SEPTEMBER 2021

Facial Recognition Technology

Responsible Use Principles and the Legislative Landscape

By James A. Lewis & William Crumpler

Facial Recognition Technology: Responsible Use Principles

The discussion of facial recognition technology (FRT) comes at a politically charged moment. Some of the concerns raised in the discussion of FRT are based on erroneous information. To address legitimate concerns, the use of FRT must be demonstrably consistent with constitutional protections, and this requires clear guardrails—laws, rules, and policies—for the use of FRT. These guardrails are best developed by Congress to provide consistent national rules.

The level of confusion and misinformation in the FRT discussion is astounding. Some of this is understandable given that the research literature is often opaque, but public discussion of FRT must be better informed. FRT is improving rapidly, and any critique based on data from even a few years ago runs the risk of being entirely wrong. Determining ground truth on issues of accuracy and bias—something that is currently in short supply—is essential for good policy.

Criticism of FRT is too often based on a misunderstanding about the technology. A good starting point to change this is to clarify the distinction between FRT and facial characterization. FRT compares two images and asks how likely it is that one image is the same as the other. The best FRT is more accurate than humans at matching images. In contrast, "facial analysis" or "facial characterization" examines an image and then tries to characterize it by gender, age, or race. Much of the critique of FRT is actually about facial characterization. Claims about FRT inaccuracy are either out of date or mistakenly talking about facial characterization. Of course, accuracy depends on how FRT is used. When picture quality is poor, accuracy is lower but often still better than the average human. A 2021 report by the National Institute of Standards and Technology (NIST) found that accuracy had improved dramatically and that more accurate systems were less likely to make errors based on race or gender. This confusion hampers the development of effective rules.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Some want to ban FRT, but it will continue to be developed and deployed because of the convenience for consumers and the benefits to public safety. Continued progress in sensors and artificial intelligence (AI) will increase availability and performance of the technologies used for facial recognition. Stopping the development of FRT would require stopping the development of AI, and that is neither possible nor in the national interest. This report provides a list of guardrails to guide the development of law and regulation for civilian use.

Guardrails

FRT needs to be embedded in a strong regulatory framework. There has already been substantial work in this area. Rules will vary by use case. These rules can be divided into three general categories: commercial use, general government use, and law enforcement use. The following section provides principles to guide the development of rules to ensure FRT's responsible use. One topic this report does not address is defense and intelligence use. These are already subject to legal and ethical guidelines that include substantial protections for U.S. persons and provide significant benefits to public safety.

Permissible Use: FRT can only be used in a manner consistent with constitutional protections for civil liberties and civil rights. The best way to ensure this is through legislation and regulation that outlines specific FRT uses in a manner consistent with those rights. For law enforcement, this could draw on the protections developed for other investigatory techniques, such as communications surveillance. Other government uses can also build the existing body of law regarding data use and retention. Rules will vary by use case, such as whether FRT is being used for authentication of identity, forensics, or surveillance. The use of FRT for commercial purposes does not create the same risks but points to the need for Congress to create national privacy legislation.

Transparency: Transparency means deciding when and how to notify the public that FRT is being used. The requirements for transparency will vary by use case and will be affected by decisions on what are "public" or "private" situations where people have a reasonable expectation of privacy. There is no domestic use case where transparency cannot be required. Transparency requirements could include annual reporting, public consultation, and making information publicly available on how FRT is being used. Regular reporting on use and impact statements are valuable in ensuring that use is consistent with law and regulation.

Consent and Authorization: The foundational element of public consent in a democracy is action by elected officials, legislatures, and by the courts. At the federal level, primary responsibility falls on Congress as the legitimate representative of the people. Congress needs to establish the rules for FRT, and the courts need to decide if these rules are consistent with constitutional protections and are being fairly applied. Some FRT uses will require the consent of the subject. This could be implied consent, as when you enter a store that is transparent about FRT use. Other uses may require a warrant or other court approval for use. Rules can clarify when a warrant is required for FRT use. At an individual level, ensuring that there are appropriate mechanisms to opt in or opt out of FRT use without penalty provide for consent. At airports, for example, a person should be able to choose to wait in line if they prefer.

Data Retention: One source of concern is that images collected for one purpose are then used for another without consent or transparency. There must be clear rules against this that define when images can be stored, for how long, and under what conditions any stored image can be used.

Autonomous Use: One area of concern is that FRT (and AI in general) will make decisions without human input. When used for authentication of identity, such as when accessing federal benefits or in border entry and departure processes, FRT can be autonomous as long as there is transparency in use, an ability

to opt out for those who choose to do so, and adequate mechanisms for oversight and redress. FRT use by Customs and Border Patrol in entry points is already regulated and a success story worth heeding. In law enforcement, FRT is not a silver bullet where results can be accepted without further investigation and analysis. Legislation should ensure this.

Redress and Remedy: Some FRT use cases raise problems similar to those encountered when "no-fly" lists were first employed. As with those earlier lists, the solution is to provide easily accessible processes for appeal and redress and to iteratively improve the technology. While an appeal to the courts is the ultimate remedy for redress, there should be administrative procedures that allow for the quick rectification of errors.

Oversight and Auditing: Concerns over the use of FRT can be addressed by appropriate oversight and auditing. The primary responsibility for this rests with elected officials and the courts. Each level of government that authorizes the use of FRT will need some oversight mechanism. In many cases, FRT use will need to be accompanied by some assessment of the effects on privacy, both before deployment and on a regular basis after deployment. Audits of system performance should also review and make information on accuracy public. Annual public reporting on use should be required as part of any deployment.

Algorithmic Review: Like any new technology, improvements in FRT are iterative. Between 2017 and 2021, error rates fell dramatically. This reflects improvement in the algorithms. Requiring agencies to frequently "refresh" the FRT they use to take advantage of new or improved algorithms is essential to further reducing error. Transparency about which algorithm is being used and its accuracy can help increase trust and incentivize performance. Since existing algorithms vary widely in performance, Congress may wish to establish accuracy thresholds (based on NIST's latest work) for sensitive applications.

Training Data: Some FRT uses AI and must be "trained" on huge data sets of images. Some of these data sets are created by "scraping" the internet to collect images of faces, usually without the owner's consent. This kind of collection is not illegal, but there is growing concern that it is unethical. Collection of training data should be subject to rules that require transparency and consent that allow for oversight in use.

