15

An Overview of Facial Recognition Technology Regulation in the United States

Mailyn Fidler and Justin (Gus) Hurwitz

15.1 INTRODUCTION

The United States generally takes a light-touch approach to regulation, and notably so in the technology sector. This approach applies equally to facial recognition technology (FRT). But while the US regulatory touch may be light, this does not mean that it is either simple or non-existent. This chapter chronicles regulation of FRT in the United States at federal, state, and local levels, and considers potential regulatory issues on the horizon.

Every chapter in this volume discusses FRT, so the reader is assumed to have more than passing familiarity with its salient technological capabilities and limitations. Very briefly, for purposes of our analysis, FRT is a tool by which computers can identify individuals by an image of their face, generally using sophisticated algorithms that compare visual characteristics of an image to vast databases of other faces. We emphasise the role of image-based analysis, because there are other FRTs that may use other indicators. For instance, specialised systems may use infra-red cameras to recognise the structure of blood vessels underneath the skin and use these to identify individuals. This is certainly a form of FRT, but because high-resolution infra-red imaging is not a pervasive technology (yet?), technologies such as this are not currently a focus of this debate. Similarly, research into FRT benefits adjacent fields, such as autofocus technologies that dramatically improve the quality of devices such as cameras. Because such technologies are not used for identification purposes, they generally are not directly implicated by the discussion in this chapter. However, restrictions on the use of one application of FRT could well affect the development or use of other applications of related technology.[1]

FRT presents unique challenges as an identification technology. The simple explanation for this is that faces are pervasive. Humans present them publicly every time we are outside. We cannot meaningfully obstruct them, for both practical and social

[1] While not discussed at length in this chapter, there are other potentially problematic uses of FRT beyond identification. For instance, firms are developing technologies that purport to use characteristics of facial expressions during interviews to help assess the suitability of candidates for jobs.

https://doi.org/10.1017/9781009321211.018 Published online by Cambridge University Press

reasons – and, it bears note that FRTs are increasingly able to identify individuals based even upon obstructed images of their faces. And like all biometric markers, individuals cannot alter the appearance of their faces in the same way that they can, for instance, change a password or have multiple email addresses. Taken together, this makes faces both uniquely pervasive and uniquely persistent as identification tokens.

There is a wide range of potential use cases for FRT, ranging from contextually positive, to neutral, to potentially problematic. For instance, at the possibly innocuous end of the spectrum, FRT can be used to facilitate consumer convenience features, such as information kiosks that recognise individuals and automatically present relevant information to them. Or FRT could facilitate contactless payment or check-out features. Social media platforms can use FRT to automatically identify individuals in posted images. This information could be used for tracking purposes, or to learn information about those individuals that could be used for advertisement targeting. It could also be used to alert individuals when others post recognisable images of them, potentially giving them an opportunity to take privacy-protecting steps in response.

Perhaps the most potentially concerning class of FRT use cases stems from the widespread use of surveillance cameras in public settings – all of which can, in principle, incorporate FRT systems. In this setting, FRT can be used expansively by both private and public actors. For instance, venues such as shopping malls can use FRT-enabled security systems.[2] FRT can be used to help law enforcement identify or track fugitives or other wanted individuals in public places – or to help search for missing persons. In the most extreme setting, FRT effectively eliminates any sense of privacy or anonymity that individuals may have when in public spaces. Where before the advent of FRT there was 'anonymity in crowds', today there is none.

This chapter proceeds in four parts. US law presents a complex set of regulatory tools and institutions – institutions that are often overlapping and often competing with one another. Section 15.1 provides a brief overview of this myriad of institutions. Sections 15.2 and 15.3 then bifurcate the discussion along two sets of institutions: federal and state-level regulatory efforts. Section 15.2 looks at recent federal efforts relating to FRT; Section 15.3 looks at recent state-level efforts. Section 15.4 offers some observations on issues that are on the horizon for the regulation of FRT technology in the United States.

15.2 SETTING THE STAGE: TECHNOLOGY REGULATION IN THE UNITED STATES

US law does not present a single, unified, legal system. The United States is a federation of more than fifty states and territories, each with unique constitutions and legal

[2] Joel Schipper, 'Jefferson Mall adds new security system with facial recognition' (2 August 2022), *WDRB*, www.wdrb.com/news/jefferson-mall-adds-new-security-system-with-facial-recognition/article_66714a42-128b-11ed-b95c-7fc634889bf9.html.

https://doi.org/10.1017/9781009321211.018 Published online by Cambridge University Press

environments. The federal government has its own Constitution and enacts its own laws, which sometimes displace, sometimes co-exist with, and other times are secondary to state law. Beyond that, most 'law' in the United States actually comes in the form of regulations enacted by federal or state agencies. And in many settings – perhaps most notably those relating to the technology sector and privacy-related concerns – US law relies extensively on self-regulation and sectoral regulation.

