Enabling Beneficial and Safe Uses of Biometric Technology Through Risk-Based Regulations

April 2024

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Foreword

Biometric technology use cases are growing, bringing convenience, efficiencies and a wide range of societal benefits when developed and deployed responsibly. At the same time, however, there are recognized concerns over potential harms for individuals and their rights. It is no wonder that legislators and policy-makers around the world are considering how to regulate the use of biometric technology to enable benefits and address the risks. Yet, current laws and regulations addressing the use of biometric technology are still in developmental stages and sometimes cause confusion and uncertainty for those developing and deploying biometric technologies. This new CIPL report aims to shed light on this legal uncertainty and recommends that law- and policymakers approach biometric technology regulation through a risk-based approach, with enforceable organizational accountability at its core.

CIPL's mission has always been to provide constructive thought-leadership and best practices for both policy-makers and organizations developing and using transformative technologies. To this end, in this report specifically, we:

- present a wide range of biometric technology use cases that facilitate necessary security and safety functions, healthcare solutions, and other benefits;
- explore the risks and concerns associated with biometric technology development and deployment;
- evaluate the challenges in current legal and regulatory approaches; and
- recommend a three-pronged risk-based approach to regulating biometric technology.

To promote organizational accountability and the responsible development and deployment of valuable biometric systems, CIPL encourages law- and policymakers to understand beneficial use cases, recognize the risks, and implement future-proof laws and regulations that mitigate those risks. Equally, we call on organizations developing and deploying biometric technologies to be accountable and implement policies, controls, procedures and risk mitigation measures, that are also founded on a risk-based approach. A risk-based approach to regulation and risk-based organizational accountability are both essential to ensure further advancements for the benefit of individuals and society.

Bojana Bellamy

President
Centre for Information Policy Leadership

Executive Summary

- **Uses of biometric technologies are growing and can deliver important societal and economic benefits.** Biometric systems and technologies can unlock benefits and innovations in a variety of contexts and sectors, such as device, account, and enterprise security; public and event security; online safety; accessibility; and health care. (Appendix B contains a non-exhaustive but comprehensive collection of biometric application case studies.)
- **Biometric applications encompass a wide range of risks and benefits.** Some uses of biometric technologies present low risk to individuals while providing meaningful benefits. Other uses pose higher risk of harm to individuals, groups, and society based on the sensitivity of the context; the potential for inaccuracy, bias, or misuse; the level of surveillance; or the possible effect on the exercise of civil and other rights. Sometimes a lack of accountability in the development and deployment of biometric systems—such as inadequate transparency, redress, oversight, or mitigation measures (e.g., de-identification)—can amplify these risks. A given technology's risk profile is elevated when it is used for the identification of individuals.
- **Laws vary in application and scope.** Most data protection and biometric data laws address the use of biometric systems solely in the context of establishing an individual's unique identity. Other laws, however, cover broader uses, which can unnecessarily limit or burden low-risk processing of biometric data. Risk-based and future-proof laws and regulations should focus on the intended uses of a biometric system rather than the underlying data itself.
- **Organizations need to impellent accountability and risk-based mitigations that improve protections for individuals and enable responsible uses.** Organizations need to build and implement accountable policies, controls, procedures and risk assessment and mitigation measures when developing and deploying biometric technologies. The risks associated with biometric applications depend on the specific use case (e.g., whether the application is used for identification purposes) and context (e.g., whether the use will have legally significant effects), as well as on the technical systems underlying a specific use case (e.g., whether the application would easily allow for identification even if that is not the intended purpose). A risk-based approach would permit low-risk uses that do not involve the identification of individuals. It would also encourage the use of mitigation measures that are proportionate and tailored to the risks of the specific use case, requiring more rigorous safeguards for uses posing greater risks. Such an approach avoids both overregulating and underregulating uses of biometric data.

Key Recommendations for Lawmakers, Policymakers, and Regulators

- **Regulate the use of biometric systems based on risk.** Consider the purposes, uses, applications, and capabilities of biometric technologies rather than the nature of the data; be mindful not to impede deployment of low-risk applications; acknowledge that certain technical or governance measures can reduce or mitigate risks to acceptable levels; and reserve heightened requirements or outright bans for high-risk use cases where safeguards are not available.
- **Strive for consistency across jurisdictions and industry when defining biometric data and systems.** Define "biometric data" as information representing the characteristics of a uniquely identifiable person that is intended to be interpreted by biometric technology. Define "biometric systems" as systems that process biometric data for purposes of uniquely identifying an individual. These definitions should exclude data and systems that are not associated with identifying individuals.
- **Require accountability measures to promote responsible uses.** Regulations addressing the development and use of biometric systems must include strong accountability and data governance measures—such as transparency, risk and impact assessment, purpose limitation, effective redress, and data security—that, collectively, can substantially mitigate high risks associated with the use of biometric data.
- **Implement collaborative regulatory tools such as sandboxes to support responsible development and deployment.** Regulatory sandboxes provide a testing ground for regulators and industry to advance technological innovation for the wider benefit of all and a place to assess the implications and impact of risk-based regulations.
- **Adopt a three-pronged approach for the regulation of biometric systems:**
  - **i.** Base laws and regulations on risk and proportionality, specifically referencing the risk-based approach;
  - **ii.** Require organizations that develop or deploy biometric technologies to demonstrate accountability in their data governance measures; and
  - **iii.** Provide responsive regulatory guidance and promote constructive engagement with industry.

Table of Contents

Table of Contents (continued)

I. Introduction

Biometric technologies have emerged as important tools for security, safety, convenience, and accessibility.

Biometric technologies have emerged as important tools for security, safety, convenience, and accessibility.

They also enable creativity through a wide range of social media and retail applications. Many of the use cases enabled by biometric technologies are of unquestionable benefit to businesses, individuals, and society, particularly when combined with other emerging technologies such as artificial intelligence, machine learning, and privacy-enhancing technologies.[1]

That said, certain applications can present challenges and risks with respect to ethics, privacy, and civil rights, and they can raise technical questions concerning reliability, accuracy, and security. For these reasons, the use of biometric technologies—and facial recognition technology in particular—has captured the attention of many regulators and lawmakers around the world. Some are calling for outright bans on certain uses of biometric technologies, while others are exploring possible frameworks and laws to ensure the development and deployment of such technologies in a responsible manner.

Although the potential risks of biometric technologies can undoubtedly be significant, it is important to recognize that many low-risk applications provide a wide range of benefits. For example, the use of biometric technologies for authenticating access to devices, buildings, and banking services has unlocked conveniences and increased security while posing low risks to individuals and their rights. Indeed, even some higher-risk applications may deliver significant benefits if deployed responsibly and with appropriate safeguards.

