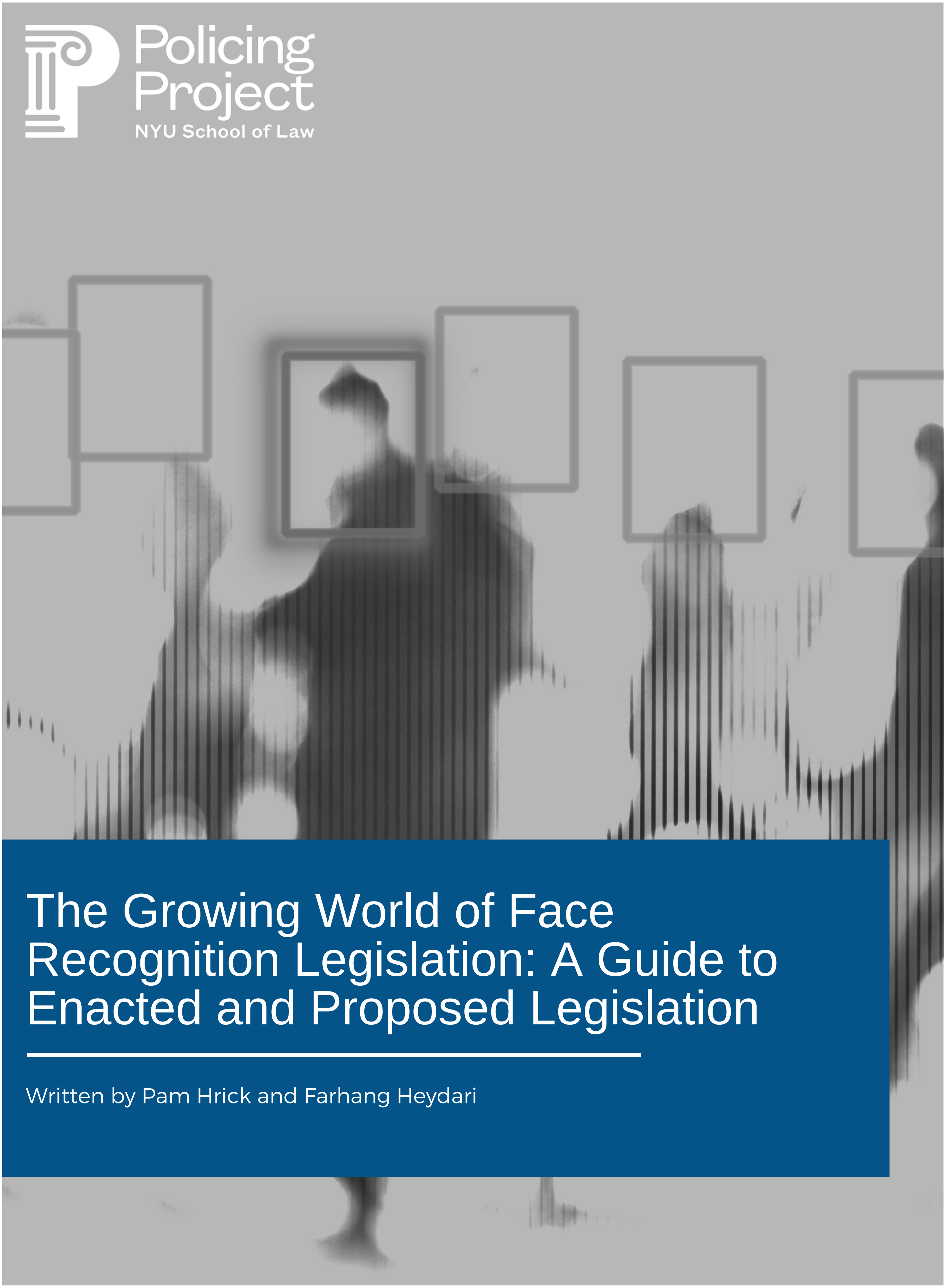
Policing Project
NYU School of Law



The Growing World of Face Recognition Legislation: A Guide to Enacted and Proposed Legislation

Written by Pam Hrick and Farhang Heydari

ABOUT THIS REPORT

This report was prepared by the Policing Project at New York University School of Law, a nonprofit organization that partners with communities and their police to promote public safety through transparency, equity, and democratic engagement. For more information, please visit **policingproject.org**.

Pam Hrick is an attorney and former junior research scholar at the Information Law Institute at NYU Law.

