

Facial Recognition in Public Spaces: Balancing National Security and Privacy in the European Union and the United States — A Comparative Legal Analysis

Dr. Rima Faraj

Head of the Department of Private Law, Professor at the Islamic University of Lebanon

Instructor at the Faculty of Law, Lebanese University

Orcid No: 0009-0005-3753-465X

(Received: 17 October 2025; Accepted: 15 November 2025; Published: 23 December 2025)

Abstract

Across borders and political systems, facial recognition has quietly redrawn the boundaries of what it means to be seen by the state. Its rise was never announced as a revolution, yet it has changed the ordinary meaning of public space. The technology's strength—instant identification—is also its greatest risk. Between security and freedom lies a legal space that both the European Union and the United States are still trying to define. The EU treats biometric surveillance as a matter of principle: it must be justified before use, restricted by the GDPR, the Charter of Fundamental Rights, and the proposed AI Act. The United States approaches the same issue through practice rather than doctrine. Regulation appears later, through court challenges, state bans, and public backlash. The contrast reveals two moral instincts—Europe's caution and America's faith in innovation. Neither instinct alone provides stability. This paper suggests a middle path: one that allows experimentation but demands transparency, periodic review, and genuine channels for contesting wrongful identification. What matters is the system not how fast operating, but whether it remains under human judgment. Technology can serve democracy only when it remembers who it serves.

Keywords: *Artificial intelligence governance, Data protection, Facial recognition, National security Surveillance law.*

1. Introduction

Facial recognition began as a technical curiosity—something that made border checks faster and airport lines shorter. But it did not stay that simple for long. What once seemed like a harmless convenience has turned into one of the most debated technologies of the past decade. Today, cameras do more than record; they identify, categorize, and even anticipate behavior. That shift has forced governments to decide where efficiency ends and intrusion begins.

In Europe, the answer leans toward caution. The European Union treats facial images as highly sensitive limiting their use under the General Data Protection Regulation (Regulation (EU) 2016/679, 2016, Art. 9(1)), the Charter of Fundamental Rights of the European Union (European Union Agency for Fundamental Rights, 2019, p. 22) and the proposed Artificial Intelligence Act (European Commission, 2021, p. 4). The idea is preventive: stop misuse before it happens. The United States takes a very different path. There isn't one unified privacy law. Instead, protection comes in fragments — a mix of agency policies, state rules, and court cases that often appear only after damage has been done. It's a patchwork that gives room for quick experimentation, and sometimes that freedom helps technology grow faster than it would in Europe. But it also means there are cracks big enough for misuse to slip through. Accountability doesn't arrive automatically; it depends on who challenges a practice and when. And that uncertainty leads to the central question running through this study: how can two democratic systems, built on such different legal traditions, draw the line between necessary security and the right to remain unobserved?

Over the past few years, this debate has grown louder on both sides of the Atlantic. In Brussels, the final stages of the AI Act (European Commission, 2021, Art. 5(1)(d)) reignited arguments about whether any form of real-time facial scanning should be permitted in public spaces. Some governments, like France and the Netherlands, argue that national security demands limited use. Others, especially within the European Parliament, believe that such tools cannot coexist with fundamental rights. Across the Atlantic, the absence of a federal privacy law has pushed cities and states to act on their own. Massachusetts, Virginia, and Washington have all restricted or temporarily banned facial recognition, usually after local protests or lawsuits (Electronic Frontier Foundation, 2021, p. 2). The details vary from one country to another, yet the unease is the same—how to protect people without eroding the very freedoms that define public life, in a world where being watched has become almost routine.

Beneath these policy differences lies a deeper cultural divide. Europe's legal tradition assumes that individuals must be shielded from the state in advance, while the American system trusts in courts and public scrutiny to repair violations afterward. Both legal systems now confront the same structural dilemma: how to preserve democratic oversight once surveillance becomes silent and continuous. Law, in this context, is more than a protective shield; it serves as a mirror that reflects a society's conception of authority and restraint. In practice, once surveillance becomes part of daily life, the focus starts to drift. It is no longer simply a matter of what technology can do; it becomes a question of who, in the end, still has the legal authority—and the moral weight—to determine when its use must finally be restrained (Council of Europe, 2021, p. 5).