CIPL's white paper explores various real-world applications of biometric technologies as well as the benefits and risks they can present. Our paper examines the global legal landscape and trends for regulating these technologies, and we urge implementation of a risk-based approach for their regulation and governance. We support adopting a more consistent definition of biometric data and technologies and the establishment of appropriate obligations in accordance with the risk level. Like other emerging technology and data protection areas, a risk-based approach enables targeted and relevant mitigations, transparency, accountability, and redress, while facilitating important and beneficial uses of biometric technologies.

1 CIPL White Paper, Privacy-Enhancing and Privacy Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age.

II. Understanding Biometric Technologies

A. Definition of Biometric Data

In this paper, we use the term "biometric data" broadly to refer to information (1) that represents the characteristics of a uniquely identifiable person, and (2) that is intended to be interpreted by biometric technology. We use the terms "biometric technologies," "biometric systems," and "biometric applications" synonymously to refer to systems that process biometric data.

Jurisdictions across the globe have different definitions of "biometric data." (See Appendix A.) Many follow the EU General Data Protection Regulation (GDPR), which defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[2] The GDPR's definition thus satisfies the two elements mentioned above.

Physiological biometric data—e.g., fingerprints, retina or iris scans, ear features, vein patterns, or DNA—is what traditionally comes to mind when thinking of biometric technology. One of the most widely recognized—and most highly scrutinized—types of physiological data is facial biometric data, which is used with facial recognition technologies. Such technologies compare facial biometric data from an image, video, or live feed to a database where facial characteristics have been processed and stored as mathematical code.

Biometric data may also encompass behavioral biometric data, which includes measurable behavioral patterns such as gait (the analysis of motion, i.e., walking or running), voice or speech rhythm, and keystroke dynamics.[3] Because technologies that process behavioral biometric data evaluate the unique behavior and inherent movements of an individual, they are used to recognize fraudulent or suspicious behavior.

Beyond these basics, various jurisdictions define biometric data differently. The significance of those differences is discussed in Sections IV and V, *infra*, and a compendium of definitions appears in Appendix A.

2 GDPR Article 4(14). GDPR Article 9(1) establishes heightened requirements for the processing of biometric data "for the purpose of uniquely identifying a natural person."

3 Various studies indicate that emotion recognition via biometric systems is generally unreliable because of how difficult it is to code for variables such as context and culture. *See* Andrew McStay, "Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy" (Big Data & Society, 2020).

B. How Biometric Technology Works and Common Applications

The deployment of biometric technologies typically includes the following steps:

i. **Initial data collection**, i.e., the process of capturing in analogue or digital form a "biometric sample," which is data that represents an individual's unique biometric characteristics, such as facial geometry, fingerprint, voice recording, or keystroke pattern;

ii. **Key or template creation**, which is the process of using technology to measure or analyze the collected biometric sample into a mathematical or algorithmic representation specific to that individual;

iii. **Matching or scoring**, which is the process of comparing a new biometric sample against the created key or template in the database; and

iv. **Storage** of collected biometric samples (in some cases).[4]

Increasingly, developers and deployers of biometric technology are turning to standards organizations to establish industry-wide consistency regarding terminology, which promotes interoperability and other benefits.

Increasingly, developers and deployers of biometric technology are turning to standards organizations to establish industry-wide consistency regarding terminology, which promotes interoperability and other benefits. This paper references the International Standards Organization (ISO) biometric vocabulary standards.[5]

Although use cases for biometric technologies span a variety of sectors and applications, the primary applications or capabilities of biometric technologies relate to *recognition* (or *identification*), *verification*[6], and *classification* (or *categorization*).

Recognition, or identification compares a collected biometric sample against a database to identify who an individual is. This is commonly referred to as a "1:N" or one-to-many search. In other words, it asks: "Who are you?"

Verification typically measures the validity of a claim by comparing a new biometric sample against a single previously collected and verifiable measurement and is commonly referred to as a "1:1" or one-to-one match. It asks: "Are you who you say you are?" This may also take the form of "1:few" verification, as in cases where a shared device can support multiple users whose profiles are associated with the same account.

Classification, categorization, or detection uses biometric data to categorize individuals into certain subgroups by making inferences, e.g., classification systems can categorize individuals by gender or age group or detect whether a human or certain body part is present. It asks, for example: "Are you human?" or "Are you 18 years of age or older?"

The overarching capability (or purpose) of a given application—identification, verification, or classification—will determine what responsible data governance looks like. For example, a biometric *identification* system will typically require a large database of biometric samples, whereas a *verification* system will need to compare a single sample against a previously collected sample.

4 These are general steps of deploying biometric technology. Some lists of biometric processes include another step—disposal of templates when no longer needed—which can be an important risk mitigation technique.

5 International Standards Organization. (2022-23). Information technology, Vocabulary, Part 37: Biometrics. (ISO/IEC2382-37).

6 The ISO defines "biometric recognition" as the "automated recognition of individuals based on their biological and behavioural characteristics" and it considers biometric recognition an umbrella term for both biometric identification and biometric verification. *See* ISO/IEC 2382-37:2022, Information technology, Vocabulary, Part 37: Biometrics.

Moreover, the risks (discussed in depth in Section III.) associated with a particular application typically derive from the architecture of the technology and its corresponding data collection and storage requirements. For example, some technologies will retain an end-user's biometric data in encrypted form on the user's device to minimize risk. Of course, risks may arise beyond the context of the architecture and technical requirements based on the status or role of the deployer (e.g., a state actor or an employer).

C. Real-World Applications of Biometric Data and Facial Recognition

Early biometric applications, such as fingerprint systems, date back to the late 1800s,[7] but technological advancements have made modern biometric systems automated and accessible, especially when combined with other technologies such as artificial intelligence. Indeed, the real-time processing of biometric data, together with artificial intelligence, has enabled important innovations for security and accessibility. It has supported not only law enforcement and national security efforts, but also everyday uses such as unlocking smartphones or accessing personal accounts. Certain applications of biometric technologies have enhanced accessibility for users completing financial transactions, going through security lines, or logging into accounts or devices. Biometric technologies have also improved online safety by verifying users, authenticating age, and flagging potential fraud.

Appendix B to this paper provides a wide range of specific examples and use cases for biometric data in a variety of settings, including applications in law enforcement, public and border security, airport efficiency, device and enterprise security, banking and financial services, workplace monitoring and safety, marketing and customer experience, transportation and logistics, automotive safety, healthcare, fitness, education, and social media. In each of these areas, the use of biometric technologies holds significant benefits.