Farhang Heydari is the Executive Director at the Policing Project at NYU Law.

INTRODUCTION

As face recognition technology (FRT) advances and spreads across the country, many have raised a variety of concerns about its deployment – from inaccuracy and potential racial disparities, to secretive and inappropriate use by law enforcement. Some have argued that particularly in the hands of law enforcement, FRT raises the specter of surveillance of political activities, protests, and engagement in other protected forms of expression and association.

Although at present FRT remains largely unregulated, an increasing number of government actors at the local, state, and federal levels have begun taking steps towards directly or indirectly constraining the use of FRT. Our review has found a wide variety of enacted and proposed legislation across the U.S. and Canada that, broadly speaking, proceeds on three (at times overlapping) dimensions:

1. General regulations that ban, pause, or study FRT;
2. Operations-based regulations that control how FRT is deployed; or
3. Data-based regulations that restrict the images used to operate FRT.

As public calls for regulation of FRT increase, we thought communities and governments might benefit from a broader understanding of the measures being adopted or proposed. Although not meant to be exhaustive, we describe many of the major categories of restrictions below (often with links to legislative measures). Although described separately, many laws contain provisions from multiple categories. Our goal is not to suggest that proper regulation should draw on only one category or another; rather, any jurisdiction considering regulating FRT may well want to consider a combination of these requirements that strikes the appropriate balance.

The proceeding article catalogs and describes laws and policies across the following categories:

1. General FRT / Surveillance Regulation:
- Complete Bans on FRT Use
- Partial Bans on FRT Use
- Moratoria on FRT Use
- Requiring Democratic Approval Prior to Acquisition or Use of Surveillance Technology
- Studies and Task Forces

2. Operation-Focused Regulation of FRT:
- Transparency in Use & Impact Assessments
- Accuracy Requirements
- Court Orders & Cause Standards
- Notice & Consent Requirements
- Limits on Using FRT-Generated Evidence
- Reporting Requirements

3. Data-Focused Regulation of FRT:
- Protections for Biometric Data
- Restrictions on Probe Images
- Restrictions on Target Database

GENERAL FRT /SURVEILLANCE REGULATION

This type of regulation is targeted at FRT (the software / algorithm that identifies an individual by their face) and places conditions on (or barriers to) its use.

Complete Bans on FRT Use

Some jurisdictions have already made the determination that FRT simply should not be used, specifically implementing a complete prohibition on its use by state actors. Three cities – San Francisco, Oakland, and Somerville (Mass.) – have recently passed ordinances banning the use of FRT by city officials, including law enforcement. Two other cities – Berkeley (Cali.) and Cambridge (Mass.) – are actively deliberating such a ban. Minneapolis may soon follow suit, as one City Councilor has recently stated he is "considering" a similar ban. At the state level, one Michigan bill (SB 342, Sens. Lucido (R) and Chang (D)) proposes to ban law enforcement use of FRT or information obtained from FRT use, while proposed legislation at the federal level (HR 3875, Rep. Tlaib (D)) would prohibit the use of federal funds to purchase or use FRT.

Partial Bans on FRT

Short of a complete ban, various jurisdictions are considering or have enacted prohibitions on the use of FRT in certain locations or on specific classes of individuals. At the federal level, the No Biometric Barriers to Housing Act (HR4008; Rep. Clarke (D) and others) would prohibit the use of biometric recognition technology, including FRT, in certain federally-assisted dwelling units. Two New York bills (A06788, Asm. Rosenthal (D) et al.; S05125, Sens. Montgomery (D) and Krueger (D)) propose something similar, prohibiting certain rental dwellings from requiring residents to use a smart access system. Contemporaneous New York bills would expressly prohibit FRT use by landlords on any residential premises (S05687, Sens. Hoylman (D) and Montgomery (D); A07790, Asm. Walker (D)).

A proposed Pennsylvania law (SB797, Sen. Phillips-Hill (R) and others) would prohibit an educational entity or third party from collecting biometrics on a student except as required by law. Another New York bill (A08373, Asm. Walker (D)) would prohibit the use of FRT on school premises. A recent Connecticut bill (HB5333, Rep. Zawistowski (R)) would have prohibited retailers from using facial recognition software for marketing purposes.

