EMERGING LAWS AND NORMS FOR AI FACIAL RECOGNITION TECHNOLOGY

Alison Lawlor Russell

The explosive growth of facial recognition technology has exceeded the ability of existing legal frameworks related to privacy around the world to adequately safeguard individuals and human rights. Laws governing the use of this technology and collection of biometric information range from nonexistent in some countries to robust in others, and in some cases, these laws favor nondemocratic regimes and threaten individuals' privacy. At this critical juncture, the United States should work with its Allies and partners to establish and promote norms protecting human rights as governments and the private sector take advantage of this increasingly robust technology.

Innovation and technological development proceed much faster than policy or norm development, and it can be a challenge for decisionmakers to modernize legislation to keep pace with social and technological changes. The adoption of a new technology, in the field of biometrics for example, leads to new practices. New laws may be implemented alongside new technologies, which in turn may affect norms and expectations of surveillance and privacy. With the rise of artificial intelligence (AI) and surveillance technologies, many governments have invested in and implemented facial recognition surveillance technology for a variety of reasons, such as public safety, pandemic-related policies, counterterrorism efforts, and domestic control.

Since 2016, there has been a dramatic increase in the use of such surveillance technologies, and it is unclear what laws and policies are being created to govern their use and the use of other biometric data, particularly in regard to privacy and human rights. In recognition of this, the UN High Commissioner for Human Rights called for a moratorium in 2021 on the use of artificial intelligence and facial recognition in public spaces until safeguards for rights are established.[1]

Dr. Alison Russell is the chair and associate professor of the Political Science & Public Policy Department and the director of the international studies program at Merrimack University, Massachusetts. She is the author most recently of Strategic A2/AD in Cyberspace *(Cambridge University Press, 2017).*

[1] Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, A/HRC/48/31, United Nations (website), September 13, 2021, https://www.ohchr.org/.

Facial recognition technology impedes on individual privacy, which is a human right that includes privacy of one's information and from observation, the moral values of autonomy—where an individual can make choices consistent with their sense of self, not because they are being monitored and perhaps threatened with punishment—and privacy for personal projects and plans. Collective privacy maintains a power balance between the state and society, particularly in liberal democratic regimes.

The impact of surveillance technology's global proliferation on laws and norms concerning privacy and human rights presents a new dimension for how technology adoption and risk are considered. As new laws are constructed, new norms will also emerge in international law applicable to cyberspace and technology.

By examining the use of AI facial recognition technology (FRT) by individual countries, this article observes how different states approach their obligations regarding privacy and human rights and looks for patterns or trends that may impact global norm development for this technology. An analysis of emerging FRT laws and policies in various countries finds both democratic and nondemocratic nations are approaching the technology in a number of different ways, with some adopting laws to govern the use of this technology.

At the same time, many countries, regardless of government type, have yet to adopt such laws, and it is unclear if and when they will. Current laws that protect human rights and privacy are thus insufficient to address critical aspects of this technology. Further, and critically, democracies that have failed to create laws and policies protecting citizens from FRT have promulgated legal voids in a similar manner as nondemocratic regimes that seek to protect those in power.

Methodology

This article employs a comparative approach to answering the main questions and investigating the conditions that may contribute to countries adopting laws that restrict privacy and expanding the use of facial recognition technology. Nineteen countries plus the European Union (EU) were selected to represent diversity in regime type (democracies and nondemocracies), geographic location, and population size.

This research is primarily focused on national laws that govern the state's use of FRT, but where possible, it also collects data on how this technology is being used within the countries and any restrictions of private-sector use of the technology. In addition, it is noted when countries regulate 1:1 and 1:N FRT differently. With 1:1 FRT, a subject's photo is matched to a specific image in a database to determine if the images are of the same person and is frequently used by applications for authentication or verification during a login process. In contrast, 1:N FRT is used to compare the subject's photo to multiple images in a database to see if any of them are a match.[2]

This research is concerned with AI facial recognition technology legislation since 2016. That year is not a decisive turning point, but rather an approximate midway

[2] "Accurate 1:1 Face Matching," FACIA (website), accessed April 24, 2024, https://facia.ai/.

point in the recent global development and proliferation of FRT. Facial recognition technology using AI in social media began in 2010 with Facebook allowing users to tag and identify people in photos, and use of the technology accelerated from there. The iPhone X, released in 2017, used FRT to unlock the phone, thereby bringing this technology into the daily lives of people.[3]

The year 2016 was selected as a reference point because while AI FRT was still relatively new at that time, it had been in existence long enough for governments to experiment integrating it with existing practices as well as to begin considering the legal implications of it. For example, in 2011 the Federal Bureau of Investigation launched the FRT component of its Next Generation Identification Interstate Photo System (NGI-IPS) with a database of over 10 million images. In 2016, the Government Accountability Office revealed that the NGI-IPS also gained access to and included over 400 million noncriminal civilian images in its database. By 2019, the database had over 640 million images.[4]

Many countries have data protection laws that were passed in the late 1990s and early 2000s. Yet laws created in that time period are less likely to address concerns that are relevant for the way FRT is deployed in the public and private sector today. Specifically, most do not address the wide-scale use of biometric data collection and AI, the need for oversight, or the requirements for storage and protection of sensitive biometric data, such as fingerprints, iris scans, and facial images.