Appendix B to this paper provides a wide range of specific examples and use cases for biometric data in a variety of settings, including applications in law enforcement, public and border security, airport efficiency, device and enterprise security, banking and financial services, workplace monitoring and safety, marketing and customer experience, transportation and logistics, automotive safety, healthcare, fitness, education, and social media. In each of these areas, the use of biometric technologies holds significant benefits.

7 Office of Biometric Identity Management, "Biometrics," US Dept. of Homeland Security.

III. Risks and Concerns for Deployment of Biometric Technologies

The benefits of biometric technologies come with risks as well. For that reason, some biometric systems have met headwinds from regulators, media, and public opinion. Governments and companies have considered or are actively pursuing moratoria or bans on certain uses of biometric technologies, even for seemingly low-risk uses.[8] Key trends in law and regulatory enforcement are discussed in more detail in Section IV.

At the root of these concerns is the recognition that inaccurate, unreliable, or unsecure uses of biometric technologies—in the absence of relevant safeguards and effective redress measures—can lead to serious harm for individuals. While some of the risks detailed below are unique to biometric technologies, others are shared with other digital technologies; some apply even outside the technology space.

A. Accuracy

Despite substantial recent improvements, the risk of inaccuracy remains a crucial element to consider when deploying biometric technology. Potential harms can range from mere inconveniences (e.g., a false negative preventing an appropriately aged user from accessing a web service) to severe bias (via profiling) and unfairness (in criminal investigations).

Accuracy measures the rate at which biometric systems correctly score the collected sample to template records, considering false matches and false non-matches. A false match (false positive) occurs when an individual's biometric characteristic is incorrectly matched to a characteristic from another individual, whereas a false non-match (false negative) occurs when an individual's biometric characteristic is incorrectly identified as not matching a collected characteristic from that same individual.[9] Ranges in accuracy depend on several factors, including the type and quality of data collected, the age of the technology, and the number of templates provided for matching. For example, accuracy for deduplication of a quality template image (i.e., the process of eliminating redundant copies of data to reduce the amount of data stored)[10] is very high for fingerprints and iris scans. Facial recognition has historically been less accurate but has improved over time.[11] Additionally, the accuracy of some biometric characteristics can change due to factors like time or illness.[12] Generally, accuracy increases with the number of data points available.

Modern applications of biometric technologies are typically more accurate than previous versions, particularly where algorithms are combined with artificial intelligence. To provide one example, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) published an evaluation of facial recognition used at airports for authentication, finding that algorithms could "perform the task using a single scan of a passenger's face with 99.5% accuracy or better—especially if the

8 Low-risk applications of facial recognition technology by a public agency may include biometric-driven access to restricted buildings and biometric-driven tools that allow a public agency to blur faces in a video or photo before responding to a public access request.

9 "Biometric recognition and authentication systems," UK National Cyber Security Centre (24 January 2019).

10 Mary Clark, "Biometric Data De-duplication: Technology and Applications," Bayometric.

11 "Practitioner's Guide: Biometric Data," World Bank, Identification for Development.

12 See, for example, Esefan Ortiz, Kevin W. Bowyer, and Patrick J. Flynn, "A Linear Regression Analysis of the Effects of Age Related Pupil Dilation Change in Iris Biometrics," 2013, and Javier Galbally, Marcos Martinez-Diaz, and Julian Fierrez, "Aging in Biometrics: An Experimental Analysis on On-Line Singature," PLoS One, 2013.

database contains several images of the passenger."[13] NIST found that the accuracy of algorithms had generally improved over time. Notably, NIST determined that demographic differences in the data subject—e.g., national origin, race, or gender—had little effect on accuracy, but that older technology could sometimes yield highly detrimental outcomes because of its higher potential for inaccuracy.

That said, even when biometric technologies perform with great accuracy, biased results may still occur, as discussed in further detail below, and responsible deployment of such technologies may likely require socio-technical mitigations.[14]

B. Bias

In the words of a NIST publication, bias in AI systems can "perpetuate and amplify negative impacts on individuals, organizations, and society."[15] Indeed, in 2018, an independent research paper[16] showed that three major commercial facial recognition systems performed better (i.e., with greater accuracy) for lighter-skinned individuals and males.

Since then, various studies have shown that biometric systems can produce more false positives in groups of women, darker-skinned people, and the very young and old. For example, in December 2019, NIST published a study of 189 facial recognition programs and reported that algorithms developed in the United States were significantly more likely to return false positives and false negatives for Black, Asian, and Native American individuals than for white individuals.[17] Similarly, a 2020 study concluded that fingerprint systems are prone to age bias because fingerprints may disappear or become less pronounced because of medical treatments, chemical exposure, or manual labor.[18]

One important avenue for mitigating such biases and improving overall accuracy is to prioritize inclusivity and diversity in the teams building and monitoring AI models, as well as in the datasets used to train them.[19] Still, labeling data is itself a challenge due to a lack of consensus on standard measures.[20] Moreover, many data protection laws around the world restrict collection and use of sensitive personal data (such as age, ethnicity, and gender), requiring consent or some other limited legal grounds for processing such data. Nevertheless, this kind of information is important for biometric systems because it allows the developer to measure how well the system performs vis-à-vis each category or sub-group.

At times, data protection laws fail to recognize bias prevention as a compatible processing purpose. To overcome this obstacle, government and industry should consider recognizing datasets that are certified for diversity, meaning they include lawfully collected datapoints for developers to use that verifiably represent physical diversity. Still, more research is needed to better understand why some biometric systems produce biased results and how such harms can be mitigated.

Further, it is important to recognize that biometric systems are deployed by humans who themselves may make errors or carry or perpetrate bias. In June 2022, a man residing in Georgia, USA, was wrongly arrested for crimes committed in Louisiana, USA, due to a false positive facial recognition match.[21] The man spent several days in jail, unable to defend himself, because the arresting documents did not mention the use of facial recognition technology, which wrongly tied him to a crime committed in a state he had never visited.

13 "NIST Evaluates Face Recognition Software's Accuracy for Flight Boarding," NIST (17 July 2021).

14 The term "socio-technical" is broadly understood to denote an analysis that considers how the "social" (related to humans and organizations) and the "technical" (related to technology) interact with one another. *See* Oxford Reference, "Socio-technical system".

15 Reva Schwartz, Apostol Vassilev, Kristen Greene, Lori Perine, Andrew Burt, Patrick Hall, "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence" (NIST Special Publication 1270, 2022).

