognition vendors and law enforcement officials. *See*, e.g., Shirin Ghaffary, "How to Avoid a Dystopian Future of Facial Recognition in Law Enforcement, *Vox*, December 10, 2019, https://www.vox.com/recode/2019/12/10/20996085/ai-facial-recognition-police-law-enforcement-regulation; *see*, e.g., Brad Smith, "Facial Recognition: It's Time for Action," *Microsoft on the Issues*, December 6, 2018, https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/; *see*, e.g., Pat Garrett, "Facial Recognition Technology," Washington County Sheriff, Oregon, June 10, 2020, https://www.co.washington.or.us/sheriff/CrimePrevention/facial-recognition-technology.cfm.