As the technology evolved into the 2010s and beyond, there was a growing recognition of the capabilities of AI-enabled FRT and the legislative measures that might be needed to regulate its use. The COVID-19 pandemic and the use of this technology to enforce lockdown measures in many countries accelerated the use of AI-enabled FRT and the public's awareness of it.

Additionally, the technology has also evolved, further surpassing previous limitations of machine-learning models, which struggled with effectiveness when using large databases. These limitations have been overcome by FRT models that harness deep learning and make them more effective with larger databases, including models that scrape vast numbers of images from social media and the internet as a whole.[5] As this technology has advanced, so too have the efforts of activists and lawyers who are concerned with its impacts on privacy, democracy, and human rights.

[3] "A Brief History of Facial Recognition," NEC (website), May 12, 2022, https://www.nec.co.nz/.

[4] Samuel Brice, "A Short History of Facial Recognition," Medium, November 7, 2020, https://samdbrice.medium.com/.

[5] FACIA, "Face Matching."

Country Studies

Argentina

In Argentina, city, state, and federal legislatures coexist and sometimes contradict each other. Argentina's federal law on data protection, enacted in 2000, fails to consider AI FRT, other biometric data, or the collection of other sensitive personal data.[6] In 2019, Buenos Aires implemented the Fugitive Facial Recognition System, but it was suspended in 2020 during the COVID-19 pandemic due to reduced effectiveness with masked faces.[7]

In September 2022, a trial judge declared this system unconstitutional because of the privacy risks it posed. Specifically, the judge found that the rights to privacy, intimacy, and data collection have collective relevance in the context of public surveillance and law enforcement. The court prohibited the operation of the Fugitive Facial Recognition System until the control and oversight mechanisms required by law are put in place.[8] Other cities currently have plans to move ahead with different facial recognition systems.[9]

Australia

In Australia, the government and civil society use facial recognition technology widely. There are limited restrictions on it and no AI-specific legislation. The proposed Identity Verification Services legislation calls for the curtailing of 1:1 FRT, such as those employed by apps for authentication during the login process. It does not regulate the use of biometric information and identity matching that falls outside of the scope of the legislation, such as 1:N FRT that is already in widespread use.[10] New legislation to regulate the "high-risk" usage of AI, such as in law enforcement or hiring practices, while minimizing restrictions on "low risk" usage, such as with chatbots, is under consideration.[11]

[6] Carolina Caeiro, *Regulating Facial Recognition in Latin America* (London: Chatham House, November 11, 2022), https://www.chathamhouse.org/.

[7] Maria Badillo, "Judge Declares Buenos Aires Fugitive Facial Recognition System Unconstitutional," *Future of Privacy Forum* [blog], September 30, 2022, https://fpf.org/.

[8] Badillo; and *Juzgado de 1ra Instancia en lo Contencioso Administrativo y Tributario No 4 Secretaría* N°7 *Observatorio de Derecho Informatico Argentino O.D.I.A. y Otros contra GCBA sobre Amparo – Otros* (Buenos Aires, Argentina: Poder Judicial Ciudad de la Buenos Aires, September 2022), https://www.cels.org.ar/.

[9] Karen Naundorf, "The Twisted Eye in the Sky over Buenos Aires," *Wired*, September 13, 2022, https://www.wired.com/.

[10] Shivaune Field, "Facial Recognition Is Everywhere – But Australia's Privacy Laws Are 'Falling Way Behind,' " *Forbes*, September 28, 2023, https://www.forbes.com.au/.

[11] Phil Mercer, "Australia Outlines Plan to Manage the Rise of Artificial Intelligence," VOA [Voice of America], January 17, 2024, https://www.voanews.com/; and *Government Response to the Privacy Act Review Report* (Barton, Australia: Australian Government, Attorney General's Department, September 28, 2023), last updated February 16, 2024, https://www.ag.gov.au/.

Belgium

Belgium banned the use of facial recognition and other biometrics-based video surveillance technology by the private sector for nonpolice use in 2018.[12] Yet there are no laws that govern the use of FRT by the government. There has been public debate and demands by human rights groups to regulate the government's use of facial recognition technology, but legislation has not been passed yet.[13]

Brazil

Brazil's General Data Protection Law makes data protection a fundamental right in Brazil, but it does not apply to data collection carried out for the purposes of public safety, national security, and defense or for investigation or prosecution of criminal offenses.[14] There have been several federal commissions formed to advise on the drafting of a bill to regulate AI as well as civil-society led demonstrations against the use of FRT in public spaces. The existing national legislation enshrines the right to privacy, so any future discussions and legislation on FRT will be grounded in the General Data Protection Law and protection of constitutional rights.[15]

Canada

Canadian law requires express opt-in consent for the use of FRT by private companies. Privacy regulators have called for more national legislation to regulate the use of this technology in Canada, as some laws are local or provincial. New legislation that addresses the shortcomings of Bill C-27, which includes the Consumer Privacy Protection Act and the Artificial Intelligence and Data Act, is before the Canadian parliament for consideration in 2024. Yet privacy experts charge that the proposed amendments to the existing legislation are inadequate because they not only fail to provide special protections for biometric information, but they also do not flag biometric data as "sensitive information" or define sensitive information at all.[16]

[12] Charles Rollet, "Belgium Bans Private Facial Surveillance," IPVM, July 6, 2018, https://ipvm.com/.