2. Security Justifications vs. Civil Liberties Risks

Every government claims the same dilemma: how to stay secure without becoming watched. Facial recognition entered public life through promises of safety and speed—airports that move faster, streets that feel safer, borders that rely less on human error. Yet beneath that narrative lies a quiet tension between protection and privacy. When the state can identify anyone at any time, security becomes inseparable from control. The question is not whether these systems work, but what kind of society they create when they do.

2.1 Facial Recognition as a National Security Tool in the EU and the U.S.

Facial recognition is often presented as a tool of necessity rather than choice; Governments do not introduce it by advertising new powers but by framing it as simple efficiency. Border agencies in the EU use it to shorten queues and verify identities automatically, especially in major entry points like airports (European Commission, 2021, p. 4). In the United States, the justification is similar but more closely tied to policing. The FBI and immigration authorities use facial databases to match suspects or locate individuals who may be avoiding detection (U.S. Government Accountability Office, 2020, p. 12). In both regions, the logic is the same: if a technology can help find a dangerous person more quickly, it seems hard to argue against it. Even so, neither system provides clear proof that facial recognition actually prevents serious crime. Much of the support rests on expectation rather than measurable results.

2.2 Risks of Mass Surveillance, Discrimination and Chilling Effects

Still, the risks are far easier to see than the promised benefits. Facial recognition is not limited to tracking suspects; it captures everyone who happens to walk through its frame. What begins as a targeted security measure quickly resembles broad surveillance. Even if no law is broken, people may change their behavior simply because they feel watched—avoiding protests, public gatherings or even casual movement in shared spaces. Research has also shown that the technology makes more mistakes with certain demographic groups, which increases the chance of unfair stops or questioning (Garvie, 2019, p. 9). The problem is therefore not only technical but social. A system designed to provide protection may instead erode trust if people believe it is used more against them than for them. The question is no longer whether facial recognition functions—but whether it does so justly, and at what cost to everyday freedom.

3. Legal Foundations Governing Facial Recognition

Before comparing how facial recognition is used in practice, it is necessary to understand the legal ground on which it stands. Europe and the United States do not regulate the technology from the same legal tradition. One builds its limits from data protection and fundamental rights, while the other relies more heavily on constitutional interpretation and sector-based rules. These foundations shape when facial recognition may be used and also who must justify it and at what stage—before deployment or only after challenge.

3.1 Data Protection and Constitutional Guarantees: GDPR & EU Charter vs. Fourth Amendment and U.S. Sectoral Rules

The starting point for understanding facial recognition law in Europe is data protection. Under the General Data Protection Regulation, facial images are not considered ordinary information; they are placed in the category of “special data,” which means they cannot be

processed unless a clear legal ground exists (Regulation (EU) 2016/679, 2016, Article 9(1)). This rule is not simply technical. It is rooted in higher constitutional rights set out in the EU Charter, which protects privacy (Article 7) and personal data (Article 8). In practice, the combination of these instruments requires authorities to justify surveillance in advance; They must show necessity and proportionality before deploying facial recognition in public settings.

The United States approaches the issue from a different angle. Instead of one clear data protection law, the United States relies on a mix of constitutional interpretation and scattered sectoral rules. Much of the legal debate falls under the Fourth Amendment which protects against unreasonable searches; But U.S courts usually apply it only when a person is seen as having a clear expectation of privacy, a standard that often excludes public spaces (*Katz v. United States*, 1967, p. 351). In practice, this means that being watched in the street is rarely treated as a legal intrusion unless the monitoring becomes extremely persistent or targeted. Because public spaces are often seen as “open,” facial surveillance is not automatically treated as a search unless it becomes overly persistent or intrusive. Outside constitutional law, regulation is fragmented. Health data, children’s data and financial data are separately protected, but biometric surveillance by law enforcement or commercial actors often falls outside federal control.

3.2 Regulatory Instruments: AI Act EU vs. Agency Guidelines and Legal Gaps U.S.

Europe has attempted to move beyond general privacy principles by setting specific rules for artificial intelligence. The proposed AI Act classifies real-time remote biometric identification in public places as a high-risk or nearly prohibited practice, allowing it only for narrowly defined purposes such as preventing serious crimes or locating missing persons (European Commission, 2021, Article 5(1)(d)). This places facial recognition with a controlled legal threshold rather than leaving it to administrative discretion. It also imposes transparency, documentation and human oversight requirements on those who deploy such systems.