Before turning to any specific US regulatory approaches to FRT, this chapter presents a brief overview of these interrelated regulatory institutions.

The starting point for understanding the US legal approach to FRT – as well as many related issues, such as privacy issues generally – is to understand US law's emphasis on protecting individual autonomy from intrusion from the government. That is, US law is largely premised on negative rights, or rights to be free from interference from the government. This stands in stark contrast to many other legal systems that are premised on positive rights, or guarantees that the government provide or protect individual liberties.

Thus, for example, the US tradition of privacy law is largely anchored in the First and Fourth Amendments.[3] Beyond those found in these amendments, Americans have limited fundamental privacy rights against the government. These amendments protect the freedom of speech and limit the government's ability to encroach upon individuals' other rights without due process of law. And the privacy rights facilitated by these amendments look very different from those anchored in other concepts, such as a right to dignity or self-determination.[4] The First Amendment guarantees that individuals cannot be compelled by the government to speak, including potentially by disclosing information about themselves. And similarly, the Fourth Amendment prohibits the government from searching and seizing individuals' property – again preventing compelled disclosure of information to the government – absent obtaining a specific warrant from a federal court subject to due process of law. Critically, both of these amendments only run against the government. Neither prohibits private entities from compelling speech or disclosure of information, such as a condition of service. And neither prevents others from sharing or disclosing facts known about others, absent specific indicia of harm.[5]

These principles give rise to a defining doctrine of US privacy law: the third-party doctrine. This doctrine says simply that one has no reasonable expectation of privacy in information disclosed or publicised to a third party. If a user shares information

[3] James Whitman, 'The two Western cultures of privacy: Dignity versus liberty' (2003–2004) 113 *Yale Law Journal* 1151.

[4] Ibid.

[5] Such 'indicia of harm' include, for instance, the so-called privacy torts. These are state-level (not federal offences) that typically include intrusion upon seclusion, disclosure of private information, false light, and appropriation of likeness. To be actionable, however, these torts generally require demonstration of concrete harm, such as monetary loss or conduct amounting to trespass. At federal level, statutes such as the Wiretap Act and Stored Communications Act create liability for specific conduct that is akin to a violation of privacy.

with another private entity, such as an online service, that entity is largely (though not entirely) free to do with that information as it pleases, and the Fourth Amendment provides the user with no protection against government efforts to obtain that information. And if an individual shares their information publicly, that information may be used generally. This includes merely being seen in public – with few exceptions, under US law an individual may have their public activities tracked, documented, and shared by other individuals and private entities. The Fourth Amendment may prohibit the government from tracking individuals in this way, but does not reach other private entities – indeed, government actors may even be able to acquire information about an individual from third parties, even where the government could not have created that information itself.

There is some limited ability for the government to impose narrowing laws. For instance, it can write laws that constrain its own conduct. Laws such as the Wiretap and Stored Communications Acts were adopted principally to limit the conduct of law enforcement agencies that might have otherwise been considered permissible under the Fourth Amendment. In other cases, most notably where concrete and particular harms are identifiable from information disclosure, the government may be able to proscribe such disclosures. This most often happens in heavily regulated industries that transact in sensitive information, such as health and financial information. For instance, the Stored Communications Act prohibits electronic communications services from disclosing the contents of users' communications except under specific circumstances. Even then, however, the First Amendment limits the extent of such regulations. For instance, a law that prohibited the exchange of consumer data for marketing or promoting prescription drugs has been found to violate the First Amendment rights of pharmaceutical research companies and manufacturers who may have reason to use that data.[6]

The discussion so far has focussed primarily on the federal government as a regulator. The federal government may regulate by writing laws (which happens through Congress); it also relies extensively on federal agencies to promulgate and enforce regulations. In the United States, these regulators are generally sector-specific. For instance, the Federal Aviation Administration regulates the airline industry; the Federal Communications Commission regulates communications industry; and the Department of Health and Human Services regulates the healthcare sector. Regulators such as the Federal Trade Commission have more general regulatory authority – but the courts and Congress have generally been sceptical of efforts by such generalist regulators to use their authority to regulate pervasive or cross-industry practices.

In addition to the federal government, the states play an important role in regulating these issues. For instance, every state recognises various 'privacy torts'.