16 Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification".

17 "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," NIST (19 December 2019).

18 Andrea Rosales and Mireia Fernández-Ardèvol, "Ageism in the era of digital platforms" (Convergence, 2020).

19 Ayanna Howard and Charles Isbell, "Diversity in AI: The Invisible Men and Women," MIT Sloan Management Review, September 21, 2020.

20 For example, the UK census defines 19 categories for ethnicity, where the US Census Bureau defines five categories for race.

21 Kashmir Hill & Ryan Mac, "'Thousands of Dollars for Something I Didn't Do'", New York Times (31 March 2023).

To properly identify and mitigate risks associated with bias, developers and deployers of AI systems, including biometric technologies, should apply what NIST researchers call a "socio-technical" approach, which considers the context of the application.[22] In the case of the man who was wrongly arrested, a socio-technical approach would include disclosure—here, by the law enforcement agency deploying the technology—of the use of the facial recognition technology to support the issuance of the warrant.

C. Reliability and Availability

In addition to ensuring accuracy and impartiality, organizations must consider factors that impact availability of the technology and the reliability of samples, both of which are important for deriving the expected benefits from biometric applications. For example, in one well-publicized case, the Integrated Automated Fingerprint Identification System (IAFIS), developed by the U.S. Federal Bureau of Investigation (FBI), falsely matched a suspect's fingerprints to those found at the scene of a Madrid terrorist attack in 2004. Upon review, it was revealed that the FBI identification was based on an image of substandard (unreliable) quality, which returned a remarkable number of points of similarity between the two sets of prints.[23]

Reliability and availability are based on several factors, including the ability to use the application in a variety of environments, the stability of a biometric characteristic (which can change over time due to aging or injury, e.g., a deep cut on the finger pad), and the collectability of quality samples. Certain weather conditions or environmental factors, such as extreme temperatures, may decrease availability of the technology, while changes in individual biometric characteristics can impede reliance on the technology. Children's biometric characteristics are not reliable in certain cases; they may need to be updated over time as features mature. Moreover, acquiring reliable biometric samples may be difficult for certain populations (such as manual laborers, persons with certain disabilities, or persons with particular health conditions) due to the impermanence of the biometric over time or distinct biometric features or markers becoming less pronounced over time. This can, in turn, make enrolling such individuals with biometric technologies more difficult.[24]

Solutions for improving reliability and availability may be as simple as housing a biometric scanner in a weatherproof casing. Other applications may require more creative solutions, such as ensuring the use of the most recent version of a biometric system or alternative measures of identification.

D. Security

Security improvements are one of the principal advantages of biometric technologies. Biometric applications can reduce or eliminate the need for passwords and PINs, lowering the risk of unauthorized access to systems, databases, or buildings with stolen credentials such as passwords or identification badges. Passwords can be phished, forgotten, or otherwise compromised, but biometric characteristics are unique to individuals, adding a layer of security that is difficult to compromise.[25] Biometric applications also add convenience, replacing the need to remember certain things (like passcodes) with things individuals will always have with them (i.e., their hands, eyes, face, etc.).

While the use of biometric applications can increase security and add a factor of convenience, their use raises unique concerns because of their inherently individual nature. If lost or compromised, they cannot be reset or reissued. Given the pervasiveness of cyber incidents and data breaches, storing biometric data can present distinctive risks to individuals:

> "[A]lthough it may be more difficult to steal a biometric than a password, the potential consequences of this theft—e.g., the inability to reissue a biometric and the inherent linkability of the data—may be more severe. Practitioners must fully weigh these risks against the potential benefits of using biometric recognition."[26]

22 Schwartz et al., *supra* note 12, at 47.

23 "Statement on Brandon Mayfield Case," Federal Bureau of Investigation (24 May 2004).

24 "Practitioner's Guide: Biometric Data," World Bank, Identification for Development.

25 Alessandro Mascellino, "Why are biometrics better than passwords?" Biometric Update (30 August 2022); *see also* Bev O'Shea, "Which is Safer: Biometrics or Passwords?" Experian (2 August 2022).

26 *Id.*

Privacy enhancing technologies like trusted execution environments[27] can be used to store biometric data or templates securely with encryption. In such instances, biometric data or templates can be "stored without any identification information, and the data never leaves the user's device."[28] Importantly, biometric data stored in this way "cannot be accessed by the device's operating system or applications."[29]

E. Fraud

Although biometric systems can increase overall system security and prevent fraud, it is important to recognize that, absent certain mitigations, increased access to certain technological applications (e.g., deepfake videos and generative AI voice spoofs[30]) may make it easier for bad actors to exploit biometric systems and commit fraud.

Biometric systems turn biological or behavioral characteristics into "templates," and anyone with access to biometric templates can create a "spoof," or fake duplicate, to gain unauthorized access. For example, face "morphing"—a technique that relies on face scans—involves the submission of a manipulated image on an official identification document, like a passport. The morphed image is a compilation of two separate people (averaging the features of two different people into one image), allowing either of them to use the official identification document without detection.[31]

To protect against fraud, biometric system developers and deployers should consider multi-factor solutions.[32] For starters, organizations should avoid storing biometric templates in plain text and should consider using emerging technical solutions to help detect attack threats. Organizations can also use active and/or passive "liveness detection" technologies, which verify whether an individual is a live person permitted to access a system or a bad actor attempting to use a photo, video, or mask.[33] Active detection asks an individual to respond to certain prompts (e.g., by smiling), whereas passive detection applies advanced technical steps to review details such as skin texture.

While developers and deployers of biometric systems certainly need to mitigate against these kinds of risks at both a developmental and organizational level, it is much easier for fraudsters to take advantage of leaked passwords than to "spoof" biometric technologies. Successful spoofing of biometric technologies typically requires a greater degree of technical prowess than, for example, using leaked passwords or banking information.

F. Undisclosed Biometric Data Collection

Another concern unique to biometric systems is the potentially opaque nature of certain data collection settings and techniques. Some biometric data, like facial geometry, iris patterns, and the sound of an individual's voice, can be collected from a distance and without an individual's knowledge. Internet users, for instance, routinely post images of themselves online, creating the opportunity for others to collect or extract facial geometry or iris patterns from those photos without the individual's knowledge or consent.[34]

27 CIPL White Paper, "Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age", Dec. 2023.

28 *Id*. at 31.

29 *Id*.

30 A "spoof" imitates a biometric characteristic of another and attempts to trick a biometric system into producing a false result.