> *In many cases, FRT use will need to be accompanied by some assessment of the effects on privacy, both before deployment and on a regular basis after deployment. Audits of system performance should also review and make information on accuracy public.*

Moving Ahead with FRT

If the goal is to simply block the use of any FRT, that goal is unachievable. For commercial and government uses other than law enforcement, people will value the convenience and efficiency FRT provides, leading to increasing demand. Local governments do not have the authority to ban federal use for defense, and Congress is unlikely to do so given the risk to public safety and national security. Increasing public concerns over crime and safety will also raise demand for FRT use among citizens.

Creating the rules and oversight for facial recognition is a necessary task and should be approached in ways that balance privacy concerns with public safety and convenience. FRT provides greater convenience

for consumers and improves public safety. As it continues to improve, its use will also increase. Once the confusion between FRT and facial characterization is discounted, the risks of use are small. These can be further minimized by putting in place the right guardrails.

This is not the first time that the United States has had to create a regulatory framework for a new technology. What would be best to avoid is a patchwork of regulations varying by state and city. Concerns about FRT have led a number of jurisdictions in the United States to create their own rules and regulations. In the absence of federal action, this trend will likely continue, leading to regulatory fragmentation and uncertainty, slowing innovation, and creating costs for consumers and public safety. There is already the example of a doorbell that uses FRT that is allowed in most states but cannot be sold in one because it violates that state's regulations. National legislation covering the different uses of FRT—commercial, governmental, and law enforcement—is the most effective approach.

This report's recommendations for a comprehensive national framework draw upon an examination of FRT legislation at the local, state, and federal level. The next section explores the legislative landscape of proposed and enacted FRT policies across the United States.

Facial Recognition Technology: U.S. Legislative Landscape

This section begins by surveying recent actions by policymakers at the federal, state, and local levels to regulate the use of FRT by government operators, before moving on to an examination of attempts by different jurisdictions to ban the technology's use by government agencies altogether. The report then proceeds to examine attempts to regulate and ban such use by commercial operators.

Regulation of Government Facial Recognition Use

The primary focus of regulatory efforts to date has been establishing rules to govern how government operators—and particularly law enforcement agencies—make use of FRT. There have been numerous efforts at the federal, state, and local levels to institute rules to guide how the technology is used and ensure it is deployed responsibly.

Research for this report identified three major pieces of legislation at the state level and nine at the local level that have been enacted to regulate the use of FRT. These are listed in Appendix 1, along with 20 proposed pieces of state legislation. The table also includes a proposed bill from the current Congress and five from the previous Congress that provide indicators of how federal lawmakers are likely to approach these issues in the near future.

These proposed laws range in scope. Some only attempt to govern certain narrow use cases, such as the application of facial recognition to body camera footage, while others attempt to form a comprehensive governance regime. The topics covered by these laws include the authorization and oversight of FRT deployments, restrictions on the circumstances under which the technology can be used, transparency requirements for operators, testing to gauge system performance, and requirements for human review.

AUTHORIZATION AND OVERSIGHT

One common goal of regulation is to establish new processes to authorize and oversee the deployment of government FRT systems. There are three primary ways that regulations seek to achieve this.

The first is requiring operators to seek permission from a legislative body before they can purchase and install a facial recognition system. Every city listed in Table 1, except for New York, has adopted this approach and requires agencies to obtain city council approval before procuring a facial recognition system.[1]

At the state level, Arizona's proposed legislation on surveillance technologies is the only current example of a bill that would mandate this approval process for both state and local authorities. Washington's law requires agencies to file a notice of intent with a legislative authority before procuring an FRT system. A notice requirement is not the same as requiring authorization, but the notification process provides municipal councils and state legislators the opportunity to act on proposed uses they find objectionable.

The second way of instituting oversight is to authorize only a small number of organizations to use facial recognition (usually these are the state police and the agency overseeing the state's registry of drivers' licenses and IDs). If any other agency wanted to conduct a facial recognition search, they would need to submit a request to one of the few authorized operators. This reduces the number of organizations in possession of facial recognition systems and makes it easier to establish a consistent approach to governing the technology's use. Recent laws passed by Massachusetts and Utah have taken this approach, requiring all local police departments to submit written requests to state agencies which then make a determination about whether to conduct the search on their behalf.

Finally, many jurisdictions impose judicial oversight by requiring law enforcement officers to obtain a warrant or a court order before using facial recognition. Massachusetts, for example, requires a warrant for any facial recognition searches used in criminal investigations. Kentucky and Louisiana are both currently considering legislation that would implement similar measures. At the federal level, two bills introduced during the 116th Congress (S.3284 and H.R.4021) would have created warrant requirements for facial recognition searches conducted by federal law enforcement.

Additional policies expand court authorization requirements to accessing data collected by facial recognition. A bill introduced in New York would require court authorization for any state agency or contractor to retain facial recognition images or share these images with a third party.

Some regulations only impose warrant requirements for ongoing surveillance and real-time identification. An example of this is Washington's facial recognition law, as well as legislation currently being debated in Minnesota. At the federal level, legislation introduced during the 116th Congress (S.2878) would similarly have required a warrant before federal law enforcement agents could use FRT to conduct ongoing surveillance.

Some states impose different standards depending on the origin of the images being searched. For example, proposed bills in Iowa, Kansas, and Michigan would require a warrant for FRT used in conjunction with a police body camera. Massachusetts is currently considering a proposal to ban the use of facial recognition on data collected by unmanned aerial vehicles unless authorized by a warrant. In Louisiana, a proposed bill would require a court order for all searches involving the state's drivers' license database (but not for searches involving arrest records). A stricter version of this is a proposed bill in New Hampshire, which would maintain the state's current ban on using facial recognition on drivers' license photos while allowing other databases to be searched after obtaining a warrant. The Justice in Policing Act of 2020 (S.3912) would have imposed similar requirements at the federal level.

1 Santa Clara, Lawrence, Pittsburgh, and Nashville allow limited exceptions to this requirement.

These three approaches are not mutually exclusive. Some jurisdictions use a combination to provide additional safeguards. Massachusetts, for example, both limits which agencies can conduct facial recognition searches and requires warrants before searches can occur.

USE RESTRICTIONS

One important goal for FRT regulations is to clarify the circumstances under which FRT can and cannot be used. Many regulations approach this question by explicitly listing the purposes for which government operators can use FRT and by banning uses falling outside of that scope. A proposed bill in Hawaii, for example, would only allow law enforcement agencies to use FRT to create a photo lineup for eyewitnesses or to compare surveillance photos against arrest records (but not state IDs).