[13] Act on the Protection of Natural Persons with Regard to the Processing of Personal Data [unofficial translation], Data Protection Authority, Government of Belgium, July 30, 2018, https://www.dataprotectionauthority.be/; and Maïthé Chini, " 'Protect My Face': Facial Recognition Petition Demands Ban in Brussels Public Spaces," *Brussels Times*, March 15, 2023, https://www.brusselstimes.com/.

[14] "Data Protection Laws of the World: Brazil," DLA Piper, last modified January 28, 2023, https://www.dlapiperdataprotection.com/; and Rennó Penteado Sampaio Advogados, trans., "Brazilian General Data Protection Law (LGPD, English translation)," IAPP [International Association of Privacy Professionals], October 2020, https://iapp.org/.

[15] Caeiro, *Regulating Facial Recognition*.

[16] Howard Solomon, "Proposed Privacy, AI Legislation Doesn't Limit Business Use of Facial Recognition, Complain Rights Groups," IT World Canada, November 1, 2023, https://www.itworldcanada.com/.

China

China is the most surveilled country in the world and helped to fuel the explosion of facial recognition technology globally. In August 2023, the Chinese government issued rules to oversee the management of FRT. The Cyberspace Administration of China stated that FRT can only be used when there is a specific purpose and necessity and must be accompanied by strict protective measures. The Cyberspace Administration states biometric data should only be used with the individual's consent and other nonbiometric means of identification should be used when they are equally effective.[17] FRT should be reserved for the purpose of maintaining public safety, although there are circumstances in which administrative use of this technology does not require individual consent.[18]

This law attempts to protect citizens from capitalist surveillance but does not restrict the use of government surveillance or use of FRT on the general population. It also encompasses broad exceptions for national security and public safety. Overall, it enables a continued state of surveillance and overt government exceptionalism to restrictions on individuals' privacy, but it also grants individuals new rights to protect their privacy and personal data from businesses that stand to profit from them.[19]

European Union

In December 2023, the EU agreed to new rules to regulate the use of AI and biometric surveillance. The regulations are being hailed as a regulatory breakthrough and a global standard.[20] According to the new agreement, governments can only use real-time biometric surveillance in public spaces in certain circumstances, such as "the prevention of genuine, present, and foreseeable threats . . . and searches for people suspected of the most serious crimes." The indiscriminate scraping of facial images from the internet or closed-circuit television (CCTV) is prohibited, and consumers "would have the right to launch complaints and receive meaningful explanations."[21]

[17] "Provisions on Security Management in the Application of Facial Recognition Technology (Trial) (Draft for Comment)," China Law Translate, August 2023, https://www.chinalawtranslate.com/; and Josh Ye, "China Drafts Rules for Using Facial Recognition Technology," Reuters, August 7, 2023, https://www.reuters.com/.

[18] Evelyn Cheng, "China Releases Plans to Restrict Facial Recognition Technology," CNBC, August 8, 2023, https://www.cnbc.com/.

[19] Johanna Costigan, "New Chinese Facial Recognition Regulations Could Shield Citizens from Surveillance Capitalism," *Forbes*, August 9, 2023, https://www.forbes.com/.

[20] Adam Satariano, "E.U. Agrees on Landmark Artificial Intelligence Rules," *New York Times*, December 8, 2023, https://www.nytimes.com/.

[21] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, February 2, 2024, EU Artificial Intelligence Act (website), https://artificialintelligenceact.eu/; and Foo Yun Chee, Martin Coulter, and Supantha Mukherjee, "Europe Agrees Landmark AI Regulation Deal [*sic*]," Reuters, December 11, 2023, https://www.reuters.com/.

The European Parliament voted on the final legislation in March 2024, which will enter into force in summer 2024.[22]

France

In March 2023, France passed a controversial law to allow police to use surveillance cameras and AI for public safety ahead of the 2024 Olympics. The law allows law enforcement to identify threats "such as dangerous crowd movements and unattended bags," but facial recognition technology is not permitted.[23] France's new law varies in certain ways from the EU's new AI Act, so there may be a potential clash between EU and French laws.[24]

India

India does not have laws that directly govern the use of facial recognition technology, as the Personal Data Protection Bill of 2019 and Information Technology Act of 2000 do not address it.[25] AI FRT is used in many parts of the country to solve crimes. The government is promoting a "smart cities" approach through the use of drones, AI-enabled CCTV, and FRT that appears to enjoy support across the political spectrum.[26]

In 2022, the Criminal Procedure (Identification) Act took effect, expanding the government's authority to collect biometric and behavioral data for people who are arrested, have court dates, or are convicted criminals. India's National Crime Records Bureau is looking to build one of the largest facial recognition systems in the world. It seeks to create a database of "mugshots of criminals, passport photos, and images collected by agencies such as the Ministry of Women and Child Development," that could be matched to images from CCTV cameras across the country.[27]

[22] Caitlin Andrews, "European Parliament Approves Landmark AI Act, Looks Ahead to Implementation," IAPP, March 13, 2024, https://iapp.org/; Joe Jones, "EU AI Act: Next Steps for Implementation," IAPP, last updated January 2024, https://iapp.org/; and Lisa Peets, Marianna Drake, and Marty Hansen, "EU AI Act: Key Takeaways from the Compromise Text," Covington, *Inside Privacy* [blog], February 28, 2024, https://www.insideprivacy.com/.