31 Kramer, R.S.S., Mireku, M.O., Flack, T.R. et al. Face morphing attacks: Investigating detection with humans and computers. Cogn. Research 4, 28 (2019).

32 "Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces," Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, August 2021.

33 Smita Khairnar, Shilpa Gite, Ketan Kotecha, and Sudeep D. Thepade, "Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions" (Big Data & Cognitive Computing, 2023).

34 "Street-level Surveillance: Iris Recognition," EFF.

The "10-year challenge" on Facebook (to post a photo of yourself now and a photo from 10 years ago) and the "eye challenge" on TikTok (to post an up-close, high-resolution video of your iris) are examples of online trends that created opportunities for biometric data collection.[35] A more extreme example was Clearview AI's mass scraping of publicly posted images to build a database of more than 20 billion images for its artificial intelligence-powered facial recognition product.[36] A retail store's alleged failure to disclose the use of facial recognition technologies in its stores, allegedly supported by employees' covertly taking photos of patrons, resulted in an enforcement action by the U.S. Federal Trade Commission in 2023.[37]

G. Privacy and Civil Rights

The risks discussed above—particularly those related to bias, security, and lack of transparency—have raised questions related to biometric technologies' impact on privacy and civil rights. Because biometric data is inherently personal and can be immutable over time,[38] the collection of such data and the use of these technologies can present significant privacy challenges. These may stem from the covert or surreptitious collection of personal data (as discussed above); the cross-matching or correlation of biometric data from unrelated datasets; the processing of biometric data for secondary, undisclosed purposes; or the collection of secondary information (such as health information) from biometric data.[39] Other risks and concerns regarding broader civil rights—such as freedom of movement, expression, and speech—can also arise depending on how biometric technology is used and within what context. These concerns are particularly present when state actors use biometric data for surveillance purposes.

In addition to the context of a given use case, risks to individual rights arise from other factors, such as the selection of safeguards measures (i.e., whether biometric data is stored on company servers, whether it is stored in plain text or as an algorithmic template), the size of the dataset underlying the biometric system, the method of collection, the use of the data (i.e., whether the data is used for identification, verification, classification, or detection purposes), the reliability and accuracy of data, and the measures taken to mitigate any of the above risks.

By way of example, greater risks are associated with one-to-many matching than with one-to-one or one-to-few matching.[40] In the case of one-to-one or one-to-few matching,[41] risks are generally lessened because the individual has previously provided a sample for verification purposes and where the sample template is locally stored on the individual's device.

By contrast, in settings that use one-to-many matching, newly collected samples are compared against many sample templates in a database, which may include sample biometric data that has aged. The level of risk, while generally elevated, varies based on the method of collection, the accuracy and reliability of the data, the safeguards used to prevent bias or correlation with other databases, the purposes of data matching, and the implementation of security controls. Without protections and mitigations, large databases for one-to-many matching can pose significant risks to privacy and other civil rights.

Large, commercial biometric identification systems can also pose significant risks for misuse. As mentioned above, Clearview AI amassed without consent over 20 billion photos from social media and public websites to be fed into its facial recognition system, which was subsequently offered to law enforcement agencies and private companies. Privacy regulators from various jurisdictions swiftly commenced investigatory actions, finding in many cases that the company violated the privacy rights of individuals. Notably, the French CNIL fined Clearview AI €20 million for collecting and processing sensitive data without a valid

35 Allison Fiedler, "New Trends May Help TikTok Collect Your Personal, Unchangeable Biometric Identifiers," ACLU (14 April 2022).

36 Christopher Burgess, "Clearview AI commercialization of facial recognition raises concerns, risks," CSO Online (8 March 2022).

37 Complaint for permanent injunction and other relief at 6, *Federal Trade Commission v. Rite Aid Hdqtrs. Corp.*, No. 2:23-cv-05023 (E.D. Pa. Dec. 19, 2023).

38 See, *supra*, Section III.C: Reliability and Availability

39 Data at Your Fingertips Biometrics and the Challenges to Privacy, Office of the Privacy Commissioner of Canada (February 2011).

40 An example of one-to-one matching would be an employee needing to scan both an access card and his fingerprint to enter a secure building (i.e., user data is searched first from the access card, then that data is matched with the provided biometric data). Contrastingly, one-to-many matching would be if that employee only used fingerprint matching (i.e. the provided fingerprint is compared against all users in the database).

41 One-to-one (or one-to-few) verifies an individual by using a primary identifier (ID card), which compares a newly collected sample to a single stored template or small number of stored templates associated with the user.

legal basis,[42] and the UK Information Commissioner's Office fined the company £7.5 million for similar violations. Additionally, data protection authorities in Austria, Australia, Canada, France, Italy, Greece, and the UK ordered Clearview AI to delete all existing data belonging to individuals in those countries.[43]

H. Cost and Social Impacts

In addition to the risks mentioned above, the costs of implementationand the social and political impacts of biometric systems should all be considered.

High costs—i.e., cost of implementing and maintaining the system, capturing the sample collection data, and checking the data against a template—can discourage implementation of biometric systems at scale.[44] Costs may also include ensuring interoperability and security of a system as well as training users and owners of those systems.[45] Costs can vary based on the context, including the type of biometric characteristic subject to collection (fingerprints, iris scans, and facial scans all have different costs associated), the specific industry, the need for reliability and availability, and the need for certain safeguards. The social and political impacts of biometric systems relate to issues of equal access and equal treatment. The ability to benefit from the use of biometric technologies must be accessible to all populations. For example, biometric applications should not require individuals to change their behavior or appearance for the system to work properly, such as by requiring the removal of head coverings (which could impact religious sensibilities). Nor should they require a response to an auditory or visual cue (which could exclude individuals with sight or hearing limitations), without an alternative. To respect individual rights, developers and deployers should account for inclusivity and accessibility in the design of biometric systems or create easy and clear alternatives.

42 "CNIL Fines Clearview AI 20 Million Euros for Unlawful Use of Facial Recognition Technology", Hunton Andrews Kurth: Privacy & Information Security Law Blog (24 October 2022), available at

43 Austria, Australia, Canada, France, id., Italy, Greece, UK.

44 "Practitioner's Guide: Biometric Data," World Bank, Identification for Development.

45 Jessica Groopman, "In biometrics, security concerns span technical, legal and ethical," TechTarget (June 2020).

IV. Landscape of Laws on Biometric Data

In recognition of the risks associated with biometric technologies, legislators and regulators have advanced a range of proposals and requirements, from notice-and-consent regimes to outright bans in certain settings. This section provides an overview of the various regulatory approaches enacted and proposed in the United States, the United Kingdom, the European Union, and around the globe.