[6] *Sorrell* v. *IMS Health* (2011) 564 U.S. 552; see also *Zauderer* v. *Office of Disc. Counsel* (1985) 471 U.S. 626 (providing other protections for commercial speech).

These cover harms such as intrusion upon seclusion, disclosure of private information, presenting someone in a false light, and appropriation of likeness. This means, among other things, that enforcement generally occurs in the courts of the state where a given injury occurred. There may also be substantive differences in these laws between the states, including both whether specific causes of action are even recognised and the damages available for violating them. Each state also has its own constitution and legal system – there are sometimes important differences between these constitutions, both between the states and between the states and the federal Constitution. For instance, the federal Constitution has more onerous standing requirements than many state constitutions, which means that federal courts may not be able to recognise certain types of harms as allowing judicial remedies, whereas state-level courts may be able to adjudicate those same claims.

More recently, many states have adopted specific statutes that may relate to FRTs. Illinois's Biometric Information Privacy Act (BIPA), discussed in Section 15.4, for instance, directly affects the use of FRT and has caused firms such as Facebook to alter the services they offer to individuals located in that state. State-level laws create a complex set of implementation issues, including compliance costs and difficulties, especially where the specific requirements of a law may not be clear at the time it is enacted and the need (at times) to comply with contradictory requirements between state laws. The relationship between state and federal law can also be uncertain. In many cases, the existence of a related federal law will pre-empt state laws – it can even be the case that the non-existence of a federal law or regulation can prevent the adoption of a state law. While these issues are foundational to the operation of any legal system, as modern technology has increasingly brought state-level regulations into tension with those of other states and the federal government, there has been a surprising amount of debate in the United States as to how they ought to play out.

Extra-regulatory tools play a significant role in governing technologies such as FRT in US law. Such tools include mechanisms such as self-regulation and self-regulatory organisations, and executive regulatory tools such as government procurement policies. Self-regulation comes up in many contexts. Legally, it is closely related to consumer protection law: self-regulation often requires firms or industries to publicly disclose governance principles and to implement them in a binding way. A failure to do so might be the basis for liability based upon unfair or deceptive practices claims. Self-regulation can also be based upon the threat of legislation or even mere investigation: Congressional hearings into a firm's or industry's business practices can be disruptive or costly.

The use of procurement policies as a regulatory tool draws from the government's role as a large purchaser of goods and services, including of technology products and services. Government entities can decide which goods and services to purchase without the need for legislative or regulatory authority. For instance, the president

or a local government entity can often issue a policy directive that prohibits law enforcement from using certain technologies (such as FRT) or that directs how they may be used (such as for locating missing persons but not for tracking criminal suspects). Because the federal government is one of the largest purchasers of goods or services in the country (even the world), these policies have the potential to shape entire industries. A decision to use, or to not use, certain types of technology can cause private industry to invest billions of research and development dollars to develop technologies that meet those needs.

The brief discussion here offers a capsule summary of many aspects of US legal institutions that are relevant to regulation of FRT. It is far from a comprehensive introduction to US law. But for readers unfamiliar with these institutions it introduces several important idiosyncrasies and provides context for the discussion that follows – and for all readers it begins to develop themes that will be seen in the remainder of this chapter.

15.3 FEDERAL REGULATION OF FACIAL RECOGNITION TECHNOLOGY

Federal FRT regulation is still nascent in the United States. Administrative agencies have played the biggest role so far, approaching the issue through standard-setting and existing consumer protection regulation. For instance, since 2017, the National Institute of Technology and Standards (NIST), a non-regulatory agency under the auspices of the Department of Commerce, has developed standards for absolute and comparative accuracy of facial recognition algorithms and publishes results for software available through commercial vendors.[7] And these federal standards inform state approaches. For instance, Virginia allows its police to use only facial recognition software that performs well according to NIST standards.[8]

The Federal Trade Commission, the US consumer protection agency, published a set of 'best practices' regarding the use of FRT in 2012.[9] Publications such as these 'best practices' may inform future Commission activity, but do not constitute legally binding rules. More recently, the Commission has enforced general consumer protection principles against at least one software company for misleading consumers about when and how facial recognition software would be used on photo and videos uploaded to the app. In 2021, the Commission settled with a photo app company called Everalbum for allegedly only using facial recognition

[7] Patrick Grother, Mei Ngan, Kayee Hanaoka, Joyce Yang, and Austin Hom, 'Ongoing face recognition vendor test (FRVT)' (28 July 2022), National Institute of Standards and Technology, https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf.