[23] Relatif aux Jeux Olympiques et Paralympiques De 2024 - (N° 809) [Relating to the 2024 Olympic and Paralympic Games - (No. 809)], Amendment No. CL400, National Assembly of the Republic of France, March 4, 2023, https://www.assemblee-nationale.fr/; and Peter O'Brien, "France Passes Controversial AI Surveillance Bill Ahead of 2024 Olympics," France 24, March 24, 2023, https://www.france24.com/.

[24] Masha Borak, "French Senate Votes in Favor of Public Facial Recognition Pilot," BiometricUpdate.com, June 14, 2023, https://www.biometricupdate.com/.

[25] Pavan Duggal, "Facial Recognition in India – Some Legal Challenges," CyberLaws.net, accessed April 24, 2024, https://cyberlaws.net/; and Rishabh R. Jain, "Facial Recognition Wielded in India to Enforce COVID Policy," AP, December 20, 2022, https://apnews.com/.

[26] Jain.

[27] Julie Zaugg, "India Is Trying to Build the World's Biggest Facial Recognition System," CNN, October 18, 2019, https://www.cnn.com/.

Israel

In September 2023, the Israeli government received cabinet approval for its bill to place FRT cameras in public places during events, such as protests, as long as a police officer is convinced it does not amount to the "undue invasion" of any individual's privacy.[28] The legislation allows for the use of facial recognition cameras and their data "to prevent, thwart, or uncover serious crime" and the individuals involved.[29]

Human rights organizations, such as Amnesty International, have alleged that Israel is increasingly using FRT to surveil and track movements of Palestinians in the West Bank and East Jerusalem.·

Since the attacks on October 7, 2023, the Israeli military has used an expansive facial recognition program to search for hostages taken by Hamas, track Palestinians in Gaza, and identify anyone with ties to Hamas or other militant groups. Yet the program has, at times, wrongly identified civilians as militants. The Israeli Defence Forces does not dispute the use of the mass surveillance program but states it is carrying out "necessary security and intelligence operations."[30]

Japan

Japanese technology is often at the forefront of innovation, and FRT is widespread in Japan. With the addition of its new extension, Osaka Station has been billed as the most high-tech train station in the world, with a trial for facial recognition scans for passenger entry underway. In other parts of Japan, drone delivery of medicines is being tested with FRT embedded to verify that an authorized person receives the delivery.[31]

Japan recognizes facial features as biometric data that are protected by the Personal Information Protection Code, which requires consent of the individual. But in practice, the private sector uses facial recognition cameras in large areas where consent of every individual is not possible and police have access to the data.[32] It appears Japan does not have any legal requirements concerning the handling of facial recognition data, except that FRT must be accompanied by a public notice of the purpose of the data, or notification of the subject whose information is being collected.[33]

[28] Josh Breiner, "Israeli Gov't Pushes Bill for Facial Recognition Surveillance Cameras in Public Spaces," Haaretz, September 18, 2023, https://www.haaretz.com/.

[29] Carrie Keller-Lynn, "Ministers Back Bill to Legalize Widespread Police Use of Facial Recognition Tech," *Times of Israel*, September 18, 2023, https://www.timesofisrael.com/.

[30] Sheera Frenkel, "Israel Deploys Expansive Facial Recognition Program in Gaza," *New York Times*, March 27, 2024, https://www.nytimes.com/.

[31] Joel R. McConvey, "Trains, Drones and Robotic Feels: Japan Deploys Facial Recognition across Sectors," BiometricUpdate.com, April 14, 2023, https://www.biometricupdate.com/.

[32] Act on the Protection of Personal Information (Act No. 57 of 2003) [unofficial translation], Cabinet Secretariat [of Japan], 2003, https://www.cas.go.jp/.

[33] Yazukazu Akada, "Review Launched into Rules Governing Facial Recognition Data," *Asahi Shimbun*, December 22, 2021, https://www.asahi.com/; and Sameshima Shigeru, "Privacy Measures of Biometrics Businesses," *NEC Technical Journal* 13, no. 2 (2018), https://www.nec.com/.