Statutory terms and definitions vary widely across jurisdictions, and most jurisdictions target biometric data linked to a uniquely identifiable person (hereinafter described as the "identification element") for heightened compliance requirements. Appendix A provides a chart highlighting how jurisdictions define key terms like *biometric data, biometric identifier,* and *biometric information* and whether jurisdictions consider biometric data to be *sensitive data*.

While legal definitions are important and have various implications, CIPL believes that lawmakers and regulators should focus on the **uses of biometric technology**—and viewing such uses through a risk-based lens—rather than focusing on the **types of data** underlying the technology.

A risk-based approach ensures that low-risk applications can be deployed without undue restraints, that higher or high-risk applications are deployed with appropriate protections and mitigation measures, and that substantial regulatory hurdles or complete bans are reserved only for high-risk uses where effective safeguards are not available.

A risk-based approach is essential to determine when, where, how, and whether the use of biometric data is appropriate in each circumstance. A risk-based approach ensures that low-risk applications can be deployed without undue restraints, that higher or high-risk applications are deployed with appropriate protections and mitigation measures, and that substantial regulatory hurdles or complete bans are reserved only for high-risk uses where effective safeguards are not available. Such an approach avoids both overregulating and underregulating biometric technologies, which oftentimes can be applied in both high- and low-risk situations (as in the case of facial recognition technology, for example).

A. United States

At the time of this writing, the United States has neither a comprehensive federal data protection law nor a federal law specifically targeting biometric technology. However, in May 2023, the U.S. Federal Trade Commission issued a policy statement on the commercial use of biometric information,[46] defining biometric information rather expansively by including photographs within its scope:

> [T]he term "biometric information" refers to data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body. Biometric information includes, but is not limited to, depictions, images, descriptions, or recordings of an individual's facial features, iris or retina, finger or handprints, voice, genetics, or characteristic movements or gestures (e.g., gait or typing pattern). Biometric information also includes data derived from such depictions, images, descriptions, or recordings, to the extent that it would be reasonably possible to identify the person from whose information the data had been derived. By way of example, *both a photograph of a person's face and a facial recognition template, embedding, faceprint, or other data that encode measurements or characteristics of the face depicted in the photograph constitute biometric information*.[47]

Most laws defining *biometric data* expressly exclude photographs from the definition.[48]

At the U.S. state level, legislative efforts have included a variety of sector-specific measures, comprehensive privacy laws, and laws narrowly tailored to biometric identifiers and/or data. At the time of this writing, a number of U.S. states have enacted restrictions addressing the processing of biometric data or biometric information of students and minors,[49] and three have enacted laws that regulate the collection and use biometric data more generally (discussed in the paragraphs that follow). In 2021 and 2022, more than half of U.S. states introduced legislation proposing restrictions and/or guidance on uses of biometric information,[50] and in 2023, more than ten states had introduced legislation regarding biometric technology deployments both in the private and public sector.[51] This level of widespread activity evidences a state-level trend in favor of regulating the use of biometric technologies.

Illinois, Texas, and Washington are the three U.S. states that have passed laws specifically regulating the commercial use and collection of biometric data. These laws largely focus on requiring informed consent from individuals for collection and use of biometric data and allowing individuals to opt out of the sale or disclosure of their biometric information to third parties.

Illinois: The Illinois Biometric Information Privacy Act (BIPA), enacted in 2008, was the first U.S. state law aimed specifically at the protection of biometric data, and it remains one of the most stringent.[52] BIPA creates parameters around the collection, use, and security of "biometric identifier[s]" and "biometric information," noting that such data carries heightened risks because "once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[53]

46 Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act, 18 May 2023. Note that FTC Policy Statements are not law and do not preempt federal, state, or local law, rather they denote the FTC's interpretation of issues within its regulatory scope.

47 *Id.*, p. 1 (emphasis added).

48 *See* Appendix A.

49 For example, Fla. Stat. § 1002.222(1)(a) is a 2014 Florida law that prohibits state agencies, primarily schools, from collecting, obtaining, or retaining biometric information of a student or a parent or sibling of a student.

50 Pam Greenberg, "2021 Consumer Data Privacy Legislation," NCSL (27 December 2021).

51 "2023 State Biometric Privacy Law Tracker: A Comprehensive Resource for Tracking U.S. State Biometric Privacy Legislation," Husch Blackwell (last updated 20 June 2023).

52 Biometric Information Privacy Act, 740 ILCS 14/1 et seq

53 740 ILCS 14/5(c).

Some of the key features of BIPA include:

- **Terminology:** BIPA's provisions apply to the use of "biometric identifiers," defined narrowly to mean a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry,"[54] and "biometric information," which means "any information…based on an individual's biometric identifier used to identify an individual."[55]
- **Scope:** BIPA applies to commercial and public sector entities but does not apply "in any manner o a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder."[56]
- **Notice and Consent:** Covered businesses are required to obtain written informed consent prior to the collection of biometric information and biometric identifiers.[57]
- **Limitation on Disclosures:** Disclosure of biometric information is permitted only under limited circumstances.[58]
- **Reasonable Security:** Covered businesses must have reasonable security measures in place, including technical, physical, and organizational safeguards.[59]
- **Retention and Destruction Policies:** Covered businesses must maintain written retention and destruction policies for biometric information.[60]
- **Prohibition on Sale:** Covered businesses are prohibited from profiting from biometric information.[61]
- **Private Right of Action:** Individuals harmed by BIPA violations are granted a private right of action.[62]

BIPA distinguishes between ***biometric identifiers***, which are limited to a prescriptive list of physiological characteristics, and ***biometric information***, which adds the identification element (i.e., the ability to be linked to a uniquely identifiable person) to the prescriptive list of biometric identifiers. The adoption of BIPA has resulted in a significant uptick in litigation, class actions, and settlements, often surrounding the issue of knowledge and consent.[63] After the Illinois Supreme Court ruled in 2023 that a separate claim occurs each time a covered business scans or transmits a biometric identifier in violation of the statute,[64] BIPA-related litigation shows no signs of abating.[65]

Texas: The Texas Capture or Use of Biometric Identifier Act (CUBI) was passed a year after BIPA, and includes many similar requirements.[66] Like BIPA, CUBI applies only to commercial use of "biometric identifiers," narrowly defined to mean "retina or iris scan[s], fingerprint[s], voiceprint[s], or record[s]s of hand or face geometry."[67] Unlike BIPA, however, CUBI does not include the identification element within its definition. Nor does it include a private right of action for individuals. Only the Texas attorney general can bring an enforcement action, but potential civil exposure and penalties are still substantial.[68] Whereas BIPA does not apply to financial institutions covered by the Gramm-Leach-Bliley Act, CUBI includes a limited exception for "voiceprint data retained by a financial institution."[69]

54 740 ILCS 14/10.