Some states place restrictions on the types of offenses that FRT can be used to investigate. Utah, for example, only allows police to use FRT to support investigations into felonies and violent crimes. Louisiana and Massachusetts are currently considering bills that would institute similar limits. Other jurisdictions only implement these restrictions for certain kinds of FRT deployments, such as those qualifying as "ongoing surveillance." The initial version of a bill currently being considered in Maryland would only have allowed ongoing FRT surveillance to be used when investigating offenses that could justify a wiretap, and only when other investigative procedures have failed or are reasonably unlikely to succeed.

One important goal for FRT regulations is to clarify the circumstances under which FRT can and cannot be used. Many regulations approach this question by explicitly listing the purposes for which government operators can use FRT and by banning uses falling outside of that scope.

Other regulations prohibit uses that might interfere with civil liberties. Washington, for example, prohibits agencies from applying FRT on the basis of an individual's religion, race, gender, political affiliation, or any other characteristics protected by law. The state also prohibits using FRT to create a record describing an individual's exercise of rights guaranteed by the First Amendment. Proposed legislation in Arizona would prohibit uses based on identified discriminatory factors, or that would have a disparate impact on any community. In Congress, a proposed Fourth Amendment Is Not for Sale Act would prohibit agencies from purchasing personal data without a warrant and would fully ban the use of data that had been illegitimately obtained, a category that includes some private facial recognition databases such as Clearview AI.

Regulations can also clarify that operators may only use FRT systems in the ways they were intended to be used. For example, Washington prohibits agencies from manipulating images submitted for matching or from using sketches as the basis for comparisons.

Some jurisdictions prohibit facial recognition matches from being used to establish probable cause in a criminal investigation in the absence of other forms of evidence. This prohibition is included in Washington's facial recognition law, as well as proposed legislation in Alabama, Hawaii, and New York. Legislation being considered in Kentucky would prohibit any information obtained from facial recognition from being received as evidence in a trial.

Aside from the investigation of criminal activities, many enacted and proposed regulations also explicitly permit law enforcement agencies to use FRT for locating missing persons,[2] identifying deceased or incapacitated individuals,[3] combating public health emergencies,[4] identifying someone who has been lawfully arrested,[5] identifying an employee in a workplace,[6] or responding to emergencies involving an immediate threat of death or serious injury.[7] While lawmakers may still implement safeguards on how these uses take place, the restrictions are almost always more permissive than in cases where FRT is used to support criminal investigations.

Regulations also frequently clarify the non-law enforcement uses allowed under the law, such as using FRT to verify an individual's identity when issuing licenses or other documents[8] or letting employees authenticate themselves when using personal devices like smartphones.[9] Many of these more benign uses of the technology could otherwise be inadvertently banned if law and regulation measures are scoped too broadly. In some cases, legislation would actually mandate the use of facial recognition, such as a proposed Minnesota bill that would require FRT to be used to prevent fraud and expedite processing times when issuing state IDs and drivers' licenses.

TRANSPARENCY

Many pieces of legislation aim to improve transparency surrounding FRT deployments by requiring that operators publicly reveal how facial recognition is being used and governed. These kinds of transparency measures focus on three areas in deploying and operating a facial recognition system.

The first is the procurement process. Some laws and proposals would require operators to submit a use policy and impact assessment for proposed FRT systems before being allowed to purchase them. Washington, for example, requires all operators to submit an accountability report containing details about the facial recognition vendor, the purpose and scope of the deployment, the measured performance of the system, and a data management policy describing how information will be used and safeguarded. This report must be submitted at least 90 days before deployment, posted publicly online, and updated every two years. Proposed legislation in Arizona would institute a similar requirement. At the local level, every city listed in Table 1, with the exception of Nashville, requires agencies to submit an impact assessment and use policy when requesting authorization to purchase a facial recognition system.

Some legislation would further require that operators actively engage with their communities prior to deploying facial recognition systems. The state of Washington and the city of Seattle, for example, both require operators to hold community consultations prior to deployment. Proposed legislation in New Jersey and Arizona would also require agencies to hold public hearings prior to use. In Utah and New York City, authorities are not required to hold community consultation, but they are required to give notice to the public before operation would begin and allow individuals to submit comments about the proposed use.

The second area for transparency efforts is the period when FRT is in operation or when images are being captured that may eventually be used as part of a facial recognition search. Utah, for instance, requires

---

2 Enacted: Washington; Utah | Proposed: Kentucky; Louisiana.

3 Enacted: Massachusetts; Washington; Utah | Proposed: Louisiana.

4 Proposed: Hawaii.

5 Proposed: Louisiana.

6 Proposed: Massachusetts.

7 Enacted: Massachusetts; Washington | Proposed: Louisiana; Minnesota; U.S. Congress.

8 Enacted: Massachusetts; Washington; Utah | Proposed: Hawaii.

9 Enacted: Massachusetts.

agencies to notify individuals whenever they are capturing images that could be used in conjunction with FRT. Another example is a proposed bill in Massachusetts that would require the state registrar of motor vehicles to post notices at all of its offices to explain how the images stored by the agency could be used as part of targeted facial recognition.

The third focus of transparency efforts is ensuring that after FRT has been deployed, the details and results of its use are recorded and made available both to the public and to any individuals that have been affected. Many regulations would accomplish this by requiring agencies that request or perform facial recognition searches to submit annual public reports detailing how the systems were used. These reports can include information such as the number of searches conducted,[10] the number of matches returned,[11] the suspected crimes being investigated,[12] the database used for the searches,[13] the race and gender of the targets,[14] the number of arrests and convictions resulting from searches,[15] what other entities the agency shared data with,[16] and complaints filed against the system.[17]

In the case of facial recognition systems used for ongoing surveillance, reports can also include details on the duration of the deployment,[18] the location where the surveillance takes place,[19] the number of people subjected to analysis,[20] and the number of misidentifications.[21]

Jurisdictions requiring warrants for facial recognition searches may require the judges approving warrant requests to submit reports detailing the number of warrant applications they receive,[22] the number they grant,[23] and the identity of the requesting officers and agencies.[24]

Regulations can also mandate more intensive audit procedures to ensure operators are complying with the law and with their declared use policies. Proposed legislation in Louisiana, for instance, would require agencies to adopt an audit process to ensure facial recognition is only being used for legitimate law enforcement purposes.