Myanmar

In Myanmar, surveillance technology was adopted without public consultation and is used to identify people and license plates. There are over 300 AI-equipped surveillance cameras that are capable of facial recognition across the capital city as part of the Safe City Initiative. National law requires the collection of biometric data when purchasing a smartphone, leading to the creation of a national database on biometric data.[34]

Russia

Russia's Law on Personal Data protects information related to an identifiable person and requires consent of the individual for the collection of biometric data through facial recognition technology. Yet laws on public security and crime prevention, such as the Law on Experimenting with Artificial Intelligence, provide exceptions to this requirement for consent, rendering it ineffective. According to human rights activists, the law does not provide any mechanisms for judicial or public oversight for surveillance collection and technologies and therefore lacks appropriate or sufficient guardrails to prevent the misuse of the technology and data.[35]

Human rights organizations assert that facial recognition technology is widely used throughout Russia with no regulation, oversight, or data protection. Furthermore, Russian authorities have begun to implement silhouette recognition technology in instances when the face is not visible. The lower house of the Duma passed legislation in December 2022 that set up a legal framework for collection, storage, and management of biometric data and outlawed the forceful collection of biometric data—face and voice—from any individual.[36]

South Africa

Facial recognition technology is legal, widespread, and largely unregulated in South Africa. In February 2021, the constitutional court of South Africa found the Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 to be unconstitutional because it failed to provide adequate safeguards to protect the right to privacy.[37]

[34] Katya Pivcevic, "Police Facial Recognition Use in Belarus, Greece, Myanmar Raises Rights, Data Privacy Concerns," BiometricUpdate.com, March 15, 2021, https://www.biometricupdate.com/; and Luana Pascu, "Myanmar to Introduce Mandatory Biometric Data Collection for Massive National Database," BiometricUpdate.com, December 6, 2019, https://www.biometricupdate.com/.

[35] *2022 Country Reports on Human Rights Practices: Russia* (Washington, DC: US Department of State, Bureau of Democracy, Human Rights, and Labor, 2023), https://www.state.gov/.

[36] Ayang Macdonald, "Russian Lawmakers Okay Legal Framework for Biometric Data Collection and Processing," BiometricUpdate.com, December 23, 2022, https://www.biometricupdate.com/.

[37] Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v Amabhungane Centre for Investigative Journalism NPC and Others CCT278/19 & CCT279/19, Constitutional Court of South Africa, February 4, 2021, https://www.saflii.org/.

In May 2021, South Africa's Department of Home Affairs drafted an identity management policy to grant police "unfettered access" to citizens' biometric data without a court order. The policy proposed that all biometric data of all citizens should be centralized in a database and that an automated biometric identification system be created, but South Africa does not have any laws regulating police use of facial recognition software or related surveillance technology.[38]

South Korea

South Korea has promoted facial recognition technology through its ministries and local governments in recent years but does not appear to have laws or policy providing its oversight or regulation. In January 2023, the National Human Rights Commission of Korea warned against the dangers of implementing FRT without legislative regulations in place and asked the speaker of the National Assembly to delay the implementation of this technology in public institutions until a law is created.[39]

The commission recommended to the prime minister that all real-time FRT in public spaces be suspended until relevant laws are created to protect privacy and human rights. Additionally, the commission recommended that real-time facial recognition should be generally prohibited, except in extraordinary circumstances "based on clear and imminent public interest . . . such as searching for missing children."[40]

United Arab Emirates

The United Arab Emirates (UAE) passed a law in February 2021 allowing the use of facial recognition technology in certain private and government sectors to verify the identity of individuals and reduce paperwork.[41] This legislation came after several emirates implemented policies using FRT. In 2021 the UAE implemented a national digital identity and solutions system for citizens and residents, called the "UAE Pass," that uses facial recognition and smartphones to provide government services.[42]

[38] Ayang Macdonald, "South Africa's Proposed New Biometrics Policy Meets Sharp Criticism," BiometricUpdate.com, May 17, 2021, https://www.biometricupdate.com/.

[39] Alessandro Mascellino, "South Korea Privacy Watchdog Warns against Public Facial Recognition Deployments," BiometricUpdate.com, January 25, 2023, https://www.biometricupdate.com/; and Chai Yoon-tae, "Korean Rights Watchdog Advocates Curbs on Government's Use of Facial Recognition Data," *Hankyoreh*, January 26, 2023, https://english.hani.co.kr/.

[40] Chai.

[41] Federal Decree-Law No. 45 of 2021 regarding the Protection of Personal Data ('the Law') [United Arab Emirates], September 20, 2021, https://www.dataguidance.com/; Ayang Macdonald, "UAE Cabinet Approves Trial of Facial Recognition for Private Sector Services," BiometricUpdate.com, February 17, 2021, https://biometricupdate.com/; and Jay Hilotin and Vijith Pulikkal, "UAE Approves Facial Recognition in Some Key Sectors: How the Technology Is Changing Our World," *Gulf News*, March 13, 2021, https://gulfnews.com/.

[42] "UAE Government to Employ Biometric Face Recognition to Register Customers under 'UAE Pass' App," Emirates News Agency, April 4, 2021, https://wam.ae/.