55 *Id.*

56 740 ILCS 14/25.

57 740 ILCS 14/15(b).

58 740 ILCS 14/15(d).

59 740 ILCS 14/15(e).

60 740 ILCS 14/15(a).

61 740 ILCS 14/15(c).

62 740 ILCS 14/20.

63 *See*, for example, the ACLU's settlement with Clearview in which Clearview has agreed to a nationwide injunction barring access to the Clearview App by: (i) any private entity or private individuals unless such access is compliant with BIPA; or (ii) any governmental employee not acting in his or her official capacity. Cleary, Shifrin, and Green, "Facial Recognition: Clearview-ACLU Settlement Charts a New Path for BIPA and the First Amendment," National Law Review (12 May 2022).

64 Cothron v. White Castle Systems, Inc., 2023 IL 128004 (February 17, 2023) ("We hold that a separate claim accrues under the Act each time a private entity scans or transmits an individual's biometric identifier or information in violation of section 15(b) or 15(d).")

65 The Illinois legislature considered legislation in 2024 to amend BIPA, including the statutory definition of "biometric identifier", consent requirements, and limiting damages available to claimants. *See* S.B. 2979, 103rd Gen. Assemb. (Il. 2024).

66 Tex. Bus. & Com. Code Ann. § 503.001.

67 *Id.* § 503.001(a).

68 Up to $25,000 for each violation. *Id.* § 503.001(d).

69 *Id.* § 503.001(e).

Washington: The State of Washington has two laws that address biometric data—one targets the use of biometric identifiers for commercial purposes[70] and the other focuses on the use of biometric identifiers by state agencies.[71] The statute targeting commercial use, similar to CUBI and BIPA, applies to biometric identifiers "enrolled" for a commercial purpose.[72] Enrolled means "to capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual."[73] "Biometric identifier" means "data generated by automatic measurements of an individual's biological characteristics…or other unique biological patterns or characteristics that is used to identify a specific individual."[74] As emphasized, Washington's law does include the identification element within its definition.

The law exempts organizations that enroll biometric identifiers for security purposes from notice and consent requirements.[75] Like BIPA, it does not apply to financial institutions subject to the Gramm-Leach-Bliley Act.[76]

Like CUBI, Washington's law does not include a private right of action; only the Washington Attorney General has the power to enforce its provisions.[77] Washington law authorizes a maximum of $7,500 penalty per violation.[78]

Other State Efforts: Some additional, more targeted approaches to biometric data exist in other U.S. state laws. Here are few examples:

- **Arkansas** amended its data breach notification laws in 2019 to require notification when biometric data is compromised. Under this law, biometric data is included in the definition of covered personal data and is defined as an individual's "fingerprints; faceprint; retinal or iris scan; hand geometry; voiceprint analysis; deoxyribonucleic acid (DNA); or any other unique biological characteristics."[79]
- **Maryland** prohibits employers from using facial recognition technology during employment interviews unless the applicant provides informed consent.[80]
- **New York** passed a law that prohibits collecting or using fingerprint data as "a condition of securing employment or of continuing employment."[81]

Numerous U.S. cities have adopted ordinances governing biometric data, often specifically directed at facial recognition technologies.[82] Portland, Oregon, for example, has banned private entities from using facial recognition technologies in public spaces.[83] New York City, for example, requires a notice of collection of biometric data and prohibits the sale of biometric data by commercial organizations; it also provides individuals with a right to sue.[84] Baltimore enacted a temporary facial recognition moratorium that has since been lifted.[85]

70 Wash. Rev. Code § 19.375 (2017).

71 See Wash. Rev. Code § 40.26.020 (2022).

72 Wash. Rev. Code § 19.375.020(1).

73 Wash. Rev. Code § 19.375.010(5).

74 Wash. Rev. Code § 19.375.010(1) (emphasis added).

75 Wash. Rev. Code § 19.375.020(6), (7). Security purpose is defined as: "preventing shoplifting, fraud, or other misappropriation or theft; and other purposes to protect the security or integrity of software, accounts, applications, online services, or any person." Wash. Rev. Code § 19.375.010(8).

76 Wash. Rev. Code § 19.375.040(1).

77 Wash. Rev. Code § 19.375.030(2).

78 *See* Wash. Rev. Code § 19.375.030. *See also* Wash. Rev. Code § 19.86.140.

79 Arkansas Code §4-110-103(7). New York similarly amended its breach notification law to include biometric information. *See* SHIELD Act, New York Laws 2019, ch. 117,Sec. 3, eff. 10/23/2019, codified at N.Y. Gen. Bus. Law § 899-AA.

80 Maryland Labor and Employment Code § 3-717.

81 N.Y. Lab. Law §201-a.

82 Nathan Sheard and Adam Schwartz, "The Movement to Ban Government Use of Face Recognition," Electronic Frontier Foundation (5 May 2022).

83 "City Council approves ordinances banning use of face recognition technologies by City of Portland bureaus and by private entities in public spaces," Portland.gov (9 September 2020).

84 N.Y.C. Admin. Code §§ 22-1201 to 22-1205.

85 City of Baltimore Council Bill 21-0001, *the Ordinance Concerning Surveillance Technology in Baltimore*. The moratorium expired at the end of 2022.

Comprehensive State Privacy Laws: In addition to legislation specifically addressing biometric data, many U.S. states have passed "comprehensive" (or otherwise broad-reaching) data privacy laws.[86] Each of these laws covers "biometric data," and each classifies it as "sensitive data." The definitions, however, differ slightly under each law.[87] For example, California's law is the only one that explicitly includes DNA in the definition of biometric information.[88] The laws of Colorado,[89] Connecticut,[90] New Hampshire,[91] Utah,[92] and Virginia[93] specifically exclude digital and physical photographs, audio or voice recordings, or data generated from either of those.