Many regulations would also require that information about facial recognition searches be disclosed to defendants whenever FRT was used to assist in an investigation. Washington, for example, requires that agencies disclose their use of facial recognition to defendants in a timely manner prior to trial but does not detail what information must be provided. Under legislation currently being considered in Louisiana, anyone arrested as a result of an investigative lead generated using FRT must be notified within 48 hours and provided with information about the purpose of the search, the database used, and the details contained in the authorizing court order. A proposed revision of Massachusetts' recent law would require

---

10 Enacted: Massachusetts; Utah | Proposed: Louisiana.
11 Enacted: Massachusetts; Utah.
12 Enacted: Massachusetts; Utah | Proposed: Louisiana.
13 Enacted: Massachusetts; Utah.
14 Enacted: Washington | Proposed: Massachusetts; Louisiana.
15 Proposed: Louisiana.
16 Enacted: Palo Alto; Santa Clara; Lawrence; Yellow Springs | Proposed: Arizona.
17 Enacted: Palo Alto; Santa Clara; Lawrence; Yellow Springs | Proposed: Arizona.
18 Enacted: Washington; Lawrence | Proposed: Minnesota; Arizona; U.S. Congress.
19 Enacted: Washington; Lawrence | Proposed: Minnesota; Arizona; U.S. Congress.
20 Proposed: Minnesota; Arizona; U.S. Congress.
21 Proposed: Minnesota; U.S. Congress.
22 Enacted: Washington | Proposed: Minnesota; U.S. Congress.
23 Enacted: Washington | Proposed: Minnesota; U.S. Congress.
24 Enacted: Washington | Proposed: Minnesota; U.S. Congress.

all records about the facial recognition search to be provided to defendants and their attorneys, including the results of the search, other possible matches identified by the system, the accuracy rate of the technology, and the process by which the defendant was selected as the most likely match.

TESTING REQUIREMENTS

Some laws and proposals would require operators to test FRT systems to determine their performance and check whether accuracy rates varied for different demographic groups. Washington's facial recognition law, for example, requires agencies to test proposed facial recognition systems in operational conditions before they can be used to make any decisions that could have legal or other similarly significant consequences on individuals. Proposed legislation in Minnesota and from the 116th U.S. Congress (S.2878) would require agencies to devise a procedure for independently testing systems' performance in operational conditions and assess whether there were any performance differences across different demographic groups. Agencies are required to address any demographic differences that are identified. The proposed Algorithmic Accountability Act of 2019 (S.1108/H.R.2231) would have required the Federal Trade Commission to promulgate regulations mandating all operators of high-risk algorithmic decision systems (which would almost certainly include facial recognition systems) to conduct an assessment of their algorithms' accuracy, bias, privacy impacts, and security risks.

It is notable that these regulations specify that tests be conducted in operational conditions. Laboratory tests assess an algorithm's performance on curated image sets that are designed to evaluate how well algorithms handle particular situations, such as off-angle, poorly illuminated, and pixelated images; images of people wearing face masks; images of individuals who are members of particular racial groups and sexes; and photos of individuals at different ages. In contrast, operational testing allows agencies to collect information about the real-world performance of the full systems in their deployment environments. Operational performance is often much lower than laboratory testing performance, due to factors like operator error and unpredictable subject behavior.

Proposed legislation in New Jersey is somewhat unique in that it creates an obligation for the state's attorney general to arrange for independent, third-party testing of the five most commonly available facial recognition systems. This testing must be conducted regardless of whether these systems are actually in use in the state.

Washington also created an obligation for facial recognition service providers to provide application program interfaces (APIs) or other technical means for independent third-party tests of the system's accuracy and bias. If these tests identify any bias in facial recognition performance, all agencies using that service are required to implement a plan for mitigating those differences.

HUMAN REVIEW

One of the primary goals of facial recognition regulation is to protect individuals against possible harm related to algorithm errors. One way of mitigating these risks is by ensuring that a human is involved in reviewing the matches returned by facial recognition software.

Washington has attempted to codify this safeguard by requiring any operators using facial recognition to make decisions that have legal or other similarly significant impacts on individuals to ensure those decisions are subject to meaningful human review. Washington's legislation defines this as ensuring that trained human operators with the power to alter the decisions made by facial recognition systems are overseeing the operation of the system or are available to review decisions once they have been made.

Proposed legislation in Louisiana would institute a similar requirement, though it does not provide a definition of meaningful human review.

Proposed legislation in Minnesota and from the 116th U.S. Congress (S.2878) would specify that law enforcement agencies cannot interact with anyone that has been identified by a facial recognition system unless an officer has examined the output. In Utah, legislation goes further, requiring any possible matches to be reviewed by two separate employees. Each must agree that the individual returned by the system is a probable match before the results can be returned to a law enforcement agency.

> *One of the primary goals of facial recognition regulation is to protect individuals against possible harm related to algorithm errors. One way of mitigating these risks is by ensuring that a human is involved in reviewing the matches returned by facial recognition software.*

To ensure that human review is a robust safeguard, some legislation would also specify that the employees must be properly trained before being allowed to operate or review the decisions of facial recognition systems. Washington, for example, requires agencies to conduct periodic training of all employees who operate facial recognition services. This training must cover the system's capabilities and limitations, how to interpret and act on matches that are returned, and what it means for them to satisfy requirements for meaningful human review. In Utah, the law prohibits searches from being conducted by anyone who is not trained in how to make a facial recognition comparison and who has not completed implicit bias testing. Proposed legislation in Hawaii would also restrict operation to trained personnel but does not provide a definition of what this entails.

Bans on Government Facial Recognition Use

Instead of trying to regulate the use of facial recognition, some jurisdictions have instead decided to ban the technology. Some of these bans are relatively narrow, prohibiting the use of FRT in schools or residential complexes, outlawing its use in connection with drones or police body cameras, or preventing authorities from using the technology to support federal immigration authorities. Other bans have been broader in scope, outlawing any use of FRT by government agencies.

As of the time of writing, two states and 19 municipalities have enacted bans on the government's use of FRT. For example, the King County Council in Washington passed an ordinance prohibiting FRT usage by county officials, including those in its local police agency, the King County Sheriff's Office. A further seven states, as well as a large number of municipalities, are currently considering similar bans. No ban has been enacted at the national level, though two pieces of legislation introduced during the 116th Congress would have created broad prohibitions for federal agencies. The Facial Recognition and Biometric Technology Moratorium Act of 2021 (S.2052/H.R.3907)—which was recently reintroduced in the 117th Congress after its initial introduction in 2020 (S.4084/H.R.7356)—would ban the use of FRT by federal officials. This legislation also reiterates the prohibition first introduced in H.R.3875 against any federal funds from being used to purchase or use facial recognition systems.