The United States has no equivalent federal legislation. Federal agencies, such as Customs and Border Protection or the FBI issue their own policies on facial recognition use but these are internally drafted and rarely binding outside their departments (U.S. Government Accountability Office, 2020, p. 12). In many cases, deployment proceeds without independent assessment. Some states have tried to fill the gap—Illinois, Washington and California have enacted restrictions on biometric use—but these measures are local rather than national. As a result, the U.S. model leaves considerable freedom at the enforcement stage but limited clarity at the regulatory one.

4. Governance Models of Public and Law Enforcement Use

Even when laws define the limits of facial recognition, what truly matters is how those rules are applied in practice. Some systems require official authorisation before surveillance tools can be used; others allow deployment first and justification later. Europe generally treats facial recognition as a controlled power that must be supervised before it reaches public spaces. The United States, by contrast, often leaves such decisions to individual agencies or local authorities, intervening only when controversy forces a response. These different attitudes toward authorization and accountability reveal not just legal contrasts, but contrasting expectations of trust between citizens and the state.

4.1 Prior Authorization and Proportionality Tests in the EU vs. Permissive Deployment in the U.S.

In the European Union facial recognition is not simply deployed at the discretion of law enforcement. Most countries require prior legal authorization before cameras can be used for biometric identification in public spaces. In France for example, police must obtain approval from both judicial authorities and data regulators before trial deployments of facial recognition at large events (CNIL, 2019, p. 6). Germany follows a comparable approach through its Federal Data Protection Act, which obliges authorities to demonstrate that any biometric surveillance is genuinely proportionate before it is introduced in public spaces (Bundesdatenschutzgesetz, 2018, §47). Put simply, the state cannot switch on facial recognition and justify it later — it must show in advance why it is needed, how long it will be used and who it might affect.

The United States moves in the opposite direction. Facial recognition is often rolled out first and only examined once concerns arise. Local police forces or transit agencies can install the technology without external clearance as long as they use commercially available software or existing camera networks (Woodrow & Bedoya, 2021, p. 14). Regulation arrives after deployment rather than before.

Only when there is public backlash or media exposure do questions about proportionality emerge. In several cities, facial recognition was discovered in use only after journalists filed freedom of information requests. The legal burden falls on citizens or advocacy groups to challenge its use rather than with law enforcement to substantiate it from the outset. This contrast goes deeper than administrative habit; it reflects two different ways of thinking about state authority. In Europe, privacy is seen as something that must be secured before the state can act. Oversight is therefore built into the legal process itself — no measure is legitimate until it passes a proportionality test. In the United States, the logic runs the other way. Innovation is assumed to be lawful until someone proves otherwise. The courts, the press, and public advocacy become the main instruments of correction once harm is revealed (Kosta, 2021, p. 180). These two legal traditions reflect the deeper divide between civil-law systems, which rely on prior control, and common-law systems, which depend on correction after the fact. Each seeks to protect liberty, though by opposite routes: one through precaution, the other through confrontation. Yet both now face the same dilemma — technology moves faster than the frameworks designed to contain it. The question is no longer whether the law will respond, but whether it can respond in time before the idea of accountability becomes purely symbolic.

4.2 Oversight Mechanisms: Data Protection Authorities EU vs. Litigation and State Bans U.S.

Oversight in Europe is largely administrative. National Data Protection Authorities supervise the use of facial recognition, investigate complaints and can issue binding corrective measures. Spain's AEPD and Italy's Garanti have already imposed temporary bans on certain municipal surveillance projects where prior assessment was lacking (AEPD, 2021, p. 3; Garante per la Protezione dei Dati Personali, 2022, p. 5). These bodies do not wait for harm to occur they can intervene pre-emptively if they believe legal standards are not met. In some cases, they require impact assessments or demand the suspension of software until safeguards are proven adequate.

In the United States, oversight relies far more on confrontation than administration. Litigation is the main corrective tool. When police departments in cities like Detroit and Boston

were found using facial recognition without public knowledge, it was lawsuits, not regulators, that forced transparency (Buolamwini & Raji, 2020, p: 75). Some states, like Massachusetts and Virginia, have passed outright bans or moratoriums on public agencies using facial recognition. However, these bans are very different in terms of how they are enforced and what they cover. (Electronic Frontier Foundation, 2021.p. 2). Rather than one nationwide authority there is a patchwork of resistance driven by public pressure by local politics and civil rights litigation.