Moratoria on FRT Use

Legislators in Michigan, Massachusetts, and Washington have recently proposed placing a moratorium – a temporary ban for a set period of time – on state use of FRT. Two Massachusetts bills (S.1385, Sen. Creem (D); H.1538, Rep. Rogers (D)) would prohibit state use of any biometric surveillance system, including FRT, absent express statutory authorization which much satisfy certain enumerated criteria. A Michigan bill (HB 4810, Rep. Robinson (D)) would place a five-year moratorium on police use of FRT to enforce state and local laws. As introduced, two Washington bills (SB 5528, Sens. Hasegawa (D), Saldaña (D), Nguyen (D); HB1654, Reps. Ryu (D) and others) would place a moratorium on the use of FRT by state and local officials pending a report from the Attorney General, receipt of a task force report on the potential consequences of FRT use by governmental actors, and legislation on the basis of these reports setting restrictions on FRT use by government agencies.

It appears that Montreal became the first Canadian city to consider targeted action to constrain FRT when its City Council considered a motion this month to impose a moratorium on its use by police and other municipal services so "reasonable rules can be put in place." Following the disclosure of FRT use by the Toronto Police Service, the Canadian Civil Liberties Association has similarly called for a moratorium on the future use of FRT by police in that city for the time being.

Requiring Democratic Approval Prior to FRT Acquisition or Use of Surveillance Technology

Multiple legislative bodies across the United States, primarily at the municipal level, have enacted, proposed, or are contemplating regulations that create prerequisites for the acquisition and use ofsurveillance technologies such as FRT by government actors, including law enforcement. Much of this movement on democratic surveillance oversight is grounded in the advocacy of the ACLU to promote Community Control Over Policing Surveillance (CCOPS), including the organization's development of a model bill. Berkeley (Cali.), Davis (Cali.), Cambridge (Mass.), Seattle, and Yellow Springs (Ohio) are among the cities that have adopted ordinances creating democratic oversight of surveillance technologies. According to the ACLU, efforts to enact similar legislation are also underway in additional municipalities, including Charlottesville (Vir.), Evanston (Ill.), Madison (Wisc.), and Muskegon (Mich.).

At their core, these statutes provide an opportunity for public input regarding the use of specific surveillance technology and require that government actors obtaining approval by elected officials prior to acquiring or using surveillance technologies, including FRT. (As discussed in more detail below, these laws also include a series of operational requirements.)

At the state level, a bill (H.470, Rep. Rachelson (D)) is currently before the Vermont legislature that would require specific authorization from the General Assembly prior to the state or law enforcement using certain types of surveillance technology, including FRT.

Studies & Task Forces

Rather than taking direct legislative action, several states and municipalities have opted to study or propose to study automated decision-making, surveillance technologies (including FRT), and/or general privacy regulations that could implicate FRT use.

Legislators in both New York (S06623, Sen. Sanders (D); A08042, Asm. Vanel (D)) and New Jersey (AJR206, Asms. Conaway (D) and Zwicker (D)) have proposed creating task forces that would study the impact of using FRT in both of those states, reporting back to their respective legislatures and governors. Another New Jersey bill (AB5300, Asms. Conaway (D) and Zwicker (D)) would require the Attorney General to obtain independent third-party testing and auditing of commonly available FRT systems, followed by a report back to the legislature on the results.

Among a current spate of FRT-related legislation in Massachusetts, one bill (H.2121, Rep. Provost (D)) has proposed to create a task force to develop a uniform code for the use of body cams, including a prohibition on the use of FRT in conjunction with this technology.

In 2018, Vermont struck an "Artificial Intelligence Task Force" (H.378, Rep. Cina (P)) whose mandate includes making recommendations on the use of artificial intelligence in state government and state regulation in the artificial intelligence field. This year, both Hawaii (HRC 225; Rep. Lee (D)) and Texas (HB 4390, Rep. Capriglione (R) and others) have convened groups to examine and recommend laws in relation to privacy and the protection of personal information.

Finally, two New York bills (A06787, Asm. Wallace (D) and others; S05140, Sen. Kavanagh (D) and others) propose to direct the Commissioner of Education to study the use of biometric identifying technology (including FRT) in schools, while prohibiting schools from purchasing or using such technology until July 1, 2022.

OPERATION-FOCUSED REGULATION OF FRT

The second category of FRT-related legislation focuses on regulating FRT's actual operation.

Transparency in Use & Impact Assessments
Several legislatures are currently considering artificial-intelligence-specific pieces of legislation that would promote transparency in and/or set standards for the types of algorithms that are central to the functioning of FRT.