Most of these bans are indefinite, but in some cases, they may be limited to a certain number of years, or until some condition is met, such as the passage of a more comprehensive set of safeguards. The bans enacted

by Vermont and Virginia and proposed in S.4084/H.R.7356, for example, explicitly state that the bans are to remain in place until the technology's use is expressly authorized through new legislation. In ordinances enacted by Springfield and Portland, as well as legislation proposed in New Jersey, restrictions would only be in place until more comprehensive protections can be enacted by the legislature. Washington's proposed ban is an example of one that is time limited; this ban would only last until July 1, 2026.

Many of these bans create exceptions for certain kinds of uses. For example, some would still allow authorities to use the results of facial recognition searches sent to them by other agencies, so long as the search was not explicitly requested.[25] Other jurisdictions would make exceptions for facial recognition tools purchased by agencies for user authentication or access control[26] or for redacting video recordings to protect individuals' privacy.[27] Several jurisdictions would allow FRT to be used when investigating missing or exploited children,[28] while Nebraska would allow searches as long as images had been gathered with subjects' consent. Virginia's ban allows an exception for deployments at commercial airports, and Vermont's ban allows the technology to be used on drone footage so long as agents obtain a warrant.

In addition to these examples of broad restrictions, some jurisdictions have proposed more limited bans that would only cover specific uses that legislators deem risky. The most common target of these partial bans is police body camera footage. Laws enacted in California, New Hampshire, and Oregon have all prohibited law enforcement from using facial recognition on footage obtained from body camera recordings. New Jersey, New York, and South Carolina are all currently considering similar proposals. At the federal level, two bills introduced in the 117th Congress (H.R.1163 and H.R.1280) would ban this practice for federal agencies.

Other targets of partial bans include FRT use in schools,[29] in housing complexes,[30] in speeding enforcement,[31] and on footage recorded by drones.[32] Some laws and proposals would also specifically prohibit using the technology for immigration enforcement. Utah, for example, prohibits agencies from using facial recognition to support investigations of civil immigration violations. Illinois, Maryland, and Rhode Island are all currently considering similar proposals that would prevent agencies from using FRT when working with federal immigration authorities.

Notably, several federal proposals during the 116th Congress would have attempted to achieve a de facto ban on the use of FRT by state and local governments by penalizing any agency that uses facial recognition. The Facial Recognition and Biometric Technologies Moratorium Act of 2021 (S.2052/H.R.3907), for example, would make any agency using facial recognition ineligible for federal assistance under the Byrne grant program. The Stop Biometric Surveillance by Law Enforcement Act (H.R.7235) would have withheld funding from not just the Byrne grant program but also the Urban Area Security Initiative and State Homeland Security Grant for any agency that used facial recognition on body camera footage.

---

25 Enacted: Alameda; Berkeley; Oakland; San Francisco; Santa Cruz; New Orleans; Boston; Cambridge; Easthampton; Madison | Proposed: Maine.

26 Enacted: Berkeley; Boston; Easthampton; Minneapolis; Portland (ME); Portland (OR); Madison; Baltimore | Proposed: New Jersey; New York; Maine; Oregon.

27 Enacted: Maine; Oregon | Boston; Easthampton; Minneapolis; Portland (ME); Portland (OR); Madison; Baltimore.

28 Enacted: Vermont; Boston; Madison | Proposed: Maine.

29 Enacted: New York | Proposed: Pennsylvania.

30 Proposed: New York; U.S. Congress.

31 Proposed: California.

32 Proposed: New York.

Regulation of Commercial Facial Recognition Use

While most legislative efforts in past years have focused on regulating the use of FRT by government actors, some jurisdictions have also been working to address how private actors are using the technology. As with government operators, some of these efforts have been aimed at banning commercial use altogether, while others have attempted to create rules to govern how the technology is deployed. Some do this by focusing on facial recognition specifically, while others focus more broadly on the management of users' biometric data. Some states like California and Virginia have also enacted general data privacy laws that regulate a broad range of commercial data collection, including facial recognition. A non-comprehensive list of the most prominent examples of these laws and proposals appears in Appendix 4.

So far, every law or proposal regulating the commercial use of facial recognition would require operators to gain subjects' consent before collecting their biometric data. Regulations are not always consistent about what this would mean. Some legislation requires consent to be opt-in (usually referred to as "affirmative," "written," or "unambiguous" consent),[33] as well as freely given,[34] specific,[35] and informed.[36] Others do not specify what is meant by consent.[37] Proposed legislation in Massachusetts and the 116th Congress would also have clarified that operators cannot refuse service to individuals who do not provide their consent, so long as the use of FRT is not necessary for delivering the service in question.

General data privacy regulations also place a heavy emphasis on consent. California, Virginia, and Colorado's privacy laws and proposed legislation from Ohio and Massachusetts require commercial operators to obtain consent before processing the biometric data of consumers. Future federal legislation is likely to include similar provisions. These laws also require operators to provide consumers with privacy notices that detail what data is collected, how it is used, with whom it may be shared, and how consumers can exercise their personal data rights.

Some regulations provide exceptions to this consent requirement. Washington's biometrics law, for example, does not require operators to obtain consent if they provide notice to users affected by the system or provide a mechanism for users to later restrict how their biometrics can be used. Washington and Virginia would also exempt operators from having to provide notice or obtain consent if they were collecting data for security and fraud-prevention purposes. The Commercial Facial Recognition Privacy Act of 2019 (S.847) would have provided a similar exception for security applications, as well as in emergency situations and uses involving file management or the identification of public figures for certain purposes. S.847 would also have allowed FRT to be used to determine whether an end user had given affirmative consent, so long as all data was deleted if they had not. This clarification would allow for some uses like public-facing building access control systems to continue, though it specifically would not authorize "mass scanning" in areas where individuals would not have a reasonable expectation that FRT was being used.

In addition to consent requirements, some laws and proposals would institute other restrictions on how commercial operators can use facial recognition. Proposed legislation in Massachusetts, for example, would prevent operators from using facial recognition to make any decisions carrying legal or similarly significant effects, including decisions that could deny access to financial services, housing, education, employment, healthcare, and basic necessities, among others. The Massachusetts bill would also broadly prohibit any

---

33 Enacted: California; Illinois; Virginia | Proposed: Kentucky; Maryland; Massachusetts; New York; U.S. Congress.

34 Enacted: California; Virginia | Proposed: Massachusetts.

35 Enacted: California; Virginia | Proposed: Massachusetts; New York.

36 Enacted: California; Illinois; Virginia | Proposed: Maryland; Massachusetts; New York; Vermont.

37 Enacted: Texas; Washington.

uses that would "conflict with an end user's best interests" and charge the Massachusetts attorney general with interpreting and enforcing this protection.