[8] 117th Congress American Data Privacy and Protection Act 2022.

[9] Federal Trade Commission, 'Facing facts: Best practices for common uses of facial recognition technologies' (22 October 2012), www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

https://doi.org/10.1017/9781009321211.018 Published online by Cambridge University Press

after affirmative consent from users, when, in reality, the company automatically activated the feature.[10]

The US Congress has begun debating legislation that would regulate both the US government's own use of federal regulation technology, as well as private use of regulation technology. But the fates of each of these bills is far from certain. In June 2021, Senator Markey proposed a bill that would regulate the federal government's own use of facial recognition.[11] The bill, which was not enacted into law but was reintroduced again in 2023, would prohibit any federal agency from using FRT, or information obtained from any such technology, without specific approval from Congress.

Congress also commissioned a study of the federal government's use of FRT by the Government Accountability Office, which was published in August 2021.[12] Most of the agencies used some form of facial recognition to help ensure the digital security of agency devices. Six reported using the tool for law enforcement purposes and five for security purposes, including live monitoring of locations.

The Internal Revenue Service (IRS), the United States' taxation authority, came under bipartisan scrutiny in 2022 for using FRT to verify the identities of taxpayers online. Lawmakers criticised the agency's use of the tool as intrusive and requiring taxpayers to sacrifice privacy for data security. Advocates criticised the tool's potential for bias.[13] The IRS eventually reversed its plans and now offers an identity verification tool that does not involve facial recognition software. But even after this controversy, other federal agencies, including the US Patent and Trademark Office, are still moving forward with plans to use the same software.[14]

The US Congress has recently turned serious attention to a potential federal privacy regulation bill that would cover many contexts, including facial recognition.[15] The bill's political future is uncertain, but the proposed language would place restrictions on the purposes for which companies could collect certain data, including facial recognition data, requires privacy policies, requires consent from consumers,

[10] Federal Trade Commission, 'FTC finalizes settlement with photo app developer related to misuse of facial recognition technology' (27 May 2021), www.ftc.gov/news-events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology.

[11] 117th Congress Facial Recognition and Biometric Technology Moratorium Act of 2021, S.2052. This bill was not enacted into law during the 117th Congress. On March 7, 2023, the bill was re-introduced for consideration in the 118th Congress. 118th Congress Facial Recognition and Biometric Technology Moratorium Act of 2023, S.681.

[12] US Government Accountability Office, 'Facial recognition technology: Current and planned uses by federal agencies' (24 August 2021), www.gao.gov/products/gao-21-526.

[13] ACLU, 'Coalition letter on government use of facial recognition identify verification services' (14 February 2022), www.aclu.org/letter/coalition-letter-government-use-facial-recognition-identify-verification-services.

[14] Alessandro Mascellino, 'USPTO to start verifying identities, including with biometrics, for trademark submission' (1 July 2022), BiometricUpdate.com, www.biometricupdate.com/202207/uspto-to-start-verifying-identities-including-with-biometrics-for-trademark-submission.

[15] 117th Congress American Data Privacy and Protection Act 2022.

https://doi.org/10.1017/9781009321211.018 Published online by Cambridge University Press

and prohibits forms of algorithmic bias. Again, this bill would apply to FRT, but also to much wider categories of data. Similarly, the Federal Trade Commission (FTC) has recently announced a potential proposed rulemaking relating to 'Commercial Surveillance and Data Security' in which the Commission is considering, among many other issues, 'limiting commercial surveillance practices that use or facilitate the use of facial recognition, fingerprinting, or other biometric technologies'.[16] As with legislative proposals, the future of this potential rulemaking is uncertain.

15.4 REGULATING FACIAL RECOGNITION TECHNOLOGY IN THE UNITED STATES

States and localities have a primary advantage over the federal government when regulating new technologies: They can usually get regulations on the books faster. And, indeed, states and localities have taken an interest in regulating FRTs, but these non-federal approaches have been varied and fluid. FRT has many uses, so regulatory approaches target a similarly broad span of conduct. Some states regulate government or law enforcement use of FRT.[17] Some only regulate a sub-set of government use, such as banning use of facial recognition on drivers' licences or on police body cameras.[18] Other states regulate the technology only as applied to vulnerable populations, although the efficacy of the laws varies.[19] Yet other states regulate commercial applications.[20]

[16] Federal Trade Commission, 'FTC explores rules cracking down on commercial surveillance and lax data security practices' (11 August 2022), www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

[17] Washington, Oregon, California, Colorado, and Alabama all have limited government actor or police use. Up to date information about state regulation of facial recognition technology can be found at www.banfacialrecognition.com/map/.