5. Comparative Assessment and Future Direction

The contrast between the European Union and the United States does not lie only in their legal texts, but in the logic that drives their surveillance governance. One system assumes that certain risks must be controlled before they materialise, while the other presumes that intervention is justified unless proven harmful. Neither approach is inherently superior; both have strengths and vulnerabilities that become visible only when applied in real public environments.

5.1 Preventive Regulation EU vs. Reactive Accountability U.S: Strengths and Weaknesses

The European Union's approach has the advantage of being predictable. Before facial recognition can be used, the authorities must justify it through proportionality checks, formal authorization and detailed assessments. That means the technology cannot quietly appear in public spaces without explanation. People do not have to wait for a scandal to question it—the state must defend its decision from the start. Still, this level of control comes at a price. Approval processes can be protracted, and security services frequently contend that by the time the documentation is finalized, the necessary tools have already become obsolete (Europol, 2022, p. 11).

The United States leans in the opposite direction. Instead of waiting for legal approval agencies often deploy facial recognition first and deal with objections later. This makes experimentation easy and allows quick reactions during emergencies (National Institute of Standards and Technology, 2019, p. 3). But the burden of oversight is flipped. It is no longer the state that must prove necessity—it is the public that must prove harm. Legal action only comes after someone is wrongly identified or exposed. As a result, protection differs from one state to another, shaped less by law and more by who is willing to fight back.

5.2 Toward a Hybrid Model: Controlled Innovation with Rights-Based Safeguards

Neither system can stand on its own. that imposes excessive restrictions on technology may leave security agencies unprepared while one that allows free expansion risks normalizing constant surveillance. A realistic path forward would borrow the best elements from both regions: Europe's demand for proportionality and oversight, paired with the United States' ability to test new tools under controlled conditions. Pilot programmes could be authorized for limited periods, overseen by independent bodies, and suspended automatically unless they are shown to be both effective and fair.

Transparency would be fundamental to this model. Authorities should make clear when and why facial recognition is used, without disclosing sensitive operational tactics. Audits should review not just technical performance but also the social effects of deployment, especially on groups most likely to be misidentified. Above all, people must have a way to

challenge incorrect matches or misuse. A technology that operates on millions of faces cannot be trusted by default—it must prove that it serves the public, not the other way around.

6. Policy Recommendations and Implementation Roadmap

Neither prohibition nor permissiveness offers a stable path forward. Every model tried so far has revealed its limits: strict regulation can slow necessary innovation, while open experimentation can erode public trust long before results are proven. If facial recognition is to remain part of modern security policy, it must be used under conditions that earn consent rather than assume it. The following recommendations outline how states can permit development without surrendering oversight. Their purpose is not to halt progress but to ensure that technology is introduced with caution and evaluated with fairness and withdrawn when it fails to meet basic standards of justice.

6.1 Operational Guidelines for Responsible Deployment

Facial recognition does not need to be accepted blindly or rejected outright. The real challenge is deciding when it can be useful without silently reshaping public space into an environment of constant monitoring. One way forward is to treat deployment as an exception rather than a standard setting. Instead of granting open-ended authorizations, authorities could approve only temporary pilot programs with automatic expiry dates (*European Union Agency for Fundamental Rights, 2019, p. 22*). If a system genuinely improves security, it may be renewed; if not, it should disappear without ceremony. Every use should also have a clearly stated purpose that cannot be quietly expanded over time. What begins as a search tool for missing persons should not later be applied to monitoring protests or identifying political gatherings (*Electronic Frontier Foundation, 2021, p. 2*).

Transparency should not depend on public scandal or journalistic discovery. People do not need technical breakdowns of algorithmic models, but they deserve to know when biometric scanning is active (*AEPD, 2021, p. 3*). Visible notifications, whether digital or physical, can function as a basic recognition that consent is not presumed. Oversight must extend beyond the evaluation of accuracy in laboratory environments. The primary issue is whether some communities are disproportionately identified, interrogated, or marginalized. If a particular demography frequently appears in false alarms, the issue is not technological but systemic (Buolamwini & Raji, 2020, p. 75).