Many laws and bills would place strict limits on how biometric information could be shared with other entities. Some would allow sharing to take place if the operators obtained the users' consent,[38] if the sharing were necessary to fulfill a contract or other legal obligation,[39] or if the recipient pledged to uphold an equivalent duty of care, loyalty, and confidentiality as is imposed on the operator.[40] Some would prohibit the sale of biometric data regardless of subject consent.[41] Under California, Virginia, and Colorado's privacy laws and both Ohio and Massachusetts' proposed general data privacy bills, operators must disclose any sale of data to consumers and allow them the opportunity to opt out.

Some regulations would also institute requirements for the operational policies adopted by the organizations using FRT. Many would require that operators adopt measures to secure biometric data from unauthorized access.[42] Others would require operators to delete biometric data once the purpose of its collection had been fulfilled or after a certain period of time had elapsed.[43] Similarly, California, Virginia, and Colorado's privacy laws and a law proposed in Massachusetts require commercial operators to limit their collection of data to only what is relevant and reasonably necessary for processing.

The Commercial Facial Recognition Privacy Act of 2019 (S.847) would require operators to institute meaningful human review for any decisionmaking informed by facial recognition that could result in mental, physical, or financial harm to an end user or be considered unexpected or highly offensive. S.847 would further require that operators make an application programming interface (API) available to third parties for the purpose of conducting independent tests of the facial recognition system's accuracy and bias.

General data privacy regulations also grant consumers certain rights over personal data that has been collected from them. California, Virginia, and Colorado's privacy laws and those proposed in Ohio and Massachusetts, for example, all give consumers the right to confirm whether their data was being processed, obtain a copy of their data, correct any inaccuracies, request the deletion of their data, and opt out of the sale of their data to other organizations.

On the federal level, proposed legislation—such as the Consumer Data Privacy and Security Act of 2021 (S.1494), the Data Protection Act of 2021 (S.2134), and the Information Transparency & Personal Data Control Act (H.R.1816)—provide evidence of the growing push in Congress for more comprehensive general data protections that would affect FRT usage. Additionally, the Social Media Privacy Protection and Consumer Rights Act of 2021 (S.1667), the Children and Teens' Online Privacy Protection Act (S.1628), and the BROWSER Act of 2021 (S.113) echo the call for consent and increased transparency from operators and service providers with access to sensitive user information and personal data. While these pieces of legislation cover a broad spectrum of applications, their implications for FRT are legitimate and noteworthy. S.1667 refers to protected health information; S.1628 seeks to expand the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501) to cover information used for biometric identification; and S.113 imposes requirements on providers of broadband internet access services and any services provided over the internet and that involve sensitive user information, which can easily be interpreted to implicate FRT services at large.

---

38 Enacted: California; Illinois; Virginia; Washington | Proposed: Kentucky; U.S. Congress (S. 847, S.4400).

39 Enacted: California; Illinois; Texas; Virginia; Washington | Proposed: Kentucky; U.S. Congress.

40 Proposed: Massachusetts.

41 Enacted: Illinois; | Proposed: Kentucky; Massachusetts.

42 Enacted: California; Illinois; Texas; Virginia; Washington | Proposed: Kentucky; Massachusetts.

43 Enacted: California; Illinois; Texas; Washington | Proposed: Kentucky.

Bans on Commercial Facial Recognition Use

So far, Portland and Baltimore are the only jurisdictions that have implemented a ban on the use of FRT by commercial operators. Portland's ordinance does not ban all uses of the technology but rather prohibits facial recognition from being deployed in "places of public accommodation." Operators are still allowed to deploy the technology in distinctly private areas but are prohibited from using it anywhere that is open to the general public. Proposed legislation in Massachusetts, Oregon, and Washington would institute similar bans if enacted. On the other hand, Baltimore's recently enacted ban is much stricter in legislating that no individual or corporation—including the mayor and city council—can use any face surveillance system or information obtained from such a system. Still, in what may be a recognition of the potential losses incurred by an outright ban, this moratorium is set to automatically expire on December 31, 2022, unless the city council chooses to extend it for five more years. Appendix 3 lists jurisdictions that have imposed such commercial bans.

Enforcement

While the details outlined in these bans and regulations provide appropriate first steps, they also necessitate penalties and other enforcement mechanisms to deter negligence, abuse, and other misconduct concerning facial recognition technologies. Proposed and enacted policies have introduced a range of possible punishments ranging in severity depending on the nature of the violation.

On the federal level, policies such as the Ethical Use of Facial Recognition Act (S. 3284), the Facial Recognition and Biometric Technologies Moratorium Act of 2021 (S.2052/H.R.3907), the George Floyd Justice in Policing Act of 2021 (H.R. 1280), and the Stop Biometric Surveillance by Law Enforcement Act (H.R.7235) have threatened to remove government funding or eligibility for government assistance for state or local governments determined to be in violation of the policies. In addition to the specific programs referred to by S.2052/H.R.3907 and H.R.7235, H.R.1280 proposed to add a section to 43 USC 10101 forbidding the use of grant amounts from the Department of Justice's Office of Justice Programs to be used for expenses related to FRT. Additionally, the Commercial Facial Recognition Privacy Act of 2019 (S.847) proposed to treat violations as unfair and deceptive acts, which are defined by the Federal Trade Commission and punishable by 15 USC 45 for civil penalties up to $10,000 per violation. On the state level, proposed legislation in New York similarly calls for penalties in the form of withholding state funds from incompliant police divisions.

> *These bans and regulations also necessitate penalties and other enforcement mechanisms to deter negligence, abuse, and other misconduct concerning facial recognition technologies.*

Other enforcement mechanisms outline the rights for individuals aggrieved by violations,[44] an attorney general,[45] or other governmental entity authorized by law to bring actions on behalf of citizens[46] to bring a civil action to court and initiate proceedings for injunctive relief, declaratory relief, a writ of mandate, or

---

44 Enacted: Boston; Easthampton; King County; Oakland; Portland (ME); Portland (OR); Santa Clara | Proposed: Arizona; Kentucky; Maryland; Minnesota; Nebraska; New Jersey (A. 4211; S.1917); Oregon; U.S. Congress (S.3284; S.2052/H.R.3907); Washington.