[18] Oregon's regulation only encompasses the technology applied to drivers licenses. California's applies to police body cameras. See City of Portland, Oregon, 'City Council approves ordinances banning use of face recognition technologies by City of Portland bureaus and by private entities in public spaces' (9 September 2020), Portland.gov, www.portland.gov/smart-city-pdx/news/2020/9/9/city-council-approves-ordinances-banning-use-face-recognition#:~:text=The%20second%20ordinance%20will%20go,and%20visitors%2C%20first%20and%20foremost; Jeffrey Dastin, 'California legislature bars facial recognition for police body cameras' (12 September 2019), *Reuters*, www.reuters.com/article/us-california-facial-recognition/california-legislature-bars-facial-recognition-for-police-body-cameras-idUSKCN1VX2ZP.

[19] New York's regulation bans use of the technology in schools. Colorado's regulation includes a moratorium on new facial recognition technologies in schools for a period of time. *See* Chris Burt, 'New York school districts plan facial recognition security despite ban' (29 June 2022), BiometricUpdate.com, www.biometricupdate.com/202206/new-york-school-districts-plan-facial-recognition-security-despite-ban; Rachel Sandler, 'New York issues first-in-nation moratorium on facial recognition in schools' (22 December 2020), *Forbes*, www.forbes.com/sites/rachelsandler/2020/12/22/new-york-issues-first-in-nation-moratorium-on-facial-recognition-in-schools/; Linn F. Freedman, 'Colorado law restricts use of facial recognition technology by government agencies' (2022) XII *National Law Review* 12.

[20] Illinois and Texas both require informed consent before private actors can deploy facial recognition technology. *See also* 740 Illinois Compiled Statutes 14 and what follows (2008); Texas Business & Commerce Code Annotated s 503.001 (West 2017).

https://doi.org/10.1017/9781009321211.018 Published online by Cambridge University Press

Illinois's BIPA (2008) was one of the first state regulations of commercial use of FRT, although the bill encompasses more than just facial recognition. Before a private entity collects biometric information, the law requires (1) notice to the consumer, (2) informed consent from the consumer, (3) written policies about retention and destruction, and (4) limits retention of and profit-making from that information.[21] Suing under BIPA, consumers reached a landmark $650 million settlement against Facebook for using FRT on photos uploaded to the site without consumer consent.[22] In another major lawsuit, plaintiffs sued Clearview AI, a company that provided facial recognition software to law enforcement agencies and sector companies, under BIPA. Clearview attempted to argue that its activities – selecting and curating facial images – were protected under the First Amendment in the same way a search engine's results might be.[23] But the suit settled, and the terms of the settlement prohibit Clearview AI from selling its database to most private companies.[24]

Other states have comprehensive privacy laws that cover facial recognition data. California's comprehensive privacy law, the California Consumer Privacy Act, for example, applies to facial recognition data, requiring companies to conform to certain obligations, including giving the consumer notice, access, and the right to have the data deleted.[25] Texas and Virginia also have some of their own state privacy laws that apply to biometric information.

State laws that allow consumers to sue companies face two possible hurdles as federal regulation catches up. The first is pre-emption, which is when a new federal law essentially is substituted for a state law on the same topic. Pre-emption could happen if federal legislation regulating FRT is passed. But the most recently proposed federal privacy legislation, the American Data Privacy and Protection Act, would *not* pre-empt state laws that solely cover FRTs.[26] BIPA would also remain un-pre-empted in a special carve-out.

State facial recognition laws that end up challenged in federal court – which could happen when a state resident sues a company that is based in another state – face a standing problem. In US law, standing refers to one's legal ability to bring a suit. To

[21] Jason Binimow, 'State statutes regulating collection or disclosure of consumer biometric or genetic information' (originally published 2019), Volume 41 of the 7th series of American Law Reports, Article 4 Section 2, Annotation *2.

[22] Taylor Hatmaker, 'Facebook will pay $650 million to settle class action suit centered on Illinois privacy law' (1 March 2021), TechCrunch, https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/.

[23] Jameel Jaffer and Ramya Krishnan, 'Clearview AI's first amendment theory threatens privacy – And free speech, too' (17 November 2020), *Slate*, https://slate.com/technology/2020/11/clearview-ai-first-amendment-illinois-lawsuit.html.