6.2 Rights-Based Innovation Framework for Democratic Surveillance

Technology that affects millions of people cannot be shaped only by the institutions that plan to use it. If facial recognition is to be tolerated in a democratic system, its design and deployment must include those most likely to bear its risks (Council of Europe, 2021, p. 5). Human rights impact assessments should become a prerequisite, not a formality, before any biometric tool reaches public space. These assessments lose meaning when written solely by technology vendors or internal police units; they should instead involve data protection authorities, civil society organizations and representatives from affected communities (*European Union Agency for Fundamental Rights, 2019, p. 22*).

Protection is not achieved through abstract legal principles alone. Individuals must be able to contest automated identification decisions without needing legal expertise or political influence (*Katz v. United States, 1967, p. 351*). A person wrongly flagged should be informed when it happens and given a clear route to demand correction. Accountability cannot rely on

goodwill. It must be embedded into the system before harm occurs and not offered afterward as an apology (Buolamwini & Raji, 2020, p. 75). Innovation becomes legitimate only when it strengthens public confidence rather than testing its limits (Europol, 2022, p. 11).

7. Future Governance Challenges and Legal Adaptation

The regulation of facial recognition is only the beginning. Each legal boundary creates new ways for technology to move around it. What once identified a face now tries to read emotion or intent. Surveillance is shifting from recognition to interpretation, and the law still struggles to define where that shift should stop. These changes raise a larger question: can rules made for a single technology keep up with an ecosystem that keeps reinventing itself?

7.1 The Expansion of Biometric Surveillance Ecosystems

The challenge is that these systems rarely appear as a single, visible product. They are woven quietly into what already exists—public surveillance cameras, online platforms, and private databases—until their operation becomes almost invisible. Ordinary users may never realize that an airport camera or a social media filter is powered by several layers of algorithmic analysis working together. Once connected, these layers can produce conclusions that even their designers did not plan. What begins as a simple facial match may expand into an emotional reading or a behavioral forecast, created without any new consent from the individual (AlgorithmWatch, 2021, p. 18). This change makes it hard to tell the difference between identification and prediction. It also makes it harder to figure out who is legally responsible if something goes wrong, the developer of the software, the data controller, or the public agency that uses it?

European regulators are starting to recognize this gap. The European Union Agency for Fundamental Rights (2019, p. 22) warned that combining biometric and behavioral data could undermine existing safeguards built around transparency and purpose limitation; Yet, even this warning is only the beginning. Traditional privacy frameworks treat data as something static—collected, stored, and processed. In reality, biometric data behaves more like a flow: it changes meaning depending on context, interpretation, and the purpose for which it is reused. Laws written for isolated systems must therefore evolve into frameworks capable of supervising interaction—where multiple technologies, not a single database, determine how a person is seen and classified.

7.2 The Role of International Coordination in Digital Governance

The distance between law and technology grows wider when every country tries to manage it alone. In the United States, rules often appear only after a scandal or lawsuit, and without a federal framework, oversight shifts from one agency to another (U.S. Government Accountability Office, 2020, p. 12). Europe faces a different risk: regulation that moves faster than reality, leaving new systems outside its scope almost as soon as they emerge. The result is imbalance on both sides of the Atlantic—too much caution in one place, too much freedom in the other. A stable approach needs dialogue, not isolation. Data does not stop at borders, and neither should accountability. Coordinated standards between the EU and the U.S., supported by the OECD and the United Nations (Council of Europe, 2021, p. 5), could set a shared foundation for fairness without erasing national diversity. Perfection is not the goal; consistency is. Without it, protection depends less on rights than on geography.

8. Conclusion

Facial recognition is often described as a technological step forward, but its real weight lies elsewhere. It has forced lawmakers to confront questions that reach far beyond efficiency or innovation. The way a country regulates surveillance shows how much it trusts its own institutions. In Europe, the instinct is to act before harm appears—to prevent misuse through prior control. In the United States, the impulse is the opposite: act first, correct later. Both systems seek the same goal, yet they travel in different directions to reach it.

Neither approach is complete. Regulation that moves too cautiously risks leaving governments unprepared for genuine threats, while permissive models invite mistakes that can erode trust long before accountability catches up. The only sustainable path sits somewhere between both extremes—a system that welcomes innovation but surrounds it with limits clear enough to keep freedom intact. Facial recognition should operate only under defined legal conditions, reviewed at fixed intervals, and subject to independent oversight. People must have a real right to contest its decisions—not years later, but while those systems are still being tested.