45 Enacted: Texas; Proposed: Idaho; Kentucky; Maryland; Massachusetts; New York; Washington.

46 Proposed: U.S. Congress (S.2052/H.R.3907, S.847).

evidence suppression. Several explicitly require any facial recognition information collected or derived in an unlawful manner to be deleted upon discovery.[47] In these legal proceedings, policies permit plaintiffs to recover actual or punitive damages[48] with set minimum amounts. Beyond awarding damages, certain proposed legislation would also allow for public entities,[49] private entities,[50] or both[51] to be charged fines and civil penalties for violations. To go into further detail, some provide specifications on amounts owed dependent on whether the violation occurred because of negligence or in an intentional or reckless manner, outlining greater damages for the latter.[52] Lastly, many policies call for government employees found violating their clauses to face consequences, including retraining, suspension, termination,[53] or other appropriate disciplinary action.[54]

Protecting the Public Interest

FRT has been caught up in a larger public debate over policing, race, and privacy. These are emotional topics, but they have created a confusing narrative. The debate over facial recognition technology also reflects erratic privacy protections in the United States. Digital technologies create immense amounts of data, but the constraints on how this data can be used are inconsistent, particularly for commercial use.

One precedent for the development of rules for FRT comes from the development of constraints on government use of communications data. Creating these rules and oversight for facial recognition is a necessary task and should be approached in the same way, balancing privacy concerns with public safety, and subject to legal constraints and legislative oversight. Facial recognition technology is another example of law and policy needing to catch up to technology if society is to safely reap its full benefit.

One lesson from the storming of the U.S. Capitol on January 6, 2021, is that facial recognition technology is an irreplaceable tool for maintaining public safety. It is also not desirable to lose consumer and citizen benefits—most people would choose not to wait at an airport rather than wait 30 minutes at a Transportation Security Administration entry point or an immigration booth on return. Of course, the few who prefer to wait should be allowed to do so, and as recommended, procedures should be in place to rectify any errors swiftly and fairly. The teething pains that greeted terrorist watch lists and other screening techniques after 9/11, and the overstated concern this created, are a good precedent. The system works well, there are few errors, civil liberties have not been affected, and citizens are protected without being inconvenienced.

New technologies, especially if they affect public safety or civil liberties, require regulation. This has been true since the first safety regulations appeared in the nineteenth century. There are many precedents for facial recognition regulation and use as the United States moves to establish adequate privacy protection for all digital data. With such efforts, a future that includes responsible use of FRT is both possible and beneficial. ■

---

47 Enacted: King County | Proposed: Minnesota; Nebraska; Washington.

48 Enacted: Illinois; Oakland; Portland (ME); Portland (OR) | Proposed: Idaho; Kentucky; Maryland; Massachusetts; Minnesota; Nebraska; New York (S73, SB1933); New Jersey; South Carolina; Washington; West Virginia.

49 Enacted: Easthampton; Springfield | Proposed: Kentucky; Louisiana.

50 Enacted: Texas | Proposed: New York; Maryland.

51 Proposed: Pennsylvania.

52 Enacted: Illinois | Proposed: Idaho; Kentucky; Maryland (HB218, SB476); Massachusetts; New York; South Carolina; West Virginia.

53 Enacted: Boston; King County; New Orleans; Oakland; Portland (ME) | Proposed: Louisiana; Minnesota; New Jersey; U.S. Congress (S.2052/H.R.3907).

54 Proposed: U.S. Congress.

James Andrew Lewis *is senior vice president and director of the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***William Crumpler*** *was a research associate with the Strategic Technologies Program at CSIS.*

This report is made possible thanks to the support from NEC Corporation of America and the Department of Homeland Security as part of its homeland security mission to defend the homeland while upholding our nation's values.

This report does not constitute the official position of the Department of Homeland Security. Any questions can be directed to the Office of Public Affairs at the Office of Biometric Identity Management.

The coauthors would like to thank those people who agreed to be interviewed for this report and participated in a related roundtable series. The authors would also like to give special thanks to Luiza Parolin and Jacqueline Lee for their research assistance, as well as additional thanks to Georgia Wood for her support.

Appendix 1: Regulations for Governmental Use

Note: * indicates proposed bill failed, with legislative body adjourning sine die.

FEDERAL		
117th Congress	S.____ – Fourth Amendment Is Not for Sale Act	Proposed
116th Congress	S.1108/H.R.2231 – Algorithmic Accountability Act	
116th Congress	S.3284 – Ethical Use of Facial Recognition Act	Proposed
116th Congress	H.R.4021 – FACE Protection Act of 2019	Proposed
116th Congress	S.2878 – Facial Recognition Technology Warrant Act of 2019	Proposed
116th Congress	S.3912 – Justice in Policing Act of 2020	Proposed
STATES		
Massachusetts	MGL Ch. 6 §220	Enacted
Washington	RCW 43.386	Enacted
Utah	Utah Code 77-23e-101	Enacted
Alabama	SB113/HB485	Proposed*
Arizona	SB1583	Proposed*
Hawaii	SB156/HB1226	Proposed*
Iowa	HF43	Proposed*
Kansas	SB198	Proposed
Kentucky	SB280	Proposed*
Louisiana	HB611	Proposed*
Massachusetts	HB117	Proposed
Massachusetts	S47/HB135	Proposed
Massachusetts	S1608	Proposed
Massachusetts	S1619	Proposed
Massachusetts	HB142	Proposed
Minnesota	HF465	Proposed*
Michigan	HB5019	Proposed
Montana	HB577	Proposed*
New Hampshire	HB499	Proposed*
New Jersey	S1916/A1210	Proposed
New Jersey	A989	Proposed

New York	A768	Proposed
New York	A4916	Proposed
MUNICIPALITIES		
Davis (CA)	Davis Municipal Code 26.07	Enacted
Palo Alto (CA)	Palo Alto Municipal Code 2.30.620-690	Enacted
Santa Clara (CA)	Santa Clara Code of Ordinances A40	Enacted
Lawrence (MA)	Lawrence Code of Ordinances 9.25	Enacted
New York (NY)	NYC Administrative Code 14-188	Enacted
Yellow Springs (OH)	Yellow Springs Code of Ordinances Ch. 607	Enacted
Pittsburgh (PA)	Pittsburgh Code of Ordinances 116.15	Enacted
Nashville (TN)	Nashville Code of Laws 13.08	Enacted
Seattle (WA)	Seattle Municipal Code 14.18	Enacted