The Algorithmic Accountability Act of 2019 (S.1108, Sen. Wyden (D); HR2231, Rep. Clarke (D)), currently before both houses of Congress, would direct the FTC to require entities that use, store, or share personal information to conduct automated decision impact assessments and data protection impact assessments. The AI in Government Act of 2019 (HR2575, Rep. McNerney (D)) would require each federal agency to solicit public feedback in developing a governance plan concerning the agency's applications of artificial intelligence and make this plan publicly available online.

At the state level, a bill before the Washington legislature (HB1655, Rep. Hudgins (D) and others) would establish guidelines for government use and procurement of automated decision systems. The New Jersey Algorithmic Accountability Act (AB5430, Asm. Zwicker (D) and others) currently before that state's legislature would require certain businesses to conduct automated decision and data protection impact assessments.

Relatedly, many of the CCOPS-inspired legislation discussed above – Berkeley (Cali.), Davis (Cali.), Cambridge (Mass.), Seattle, and Yellow Springs (Ohio) – include requirements that law enforcement draft a use policy and present that policy to government officials in order to obtain authorization to acquire and use FRT. These use policies address topics such as the technology's purpose; authorized and prohibited uses, including the rules and processes required prior to use; who can access collected data and how; safeguards to prevent unauthorized data access; safeguards against any potential violation of civil liberties; how information collected may be accessed by the public; length of data retention; third-party data-sharing; training required for individuals authorized to use the technology or the data collected with it; and mechanisms to ensure the policy is followed and to monitor for misuse. The Bureau of Justice Assistance of the US Department of Justice has also issued a Face Recognition Policy Development Template for State, Local, and Tribal Criminal Intelligence and Investigative Activities.

Use policies are also contemplated by enacted or proposed legislation directed at biometric privacy. For example, two New York state bills (S01203, Sen. Ritchie (R); A01911, Asm. Gunther (D) and others) would require private entities in possession of biometric identifiers (including scans of face geometry) to develop a written policy establishing a retention schedule and guidelines for permanent destruction of the identifiers. This proposal mirrors an existing requirement under the Illinois Biometric Information Privacy Act.

Accuracy Requirements
Inaccuracy and racial disparities are frequently cited concerns when it comes to FRT, and for good reason. Numerous reports, research papers, and tests – including the First Report of the Axon AI & Policing Technology Ethics Board, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, and a 2018 test conducted by the ACLU – substantiate these concerns. Some legislation has aimed to address them by imposing accuracy requirements.

Legislation currently being drafted at the federal level but not yet introduced would require certain face recognition algorithms be audited by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST), the same government agency that currently operates the Face Recognition Vendor Test. Legislation could require, for example, that NIST set strict standards not permitting racial disparities in false positive and false negative rates, and require algorithms to meet minimum standards under a variety of conditions.

Washington state bills (SB 5376, Sen. Carlyle (D) and others; HB1854, Rep. Kloba (D) and others) would impose limits on FRT use as part of wide-ranging privacy legislation, including a requirement to verify the accuracy of FRT prior to use.

Court Orders & Cause Standards

Dating back many years, several jurisdictions have considered requiring judicial authorization or the existence of probable cause prior to state use of FRT being authorized. Maryland's Face Recognition Act (HB1148, Del. Sydnor (D)), introduced in early 2017 before being withdrawn, would have established probable cause standards – and required judicial authorization in certain circumstances – for law enforcement to run certain facial recognition searches. A failed 2002 bill (HB454, Del. Griffith (R)) in the Virginia state legislature proposed to prohibit localities and law enforcement agencies from using FRT prior to complying with certain criteria for a court order.

More recently, a New York State bill (A01692, Asm. Abianti (D)) currently under consideration would prohibit the state, state agencies and departments, and contractors doing business with the state, its agencies or departments from retaining facial recognition images or sharing such images with third parties without legal authorization by a court.

The Federal Police Camera and Accountability Act (HR3364, Reps. Norton (D) and Beyer (D)) would prohibit FRT being used on video footage obtained from police body cams and dashboard cams except with a warrant issued on the basis of probable cause.

In 2012, an investigative report by the provincial Information and Privacy Commissioner held that the province's Freedom of Information and Protection of Privacy Act prohibited the Insurance Corporation of British Columbia (a public body that issues license and identification cards) from using its facial recognition software to assist police with their investigations in the absence of a subpoena, warrant, or court order. The report was issued in the context of the Corporation offering assistance to police in the aftermath of a riot that broke out following the Vancouver Canucks Stanley Cup playoff loss.