United Kingdom

Facial recognition has been controversial in the United Kingdom for years. There is no specific facial recognition law in the UK, but the Data Protection Act of 2018 establishes some responsibilities surrounding its use.[43] In 2020, a British court ruled that the use of FRT to create a watchlist for the South Wales police force was unlawful and violated the human rights of the people whose data was collected and outlined issues that would need to be addressed for it to be lawful.[44] Privacy and civil liberty groups, experts, and lawmakers have called for a ban on live or real-time FRT in the UK, particularly in public places, because they claim it infringes on human rights and privacy.[45]

United States

The United States does not have federal laws governing the use of FRT, so some states, cities, and counties have developed their own, creating a patchwork of laws throughout the country. Twenty of the 42 federal law enforcement agencies use FRT. The majority of US states do not have restrictions on its use, but thirteen states do—Washington, Vermont, Maine, Virginia, New York, California, New Hampshire, Oregon, Utah, Massachusetts, Illinois, Texas, and Colorado—although these laws vary on whether they prohibit or regulate government or private sector use of FRT.

Cities such as Portland, Oregon and Baltimore have banned commercial use of this technology, while Portland and other cities, including Boston, San Francisco, and New Orleans, have enacted full bans on governmental use of FRT.[46] There have been several proposals in the US Congress to regulate the use of FRT, but none have gained enough support to move forward.[47]

Venezuela

Venezuela does not appear to have any laws or regulations pertaining to facial recognition technology or data protection. The Venezuelan government engages in robust surveillance activities and lacks independent oversight of the state's surveillance of citizens. The Maduro regime requires participation in government surveillance and data

[43] Data Protection Act 2018 [United Kingdom], 2018 c.12, https://www.legislation.gov.uk/.

[44] R v Chief Constable of South Wales Police, (2020) EWCA Civ 1058, https://www.judiciary.uk/; and "Facial Recognition Cameras - What Your Rights Are," *DAS Law* [blog], May 3, 2023, https://www.daslaw.co.uk/.

[45] Matt Burgess, "Police Use of Face Recognition Is Sweeping the UK," *Wired*, November 9, 2023, https://www.wired.com/; and Vikran Dodd, "UK Police Use of Live Facial Recognition Unlawful and Unethical, Report Finds," *Guardian*, October 27, 2022, https://www.theguardian.com/.

[46] Palash Basu and Jenny Holmes, "Facial Recognition Systems Regulation: Outlook for 2022," Bloomberg Law, December 23, 2021, https://news.bloomberglaw.com/.

[47] Tate Ryan-Mosley, "The Movement to Limit Face Recognition Tech Might Finally Get a Win," *MIT Technology Review*, July 20, 2023, https://www.technologyreview.com/.

collection programs to access government services and subsidies, including a virtual wallet to receive pension payments that is integrated with a biometric payment system operated by Banco de Venezuela.[48] Facial recognition technology is used by the government, police, banking, and in transportation, such as at airports and on trains.[49]

Zimbabwe

Zimbabwe also engages in robust surveillance activities yet does not have laws to specifically regulate or limit the use of FRT. Facial recognition technology is being used by government, police, banking, and transportation sectors, such as for buses, trains, and airports.[50] There are no laws that limit or restrict surveillance activities, and FRT is not covered under the Interception of Communications Act (2007), the legislation that legitimized surveillance in Zimbabwe.[51] A data protection law passed in 2021 has been criticized for having multiple shortcomings, while the government maintains that the purpose of surveillance and FRT is to ensure the safety of citizens.[52]

Analysis

An analysis of these 20 countries' regulation of facial recognition technology reveals some countries are making more progress toward regulation than others. Table 1 outlines and summarizes the country-by-country analysis based on the qualitative data presented in the previous discussion. It also incorporates data on the level of democratic governance and more specific information on FRT laws. The table data reflect the presence of national laws or judicial decisions regarding FRT since 2016 and whether these mechanisms protect individual privacy from the government or private sector, prohibit real-time 1:N systems that can be used for mass surveillance—with limited exceptions, such as missing children—or prohibit the scraping of images on the internet to build the database.

The table also shows the presence of meaningful oversight of the use of FRT and whether the new laws provided substantial limitations and oversight of state surveillance and provided avenues of recourse for individuals. It includes data on how democratic the government is in each country, as assessed by Freedom House in its annual

[48] "Venezuela: Freedom on the Net 2022 Country Report," Freedom House, 2022, https://freedomhouse.org/.

[49] Paul Bischoff, "Facial Recognition Technology (FRT): Which Countries Use It? [100 Analyzed]," *Comparitech* [blog], January 24, 2022, https://www.comparitech.com/.

[50] Bischoff.

[51] Interception Of Communications Act (Chapter 11:20) [Zimbabwe], 2007, https://www.law.co.zw/; and "Surveillance and Privacy," MISA Zimbabwe, accessed April 24, 2024, https://zimbabwe.misa.org/.

[52] Data Protection Act (Chapter 11:12) [Zimbabwe], 2021, https://www.dataguidance.com/; Ayang Macdonald, "Zimbabwe Govt Faces Criticism over Biometric Surveillance Project for New Smart City," BiometricUpdate.com, February 28, 2023, https://www.biometricupdate.com/; and "MISA Zimbabwe's Submission on the Surveillance Industry and Human Rights in Zimbabwe," UN Office of the High Commissioner for Human Rights, February 15, 2019, https://www.ohchr.org/.