As technology becomes routine in public administration, legitimacy will depend less on technical guarantees and more on openness. Citizens deserve to know when surveillance is active, who runs it, and what happens to the data it collects. Rules must evolve in the same rhythm as the systems they govern; otherwise, protection turns into a promise without practice. Oversight cannot be written once—it has to be renewed, debated, and lived.

The true measure of democracy in a digital age is not how quickly it embraces new technologies, but how wisely it limits them. Security gains meaning not from how much the state can observe, but from how carefully it decides to observe.

Perhaps the most important lesson of facial recognition has little to do with data or algorithms. It is a reminder that restraint is also a form of strength. A democracy that knows when not to use its most powerful tools shows more confidence than one that deploys them without reflection; The challenge ahead is not technological—it is ethical: to decide, again and again, where visibility must end so that freedom can continue.

In the end, the question is not whether facial recognition can be controlled, but whether societies can control themselves in using it. Law alone cannot guarantee restraint; it must be supported by civic awareness and institutional humility. When regulation, ethics and collective judgment work together technology becomes less a threat and more a test; a test of whether freedom can survive even when it is constantly being watched. That will be the real victory of law in the digital century—not the control of machines, but the preservation of meaning in what it means to be human.

Bibliography

- AEPD. (2021). *Resolution on the use of facial recognition in public transport systems* (p. 3).
- AlgorithmWatch. (2021). *Automating society report 2021: The rise of artificial intelligence in policing* (p. 18).
- Big Brother Watch and Others v. United Kingdom, App. Nos. 58170/13, 62322/14 and 24960/15 (ECHR, 2018), para. 387.
- Buolamwini, J., & Raji, I. (2020). *Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research*, 81, 75.
- Bundesdatenschutzgesetz. (2018). *Federal Data Protection Act (Germany)* (§ 47).
- CNIL. (2019). *Facial recognition: For a debate that is up to the challenges* (p. 6).
- Council of Europe. (2021). *Recommendation on the impact of artificial intelligence systems on human rights* (CM/Rec(2021)1) (p. 5). Strasbourg: Committee of Ministers.
- Electronic Frontier Foundation. (2021). *Municipal bans on face recognition* (p. 2). <https://www EFF.org/pages/face-recognition>
- European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)* (COM/2021/206 final, Art. 5(1)(d), p. 4). Brussels: European Commission.
- European Union Agency for Fundamental Rights. (2019). *Facial recognition technology: Fundamental rights considerations in the context of law enforcement* (p. 22). Publications Office of the European Union.
- Europol. (2022). *Facing the future: Law enforcement and artificial intelligence* (p. 11).
- Garvie, C. (2019). *America under watch: Face surveillance in the United States* (p. 9). Georgetown Law Center on Privacy and Technology.
- Garante per la Protezione dei Dati Personali. (2022). *Decision on the suspension of biometric monitoring systems in municipal areas* (p. 5).
- Katz v. United States, 389 U.S. 347 (1967), 351.
- Kosta, E. (2021). *The principle of proportionality in EU data protection law. International Data Privacy Law*, 11(3), 177–188. <https://doi.org/10.1093/idpl/ipab005>
- National Institute of Standards and Technology. (2019). *Face recognition vendor test (FRVT) Part 3: Demographic effects* (NISTIR 8280, p. 3).
- Organisation for Economic Co-operation and Development (OECD). (2021). *OECD principles on artificial intelligence: Shaping responsible stewardship of trustworthy AI*. OECD Publishing. <https://doi.org/10.1787/9789264386044-en>
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.
- U.S. Department of Homeland Security. (2020). *Biometric Entry-Exit Program Privacy Impact Assessment* (DHS/CBP/PIA-030[a], p. 7).
- U.S. Government Accountability Office. (2020). *Facial recognition technology: Federal law enforcement agencies should better assess privacy and other risks* (GAO-21-518, p. 12).
- United Nations. (2021). *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights* (A/HRC/48/31, p. 7).
- Woodrow, H., & Bedoya, A. (2021). *Regulating facial surveillance: The failure of U.S. oversight frameworks. Journal of Law & Technology*, 14(2), 1.