Notice & Consent Requirements

In a variety of settings, legislatures are considering or have imposed notice and/or consent requirements that restrict FRT use.

At the federal level, the Congressional Commercial Facial Recognition Privacy Act of 2019 (S.847, Sen. Blunt (R)) would prohibit certain entities from using FRT to identify or track an individual without first obtaining affirmative consent, which involves "an individual, voluntary, and explicit agreement to the collection and data use policies" of an entity.

At the state level, proposed California legislation (AB1281, Asm. Chau (D) and others) would require a business using FRT to disclose that usage at its entrance and provide information about the purposes of its use. A bill before the Massachusetts legislature (S.1429, Sen. Montigny (D)) would increase the transparency around use of DMV photos for FRT purposes, including requiring notices to be posted at licensing offices regarding law enforcement searches of license and identification photographs through targeted face recognition. Washington state bills (SB 5376, Sen. Carlyle (D) and others; HB1854, Rep. Kloba (D) and others) would impose limits on FRT use as part of wide-ranging privacy legislation, including requiring consent from consumers prior to deploying FRT in physical premises open to the public.

In Canada, Alberta's Information and Privacy Commissioner opened an investigation in August 2018 under that province's Personal Information Protection Act (the provincial private sector privacy law) concerning the use of FRT without consent at shopping centers in Calgary. Canada's Privacy Commissioner opened a parallel investigation into the same issue under the federal Personal Information Protection and Electronic Documents Act (the federal private sector privacy law). Both investigations are ongoing.

Limits on Using FRT-Generated Evidence

In the state of Washington, HB1654 (Reps. Ryu (D) and others), originally a moratorium bill, has since been superseded by a substitute bill that simply provides a police officer may not use the results of a facial recognition system as the sole basis to establish probable cause in a criminal investigation. This requirement is similar to various police department policies, including that of NYPD, which state that the results of a face recognition search are meant to provide investigative leads and should not be treated as a positive identification. As Georgetown researchers write, "In theory, this is a valuable check against possible misidentifications . . . However, in most jurisdictions, officers do not appear to receive clear guidance about what additional evidence is needed to corroborate a possible face recognition match."

Reporting Requirements

Many of the CCOPS-inspired legislation discussed above - including Berkeley (Cali.), Davis (Cali.), Cambridge (Mass.), Seattle, and Yellow Springs (Ohio) - include periodic reporting requirements to public bodies after the technology is deployed. These periodic (often annual) reports provide information on matters such as how the technology has been used, the quantity of data gathered, the sharing of data (if any) with outside entities, geographic deployment, complaints (if any) about the technology, results of internal audits, information about violations or potential violation of use policies, requested modifications to the policies, data breaches, effectiveness, costs, and whether the civil rights or liberties of any communities or groups are disproportionately impacted by the surveillance technology's deployment.

A reporting requirement currently under consideration as part of a broader FRT policy in Detroit would require police to provide a weekly report to the police Board that includes the number of facial recognition requests fulfilled, the crimes the request were attempting to solve, and the number of leads produced from the FRT.

DATA-FOCUSED REGULATION OF FRT

FRT operates by comparing a probe image – an image of an individual – to images in a target database – a database of known faces, which can be either general (e.g., all DMV photos) or specific (e.g., mugshots of convicted felons). Various jurisdictions have sought to regulate both ends of this process.

Protections for Biometric Data

Not specific to FRT, many states have enacted or are considering enacting biometric protection legislation targeting private sector collection, use, and disclosure of biometric data, including photographs or facial scans that are integral to deploying FRT. Illinois, Texas, and Washington have enacted biometric-specific legislation that requires notice and consent for the collection and/or disclosure of biometric identifiers. Facebook is currently embroiled in litigation under the Illinois statute, facing a claim that it used FRT on individuals' photographs without their knowledge or consent.

Similar legislation has been introduced in several state legislatures, including Massachusetts (S.120, Sen. Creem (D)), New York (S01203, Sen. Ritchie (R); A01911, Asm. Gunther (D) and others), and Michigan (HB5019, Rep. Lucido). Notably, The California Consumer Privacy Act of 2018, which provides expansive privacy protections including for biometric data, comes into force on January 1, 2020.

Restrictions on Probe Images

Several jurisdictions have enacted or are considering legislation or policies to restrict the type of probe images that law enforcement may use. Broadly speaking, these laws fall into at least two different categories.