[24] Cyrus Farivar, 'Clearview AI settles facial recognition suit with ACLU, will alter some practices' (9 May 2022), *Forbes*, www.forbes.com/sites/cyrusfarivar/2022/05/09/clearview-ai-facial-recognition-suit-with-aclu/; *American Civil Liberties Union, et al.*, v. *Clearview AI, inc.* (case documents available at www.aclu.org/cases/aclu-v-clearview-ai) (citation pending).

[25] California Civil Code s 1798.100 and what follows.

[26] 117th Congress American Data Privacy and Protection Act 2022.

https://doi.org/10.1017/9781009321211.018 Published online by Cambridge University Press

have standing, a person must typically have suffered a concrete injury. Under BIPA and other state FRT laws, an injury might be defined as use of biometric data without consent. Federal courts have split on whether such an injury is concrete enough to satisfy the federal requirements for standing.[27]

State regulation of police or other government actors within its own borders will not face pre-emption or standing problems. Vermont's law regulating police use of FRT, as one of the most comprehensive such laws, provides an example at one end of the spectrum of regulation. Vermont's law is straightforward: With one exception (child sexual exploitation), until otherwise approved by the legislature, police may not use FRT or information derived from such technology.[28] But Vermont is an outlier: At the other end of the spectrum, some states, such as Oregon, only regulate certain police or government use of FRT. For example, Oregon's law prevents FRT from being used in conjunction with police body cameras.[29]

State regulation of this technology continues to be fluid. Many state and local regulations have taken the form of moratoriums with sunset provisions, merely delaying an ultimate decision about regulation until a future date. Others have already added exceptions to their bans, as in the case of Vermont. The Vermont legislature added an exception to its ban on police use of FRT in all circumstances.[30] Now, police can use the technology in cases involving sexual exploitation of children.[31] And Virginia repealed its de facto ban on police use of the technology a little more than a year after the ban was passed.[32] As of July 2022, police in Virginia can use facial recognition software in certain investigatory circumstances, with 'reasonable suspicion', and only if the software achieves an accuracy score of at least 98 per cent (measuring true positives) on NIST metrics, across all demographic groups.[33] The new Virginia law demonstrates the interplay between state and federal regulation: A state law uses a federal standard to guide the technology's use within its borders.

States, cities, and other localities have also enacted regulations on FRT use within their borders. These efforts are part of a broader trend in localities regulating the use of law enforcement technology. Advocates argue that the benefits of such governance include expanded democratic control over technology, improved responsiveness to changing technology, and more timely governance than post-hoc

[27] Carmen Sobczak, 'BIPA and Article III standing: Are notice and consent more than "bare procedural" rights?' (2020) 35 *Berkeley Technical Law Journal* 1391.

[28] 2020 Vermont Acts and Resolves 799 s 14.

[29] 2019 Oregon Revised Statutes s 133.741.

[30] ACLU, 'ACLU of Vermont statement on the enactment of S.124, the nation's strongest statewide ban on law enforcement use of facial recognition technology' (8 October 2020), www.acluvt.org/en/news/aclu-vermont-statement-enactment-s124-nations-strongest-statewide-ban-law-enforcement-use.

[31] 2020 Vermont Acts and Resolves 799.

[32] Denise Lavoie, 'Virginia lawmakers ban police use of facial recognition' (29 March 2021), *APNews*, https://apnews.com/article/technology-legislature-police-law-enforcement-agencies-legislation-033d77787d4e28559f08e5e31a5cb8f7.

[33] 2020 Vermont Acts and Resolves 799.

rules developed through challenges brought through criminal litigation.[34] At least sixteen localities throughout the United States had passed facial-recognition specific regulations as of July 2022, with others having comprehensive police surveillance regulations that also apply to facial recognition.[35]

Both states and localities can regulate technology such as facial recognition in ways and at speeds that the federal government cannot. And experimentation with regulation of such technology at state and local level demonstrates ways in which these governance units are the laboratories of democracy. At the same time, the impact of these laws is limited to the boundaries of states and localities, affecting fewer people than federal regulation would. And states and local governments have their own types of problems with interest capture, raising concerns that, for instance, large companies might be able to outgun local privacy advocates. Local and state regulations are also much more easily reversible than certain federal regulations, as we have already seen with facial recognition regulation in some states and cities.

15.5 ISSUES ON THE HORIZON

Prediction is an always-fraught, if often necessary, endeavour. When it comes to predicting the future of FRT, and regulation of FRT, in the United States, it is more fraught than ever. US legal and political landscapes today are tempestuous, perhaps nowhere more so than where they relate to technology. There has been growing concern about technology in recent years on both the political left and the political right – albeit animated by very different concerns. At the same time, recent judicial decisions have made the prospects of regulation less, not more, likely. A number of issues relating to FRT that are on the horizon are identified and discussed here.