Freedom in the World report. For the EU, the average democracy score of its members is presented in the table.[53]

Each factor—other than democratic governance—was assigned a score based on a yes/no answer; if the answer was "yes" then the country received a 1, and if the answer was "no" then it received a 0. The exception to this was the United States, which was the only country to receive a partial score (0.5) for presence of national laws on FRT because of the stringent laws in some parts of the country but the dearth of national laws overall. A higher score indicates that the country has taken more measures to protect individuals' privacy from potential abuses using FRT, whereas a lower score indicates fewer national laws to protect individuals' privacy from potential abuses.

[53] *Freedom in the World 2023: Marking 50 Years in the Struggle for Democracy* (Washington, DC: Freedom House, 2023), https://freedomhouse.org/.

Table 1. Facial recognition technology laws by country

Country	Democracy?	New national laws regarding privacy or FRT?	New laws protect individual privacy vis-à-vis the government?	New laws protect individual privacy vis-à-vis businesses?	New laws prohibit real-time FRT?	New laws prohibit 1:N systems?	Laws prohibit the scraping of images from the internet?	Evidence of laws that require meaningful oversight of the use of FRT?	Laws make state surveillance harder?	Total score
Argentina	0.85	1	0	0	0	0	0	0	0	1.85
Australia	0.95	0	0	0	0	0	0	0	0	0.95
Belarus	0.08	1	0	0	0	0	0	0	0	1.08
Belgium	0.96	1	1	1	0	0	0	0	1	4.96
Brazil	0.72	1	1	0	0	0	0	0	0	2.72
Canada	0.97	1	1	1	0	0	1	0	1	5.97
China	0.09	1	0	1	0	0	0	0	0	2.09
European Union	0.9	1	1	1	1	0	1	1	1	7.9
France	0.89	1	1	1	0	0	0	1	1	5.89
India	0.66	0	0	0	0	0	0	0	0	0.66
Israel	0.74	1	0	0	0	0	0	0	0	1.74
Japan	0.96	0	0	0	0	0	0	0	0	0.96
Myanmar	0.08	1	0	0	0	0	0	0	0	1.08
Russia	0.13	1	0	1	0	0	0	0	0	2.13
South Africa	0.79	1	0	0	0	0	0	0	0	1.79
South Korea	0.83	0	0	0	0	0	0	0	0	0.83
United Arab Emirates	0.18	1	0	0	0	0	0	0	0	1.18

Table 1 *(continued)*

Country	Democracy?	New national laws regarding privacy or FRT?	New laws protect individual privacy vis-à-vis the government?	New laws protect individual privacy vis-à-vis businesses?	New laws prohibit real-time FRT?	New laws prohibit 1:N systems?	Laws prohibit the scraping of images from the internet?	Evidence of laws that require meaningful oversight of the use of FRT?	Laws make state surveillance harder?	Total score
United Kingdom	0.91	1	0	0	0	0	0	1	1	3.91
United States	0.83	0.5	0.5	0	0	0	0	0	0	1.83
Venezuela	0.15	0	0	0	0	0	0	0	0	0.15
Zimbabwe	0.27	0	0	0	0	0	0	0	0	0.27

The data in table 1 capture a wide variety of legislative, policy, and legal positions around the world. Fifteen out of 20 countries had new legislation or legal rulings pertaining to the use of biometric and/or facial recognition technology. The major avenues for state regulation of FRT appear to be no legislation at all; legislation regulating private sector use of the technology; or legislation determining government use of the technology, including requiring citizens to use it in order to access state services, such as with Myanmar and Venezuela.[54]

Most countries have older data protection laws, but they are usually insufficient for protecting the biometric data used in FRT, thereby prompting the creation of new laws. New legislation grapples with at least five different areas of concern. First, regulating government use of FRT frequently addresses who can use this technology, under what circumstances it can be deployed, and what type of capabilities are permissible. For instance, 1:1 FRT has very different implications than 1:N, and the implications of real-time FRT surveillance differ from those concerning FRT deployed on recorded or delayed surveillance recordings.

Second, the legislation typically addresses the extent of government use of the technology and may establish oversight mechanisms and systems of redress; however, the effectiveness and meaningfulness of this oversight varies significantly in each country. Third, how the database of images is constructed is an issue for legislative concern. Some FRT companies scrape images from the internet and social media to create the largest possible database but cannot gain the consent of the people whose images are included. Others construct databases of known persons of interest and limit searches to just these individuals; however, it is important to have oversight and clear criteria for adding individuals to the database to prevent misuse and abuse.

Fourth, storage and protection of databases of biometric data is also an issue for legislation so that the data cannot be stolen or illegally manipulated. This is particularly important as the data may be stored for decades. Fifth, legislation varies in addressing the scope for FRT use in society. Many existing laws do not address potential for public-private partnerships between governments, particularly law enforcement. Moreover, private security companies may own and operate cameras and provide data to the government. Many laws are not specific enough on the issue of scope.

There are interesting trends in the differences in legislation between democratic and nondemocratic countries. The countries that have passed legislation to protect privacy rights and human rights have all been democracies. The EU scored the highest in this study, followed by France and Canada; these democratic entities have prioritized protection of privacy and human rights and enacted laws to support them.