First, a variety of laws prohibit the use of FRT in conjunction with certain types of technologies, namely police body cameras and drones (or "unmanned aerial vehicles"). New Hampshire and Oregon, for example, prohibit the use of FRT in conjunction with body cams and/or video obtained from body cams. California's proposed Body Camera Accountability Act (AB1215, Asm. Ting (D)) would also expressly prohibit the use of FRT on police body cams. The federal Police Camera and Accountability Act (HR3364, Reps. Norton (D) and Beyer (D)) would require all federal officers to wear body cams while prohibiting the use of FRT in conjunction with those cameras. Finally, the federal Police CAMERA Act of 2019 (HR120, Reps. Cohen (D) and others) would authorize grants for the purchase of law enforcement body cameras, a condition of which would be limiting the use of FRT in conjunction with them to certain circumstances. It is also worth noting that the Axon AI and Policing Technology Ethics Board recently recommended that Axon not develop FRT for body cameras – a recommendation that Axon has adopted.

Similarly, laws prohibiting or restricting the use of FRT in conjunction with drones or "unmanned aerial vehicles" exist in Maine and Vermont, and have been proposed in New York (A04030, Asm. Englebright (D) and others; S06435, Sens. Ramos (D) and Salazar (D)) and Massachusetts (S.1447, Sen. O'Connor (R); S.1446, Sen. Moore (D) and others), among other places.

Second, an important substantive limitation on FRT, and one supported by the Policing Project, is limiting the types of crimes that may be investigated with FRT. In other words, for criminal investigations, limiting probe photos to serious felonies and prohibiting FRT use on low-level misdemeanors. This type of limitation was recommended by the Georgetown Law Center on Privacy and Technology, and is currently being considered for a U.S. Senate bill that has yet to be formally proposed. At the local level, a directive currently under consideration in Detroit would limit police use of FRT to specified violent crime (e.g., robbery, sexual assault, or homicide) and home invasion investigations.

Restrictions on the Target Database

In addition to limiting the types of probe photographs that may be used, numerous legislatures have enacted or are considering a variety of restrictions on target databases - the databases that law enforcement may use to identify a probe photograph.

First, a subject of recent media attention, a number of states have enacted legislation or regulations (a) prohibiting or restricting law enforcement access to such databases, or (b) restricting the use of FRT or collection of biometric data altogether. These states include Missouri, Hawaii, New Hampshire, Oregon, Vermont, and Washington. (However, notwithstanding the existence of this type of legislation in Vermont, it was recently reported that its license photograph database has been used by the FBI, as well as by Immigration and Customs Enforcement in recent undocumented immigrant raids.) The Canadian province of Saskatchewan also prohibits disclosure of its facial recognition software or information obtained using it in relation to license and identification photos to any other entity, including police, without a warrant or court order (except in the case of identity theft).

Short of prohibiting law enforcement from accessing these databases, the recently-introduced Facial, Analysis, Comparison and Evaluation (FACE) Protection Act (HR4021, Rep. Engel (D) and others) would prohibit a federal agency from using FRT on state or federal photo identification without a federal court order based on probable cause.

Another type of target-database restriction relates to the types of mugshots that law enforcement may use as part of their target database. The Georgetown Law Center on Privacy & Technology's Model Face Recognition Legislation includes provisions that would regulate police access to both identification photo databases and arrest photo databases for the purposes of FRT-assisted searches. Certain law enforcement agencies are already bound by such restrictions. Michigan State Police, for example, are required by law to delete mug shots and other biometric data of people who aren't charged or who are acquitted.

CONCLUSION

The need to regulate face recognition technology use is one of the most pressing legislative issues facing governments today. Existing and proposed measures demonstrate the wide range of available approaches to regulation, including absolute bans, carefully-crafted restrictions, and ongoing democratic accountability measures. In this article, we have aimed to provide a foundational understanding of these approaches.

Our hope is that with this information in hand, legislators and the broader public will be empowered to pursue regulatory options that are responsive to the needs of their communities and that sufficiently account for the potentially significant privacy and civil rights implications of FRT use.

CONTACT INFORMATION

Policing Project
NYU School of Law
40 Washington Square South
Suite 302
New York, NY 10012

Email: info@policingproject.org
Twitter: @policingproject
Facebook: /PolicingProjectNYU
Phone: (212) 992-6950

www.PolicingProject.org