We start with topics that are most likely to be discussed but that also seem least likely to actually translate into action: Federal legislation or regulation intended to broadly limit or even prohibit the use of FRT.[36] Such legislation is unlikely to come to pass in the United States without a strong bipartisan coalition supporting

[34] See, e.g., Mailyn Fidler, 'Local police surveillance and the administrative Fourth Amendment' (2020) 36 *Santa Clara High Technology Law Journal* 481; Barry Friedman and Maria Ponomarenko, 'Democratic policing' (2015) 90 *NYU Law Review* 103; Vincent Sutherland, 'The master's tools and a mission: Using community control and oversight laws to resist and abolish police surveillance technologies' (2023) 70 (2) *UCLA Law Review*.

[35] See www.banfacialrecognition.com/map/ for an updated list of facial recognition local regulations; see also Mailyn Fidler, 'Fourteen places have passed local surveillance laws. See how they're doing' (3 September 2020), Lawfare, www.lawfareblog.com/fourteen-places-have-passed-local-surveillance-laws-heres-how-theyre-doing.

[36] For examples of calls for such regulations, see, Evan Selinger and Woodrow Hartzog, 'The inconsentability of facial surveillance' (2019) 66 *Loyola Law Review* 101, 102; Woodrow Hartzog and Evan Selinger, 'Facial recognition is the perfect tool for oppression' (2 August2018), *Medium*, https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66&gt – this proposes an outright ban on the use of facial recognition technology; Lindsey Barrett, 'Ban facial recognition technologies for children-and for everyone else' (2020) 26 *Boston University Journal of Science & Technology Law* 223.

its adoption. Given the potential for abuses of FRT by the government and the American tradition of scepticism of government power, an outside observer might think this coalition would readily manifest. But there is strong countervailing support for law enforcement and 'law and order' policies. Narratives about the use of FRT to find missing children and track dangerous criminals – whether substantively valid or not – are likely to have great valence in policy discussions and make it unlikely that a necessary coalition will be able to form.

The dynamics are somewhat different when it comes to the potential for administrative regulation of FRT. Regulatory agencies enjoy some insulation from the political process: Congress has already delegated authority to agencies that may empower them to adopt regulations. The political question is therefore more limited to whether an agency's leadership is interested in adopting given regulations. In the case of the current FTC, for instance, it is overwhelmingly clear that the agency is interested in adopting rules that could address the use of technologies such as FRT: as discussed previously, the Commission has recently issued an Advance Notice of Proposed Rulemaking relating to Commercial Surveillance and Data Security practices, which includes some consideration of rules that could limit, or at least affect, the use of FRT in the United States.

However, while the FTC may have the political will to adopt such regulations, it is less clear whether the courts will hold that it has the legal authority to do so. Recent trends in US administrative law have been hostile to expansive claims of authority by federal agencies, especially when adopting regulations that would affect entire industries or areas of commerce.[37] It does seem likely that the FTC would be able to adopt narrow rules that prescribe specific, and likely modest, requirements governing the use of FRT; it seems less likely, however, that the courts would uphold any broad regulatory moves that FTC makes, especially were they so broad as to proscribe the use of FRT or similar technologies.

Looking beyond the borders of the United States, questions will likely arise about whether US law can be harmonised with, or otherwise show comity for, FRT regimes adopted in other countries. This will most likely come up in the context of European regulations. The relationship between US and European regulations is likely to follow much the same trajectory as we have seen in the context of privacy regulations – most notably the challenges to the Safe Harbor and Privacy Shield in the *Schrems* litigation. To the extent that European regulations are based in European conceptions of fundamental rights, those regulations are likely to conflict with US regulations; and conversely, US regulations based in the First and Fourth Amendments are likely to conflict with European regulations.

The examples here are all likely to dominate discussion about FRT, but also seem unlikely to prove viable pathways for such regulation. This does not mean, however, that FRT regulation is unlikely. Indeed, as discussed in Sections 15.2 and 15.3, we are

[37] *See West Virginia* v. *EPA*, [2022] 597 U.S. (*Law Reports* citation pending).

https://doi.org/10.1017/9781009321211.018 Published online by Cambridge University Press

already seeing FRT regulation at federal and state level. And these are also where we are likely to see substantive debates over the scope, impacts, and implementation of such regulations. Such regulations, and debates, are likely to focus on government use of FRT, government access to information collected through private FRT systems, specific uses of FRT or FRT-related practices, and generally issues arising from the relationship between competing states' laws and the federal regulations.