Yet some of the countries with the lowest scores—including Australia and the United States—are democracies that have not yet passed legislation to regulate FRT. The absence of laws creates a legal void similar to what is seen in nondemocratic countries that have chosen not to regulate FRT. Authoritarian or nondemocratic

[54] "Venezuela: Freedom on the Net"; and Pascu, "Myanmar."

regimes have tended to pass legislation that protects the regimes' interests in using FRT and stymies legal challenges to it.

The lowest scoring countries were Argentina, Australia, India, Israel, Japan, Myanmar, South Africa, South Korea, UAE, the United States, Venezuela, and Zimbabwe. There are several reasons that these countries scored so low, particularly among democracies. For some countries, cultures of privacy focus on communalism instead of individuals, thus diminishing the expectation of protection of individual privacy rights. There may also be economic goals of becoming industry leaders or pioneers in the uses of FRT, such as with Japan's AI FRT drone delivery system.[55] For others, the challenges of passing national legislation in large, diverse countries present significant difficulty and may require more time or a piecemeal approach across different jurisdictions.

In Australia and the United States, the citizenry are having robust debates over FRT and legislative efforts underway to regulate its use, but national governments have yet to pass legislation on the issue.[56] In the United States, several cities and states have passed legislation that curtails or bans the use of FRT, but there is no federal law, and the majority of the country is not covered by any particular legislation.[57] For some countries, such as Israel, the presence of ongoing conflict and national security concerns appears to outweigh the protection of privacy rights.[58] And finally, some regimes are more authoritarian in nature and do not seek to protect their citizens' privacy rights in a robust or meaningful way.

Recommendations

The use of FRT and legislation governing it vary widely in intent and implementation around the world. Facial recognition technology laws are built upon existing norms of privacy and human rights, but they also provide an opportunity for each country to decide if it will continue on the same trajectory or diverge onto a different path. Nearly every country examined had evidence of popular protest or legal challenges against the use of FRT systems, indicating that regardless of country or legislative framework, people want their privacy and human rights protected.

This research found there is not yet a meaningful distinction between the rate of legislative actions of democracies and nondemocracies. Some democracies have adopted robust laws to govern this technology, but many others have not yet—and some do not appear to be likely to do so anytime soon. When democracies have passed legislation, they have acted to protect their citizens' privacy and human rights and make

[55] McConvey, "Trains, Drones and Robotic Feels."

[56] Field, "Facial Recognition."

[57] Skye Witley and Andrea Vittorio, "Facial Recognition Software Is Everywhere, with Few Legal Limits," Bloomberg Law, April 27, 2023, https://news.bloomberglaw.com/; and Ryan-Mosely, "Movement to Limit."

[58] "Ministers to Approve Bill Legalizing Police Use of Facial Recognition Cameras," *Times of Israel*, September 23, 2023, https://www.timesofisrael.com/; and Elizabeth Swoskin, "Israel Escalates Surveillance of Palestinians with Facial Recognition Program in West Bank," *Washington Post*, November 8, 2021, https://www.washingtonpost.com/.

government surveillance more difficult or require greater oversight. Europe appears to have the greatest momentum for passing legislation to protect individuals' rights, with the passage of the new EU legislation and preexisting laws in France and Belgium. Canada and Australia have also taken significant steps in this direction.

In every country examined, FRT was implemented before legislation and policy were developed to regulate its use. Prior legislation that regulated collection of data and privacy was typically insufficient for the collection of biometric data and lacked the legal oversight mechanisms many countries sought. Concerns about privacy and human rights have been raised in almost every country in this study. Yet some have acted swiftly to address concerns, while others have moved rapidly to embrace the technology and expand its use. It may be too early to tell how FRT will impact global norms for privacy. It is clear, however, that countries are embracing FRT in different ways, and individual countries are intentionally choosing different approaches to regulating it. These approaches likely reflect economic goals as well as norms and expectations of privacy and government regulation.

These findings are relevant for senior military and civilian leaders because they provide an opportunity for leadership to advance US values and soft power. Specifically, the United States has a chance to promote global standards and norms for the responsible use of FRT consistent with its interests. It could strengthen alliances and partnerships by collaborating on legal and policy positions consistent with its closest partners. The United States could work toward creating a regional or global norm regarding the balance of technological innovation and fundamental rights.

Facial recognition technology also affects US military and civilian personnel stationed overseas and private US citizens traveling abroad. The lack of international regulation or consensus around FRT raises questions about how images and identities of US military and civilian personnel overseas can be protected. The US military can add protections for such US personnel by setting expectations and creating dialogue for regulations concerning the use of FRT. These expectations could be clarified and codified in US laws or agreed to in international forums. The United States should seize the opportunity to determine what legal and normative responsibilities and recourse could be established to protect US personnel and advance national security.

As rapid technological innovation in the field of biometric surveillance proceeds, policymakers and legislators must be aware of the implications for human rights and privacy. As governments and companies invest in developing and implementing this technology to improve safety and security, they should also invest in safeguarding the human rights and privacy of citizens. Such laws and protections will not only affect citizens but will also determine the emergence of new norms in international law applicable to cyberspace and technology. Æ

Disclaimer and Copyright

The views and opinions in *Æther* are those of the authors and are not officially sanctioned by any agency or department of the US government.