Appendix 2: Bans for Governmental Use

JURISDICTION	CODE/BILL	STATUS	SCOPE
Federal			
117th Congress	S.2052/H.R.3907 – Facial Recognition and Biometric Technology Moratorium Act of 2021	Proposed	Full
116th Congress	S.4084/H.R.7356 – Facial Recognition and Biometric Technology Moratorium Act of 2020	Proposed	Full
116th Congress	H.R.3875 – To prohibit Federal funding from being used for the purchase or use of facial recognition technology, and for other purposes.	Proposed	Full
117th Congress	H.R.1280 – George Floyd Justice in Policing Act of 2021	Proposed	Partial
117th Congress	H.R.1163 – Federal Police Camera and Accountability Act	Proposed	Partial
116th Congress	S.2689/H.R.4008 – No Biometric Barriers to Housing Act of 2019	Proposed	Partial
116th Congress	H.R.7235 – Stop Biometric Surveillance by Law Enforcement Act	Proposed	Partial
States			
Vermont	S124	Enacted	Full
Virginia	Code of Virginia 15.2-1723.2	Enacted	Full

New Jersey	A4211	Proposed	Full
New York	S79/A5492	Proposed	Full
Maine	HP1174	Proposed	Full
Minnesota	HF1196	Proposed	Full
Nebraska	LB199	Proposed	Full
Oregon	S309	Proposed*	Full
Washington	SB5104	Proposed	Full
California	California Penal Code 832.19	Enacted	Partial
New Hampshire	N.H. Rev. Stat. § 105-D:2	Enacted	Partial
New York	NY St TechL §106-b	Enacted	Partial
Oregon	ORS 133.741	Enacted	Partial
Utah	Utah Code 77-23e-101	Enacted	Partial
California	AB550	Proposed	Partial
Illinois	SB0225	Proposed	Partial
Maryland	SB0234/HB0023	Proposed	Partial
New Jersey	S1917	Proposed	Partial
New York	S73/A4352	Proposed	Partial
New York	S1076/A1601	Proposed	Partial
New York	S675/A3311	Proposed	Partial
Pennsylvania	SB37	Proposed	Partial
Rhode Island	S0253/H5652	Proposed	Partial
South Carolina	H3918	Proposed	Partial
Municipalities			
Alameda (CA)	Res. 2019-7553	Enacted	Full
Berkeley (CA)	Berkeley Municipal Code 2.99.030	Enacted	Full
Oakland (CA)	Oakland Code of Ordinances 9.64	Enacted	Full
San Francisco (CA)	SF Administrative Code 19B.2	Enacted	Full
Santa Cruz (CA)	Santa Cruz Municipal Code 9.85.030	Enacted	Full
New Orleans (LA)	New Orleans Code of Ordinances 147-2	Enacted	Full
Portland (ME)	Portland City Code 17-131	Enacted	Full
Boston (MA)	City of Boston Code 16-62	Enacted	Full

Brookline (MA)	Brookline Town By-Laws 8.39	Enacted	Full
Cambridge (MA)	Cambridge Code of Ordinances 2.128.075	Enacted	Full
Easthampton (MA)	Easthampton City Ordinances 6.22	Enacted	Full
Northampton (MA)	Northampton Code of Ordinances Ch. 290	Enacted	Full
Somerville (MA)	Somerville Code of Ordinances 9-25	Enacted	Full
Springfield (MA)	Springfield Code of Ordinances Ch. 173	Enacted	Full
Minneapolis (MN)	Minneapolis Code of Ordinances 41.120	Enacted	Full
Jackson (MS)	Ordinance Prohibiting the Use of Facial Recognition Technology by the Jackson Police Department	Enacted	Full
Teaneck (NJ)	Ordinance No. 7-2021	Enacted	Full
Portland (OR)	Portland City Council Ordnance 190113	Enacted	Full
Madison (WI)	Madison General Ordinances 23.64	Enacted	Full

Appendix 3: Bans for Commercial Use

JURISDICTION	CODE/BILL	STATUS
	States	
Oregon	SB310	Proposed*
Massachusetts	HB117	Proposed
Washington	SB5104	Proposed*
	Local	
Portland (OR)	Portland City Code 34.10	Enacted
King County (WA)	Ordinance 19296	Enacted
Baltimore (MD)	Council Bill 21-0001	Enacted

Appendix 4: Regulations for Commercial Use

JURISDICTION	CODE/BILL	STATUS	TYPE
	Federal		
116th Congress	S.847 – Commercial Facial Recognition Privacy Act of 2019	Proposed	FRT Regulation
116th Congress	S.4400 – National Biometric Information Privacy Act of 2020	Proposed	Biometrics Regulation

117th Congress	H.R. 1816 – Information Transparency & Personal Data Control Act	Proposed	General Privacy Regulation
117th Congress	S.113 – BROWSER Act of 2021	Proposed	General Privacy Regulation
117th Congress	S.1494 – Consumer Data Privacy and Security Act of 2021	Proposed	General Privacy Regulation
117th Congress	S.1628 – Children and Teens' Online Privacy Protection Act	Proposed	General Privacy Regulation
117th Congress	S.1667 – Social Media Privacy Protection and Consumer Rights Act of 2021	Proposed	General Privacy Regulation
117th Congress	S.2134 – Data Protection Act of 2021	Proposed	General Privacy Regulation
	States		
Idaho	HB492	Proposed*	FRT Regulation
Kentucky	SB280	Proposed	FRT Regulation
Maryland	S476	Proposed*	FRT Regulation
Massachusetts	HB117	Proposed	FRT Regulation
Vermont	H75	Proposed	FRT Regulation
Illinois	740 ILCS 14/1	Enacted	Biometrics Regulation
Maryland	SB16/HB218	Proposed*	Biometrics Regulation
Massachusetts	S220	Proposed	Biometrics Regulation
New York	SB1933	Proposed	Biometrics Regulation
South Carolina	HB3063	Proposed	Biometric Regulation
Texas	Texas Business and Commerce Code 11.A.503.001	Enacted	Biometrics Regulation
Washington	RCW 19.375.020	Enacted	Biometrics Regulation
West Virginia	HB2064	Proposed*	Biometrics Regulation
California	California Civil Code 1798.100 – 1798.199.100	Enacted	General Privacy Regulation
Colorado	SB190	Enacted	General Privacy Regulation
Virginia	Code of Virginia 59.1-571 – 59.1-581	Enacted	General Privacy Regulation
Massachusetts	S46	Proposed	General Privacy Regulation
Ohio	HB376	Proposed	General Privacy Regulation