We are likely to continue to see governmental entities at federal, state, and local level consider whether, and under what circumstances, to use FRT. It is unlikely that there will be significant uniformity in approaches adopted. While most of these efforts will result from legislatures acting to limit the scope of their executive's authority – for instance, by prohibiting the use of FRT by law enforcement, school systems, or other public entities – it is also conceivable that some states could find their hands forced. State constitutions embody myriad conceptions of privacy. It is certainly possible that use of FRT by governmental entities may be deemed to violate constitutional privacy protections in some states, and it would not be surprising to see litigation pushing theories such as this in coming years.

To take an example, a federal judge in Ohio recently held that a public school's use of proctoring software that uses a student's computer's video camera to 'scan' the room in which they are taking an exam may constitute a search of private property in violation of the Fourth Amendment.[38] Similar claims could potentially be levelled at FRT systems: if courts hold that they enable pervasive tracking of individuals on an automated basis, they might be deemed to violate a reasonable expectation of privacy. Litigation challenging the constitutionality of such systems is at least possible, and probably likely, at both the state and federal level. Such restrictions would be unlikely to apply on government property or in government facilities, but could easily apply in private facilities or even in public places.

Government access to private FRT systems or data, discussed earlier, will also continue to be an issue in coming years. Here we are already seeing moves to limit government access to these systems, including requirements for judicial oversight of the processes by and circumstances in which law enforcement requests these materials. Of all efforts to regulate FRT in the United States, this is likely the least controversial and the most likely to continue to develop apace.

Limitations on government access often operate in practice by forbidding private entities from disclosing information to law enforcement. These regulations might not directly prohibit government use of information unlawfully disclosed to law enforcement (although, increasingly, they do). In this sense, they illustrate a general approach to regulating the private use of FRT: Most regulation will not prohibit the general development or use of FRTs; rather, restrictions on private entities will likely focus on specific use cases (e.g., disclosure of information generated by an

[38] *Ogletree v. Cleveland State University*, ___ F.Supp.3d ___, 2022 WL 17826730 (N.D. Ohio, December 20, 2022).

FRT to law enforcement). One can speculate on a range of use cases for FRT that could be subject to regulation. For instance, the use of FRT to help evaluate job candidates could conceivably be regulated – depending upon the circumstance, such uses could even already run afoul of existing anti-discrimination laws.

A final set of issues on the horizon relate to the interplay between potential FRT regulations at the state and federal level. Importantly, these issues may arise in a range of contexts adjacent to FRT regulations. For instance, state-level privacy regulations that require disclosure of information collected about individuals, or minimisation of such information, would easily affect the technological and business practices of firms using FRT. If multiple states adopt conflicting FRT-related regulations there will be complex questions about how those regulations are applied in practice. And if the federal government also adopts other regulations – or if it deliberately decides not to adopt such regulations – there will be complex questions over whether the federal approaches to FRT pre-empt state-level regulations. On balance, this is all to say that regulation of FRT in the United States, to the extent that there are efforts to adopt such regulations, will remain fraught and unsettled for many years to come.

15.6 CONCLUSION

This chapter has considered the state of FRT regulation in the United States. The United States is not a monolith. It is a federation comprising a central federal authority along with more than fifty states and territories and hundreds of localities – all of which have legislative, executive, and administrative regulatory apparatuses. But they are also governed by the federal Constitution and share common foundational values. These values tend to limit the extent to which FRT can be regulated as a matter of law, as well as carrying a general disposition towards light-touch regulations.

This is not to say that FRT is, or will remain, entirely unregulated in the United States. For instance, the same disposition against government interference in private matters has already begun to result in regulations restricting the use of FRT by government actors. We are likely to see more of these regulations, including restrictions on private parties sharing access to their FRT systems with state actors (much in the same way that laws such as the Stored Communications Act prevent electronic communications services from sharing the content of communications with law enforcement without a court-issued warrant).

Outside limited circumstances, however, more expansive regulation of FRT in the United States is unlikely in the foreseeable future. While Congress and the Federal Trade Commission are both currently considering privacy regulations that might bear upon FRT to some extent, it is uncertain whether these efforts will be successful. Even if they are, those regulations will almost certainly face serious challenges under contemporary understandings of the United States Constitution, so will be subject to extensive and lengthy litigation. The US approach to FRT regulation is ultimately governed by broader US conceptions about privacy and regulation generally, which remain narrower than other jurisdictions and contested.

https://doi.org/10.1017/9781009321211.018 Published online by Cambridge University Press