While all of the comprehensive ste privacy laws limit their definition of "biometric data" to data that is used for the purpose of identifying a specific individual, there are inconsistencies in the statutory definitions when it comes to the identification element. The majority of state laws look at use and intent (e.g., *"data...that **is used** to identify a specific individual"*[94]), and a minority include the *potential* for identification (e.g., *"data...that **can be** processed for the purpose of uniquely identifying an individual"*[95]). As stated, all comprehensive state privacy laws include biometric data processed for identifying purposes under the scope of sensitive data and impose additional requirements on such processing activities, including additional consent or opt-out requirements[96] or requirements to conduct privacy impact assessments.[97]

B. European Union

In the EU, the primary legal obligations around biometric data come from the General Data Protection Regulation (GDPR).[98] There are other regulations,[99] directives,[100] and documents that provide guidance on the use of certain biometric technologies, such as the Council of Europe's Guidelines on facial recognition, published in June 2021.[101] Data protection authorities have also noted concerns around the use of biometric technologies and have been active in enforcement actions involving biometric data, as detailed below. The potential risks of biometric technology have also heavily impacted the negotiations around the EU Artificial Intelligence Act (AI Act).[102]

GDPR: Under the General Data Protection Regulation, "biometric data" is defined as:

> [P]ersonal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data[.][103]

86 As of March 2024, the following states adopted their own comprehensive privacy laws: California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia. We include Florida in our list of comprehensive laws, although some sources do not label it as such due to its applicability to a limited set of entities.

87 See Appendix A.

88 Cal. Civ. Code § 1798.140(c).

89 4 CCR 904-3-2.02

90 Conn. Gen. Stat. § 42-515(4).

91 S.B. 255 (N.H. 2024) (effective Jan. 1, 2025).

92 Utah Code § 13-61-101(6)(c).

93 Va. Code § 59.1-575.

94 *Id.* (emphasis added).

95 4 CCR 904-3-2.02 (emphasis added).

96 For example, Colorado, Connecticut, and Virginia all require consent for processing sensitive personal data; Utah requires clear notice and opportunity to opt-out of processing of sensitive personal data; and California creates a right for data subjects to limit the use and disclosure of sensitive personal information.

97 For example, California, Colorado, Connecticut, and Virginia have requirements for businesses conducting high-risk processing activities, which includes the processing of sensitive data.

98 Regulation (EU) 2016/679.

99 Regulation (EU) 2018/1725 – Art 3(18) (processing of personal data by the Union institutions, bodies, offices and agencies).

100 Directive (EU) 2016/680 Art 3 (13) processing for law enforcement purposes.

101 Guidelines on facial recognition, Adopted by the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), Council of Europe (June 2021).

102 The European Parliament granted final approval to the EU AI Act on March 13, 2024, with an overwhelming majority. EU Member States are set to grant their final approval by May 2024. Following this final vote, the EU AI Act will enter into force 20 days after its publication in the Official Journal of the European Union. The latest version of the text available at the time of this writing can be found here.

103 GDPR Article 4(14).

Biometric data is considered a special category of data under Article 9[104], and therefore subject to heightened compliance requirements, to the extent it is processed "for the purpose of uniquely identifying a natural person."[105] However, biometric data can also fall under Article 9 if it reveals an individual's race, ethnicity, or health data.[106]

The European Data Protection Board (EDPB) issued guidance in January 2020 addressing the processing of personal data through video devices, noting that video footage of an individual cannot in itself be considered biometric data under Article 9 if it has not been specifically technically processed in order to contribute to the identification of an individual.[107] The guidance also addressed the applicability of the GDPR in the context of biometric technology more generally, the legal basis for any such processing, and the extent to which data protection impact assessments and other mitigation measures should be considered. Notably, the guidance distinguished "raw data" (such as a photograph or video footage) from "biometric data," which (unlike raw data) involves special technical processing that results in a measurement of an individual's characteristics as captured by raw data.[108] The guidance also suggested keeping biometric templates on an individual's device rather than storing them in a database, but it emphasized the need for encryption when biometric templates are stored in a database controlled by an organization.[109]

In May 2023, the EDPB also issued guidance on the use of on facial recognition technologies in the area of law enforcement.[110] The Guidelines address lawmakers at the EU and EU Member State level, and law enforcement authorities and their officers implementing and using facial recognition technology. The Guidelines consist of the main body of guidance, along with three annexes which include: (1) a template for assessing the severity of the interference with fundamental rights caused by facial recognition technology; (2) practical guidance for authorities wishing to procure and run facial recognition technology; and (3) a set of hypothetical scenarios and relevant considerations based on certain uses of facial recognition technology.

Enforcement Efforts: As the EU advances efforts to provide guardrails around the deployment of systems using biometric data (discussed below), European data protection authorities have been active in enforcing the provisions of the GDPR. Most prominent among them are the investigations of and fines levied against Clearview AI in Italy, France, Greece, and Austria, as well as the United Kingdom.[111]

EU AI Act: The European Union's AI Act [112] applies a risk-based regulatory approach and distinguishes biometric systems in relation to their use and the risks they present to fundamental rights and freedoms. The European Parliament granted final approval to the EU AI Act on March 13, 2024, with an overwhelming majority. EU Member States are set to grant their final approval by May 2024. Following this final vote, the EU AI Act will enter into force 20 days after its publication in the Official Journal of the European Union.

Based on the latest version of text available, the "notion of 'biometric data' should be interpreted in light of the notion of biometric data as defined in [the GDPR]."[113] The AI Act goes on to introduce and distinguish between seven separate kinds of biometric systems—"biometric identification," "biometric verification," "emotion recognition system," "biometric categorisation system," "remote biometric identification system," "real-time remote biometric identification system," and "post remote biometric identification system."[114] Some biometric systems are considered prohibited[115], i.e., biometric

104 Article 9 of the GDPR prohibits the processing of special category data unless it falls in one of ten exceptions.

105 GDPR Article 9.

106 *Id.*

107 Guidelines 3/2019 on processing of personal data through video devices, European Data Protection Board, Version 2.0 (29 January 2020), p. 18.

108 *Id.* at 18.

109 *Id.* at 21.

110 Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, European Data Protection Board, Final Version (17 May 2023).

111 "When AI-powered Tools Bring (EU) Privacy Troubles – Biometric Templates Identify First," National Law Review (25 October 2022).

112 The latest version of the text available at the time of this writing (March 13, 2024) can be found here.

113 *Id.* at Recital 14..

114 *Id.* at Article 3(35)(36)(39)(40)(41)(42) & (43)

115 *Id.* at Article 5.

categorization, emotion recognition systems related to workplace and education, and the use of real-time remote biometric identification systems in public spaces by law enforcement[116], while others are considered high-risk[117], i.e., remote biometric identification, biometric categorization, and emotion recognition systems, and subject to heightened compliance and transparency requirements.

Digital Markets Act (DMA): Among other obligations, the DMA[118] prohibits large platforms designated as "gatekeepers" from combining or cross-using personal data between their core platform services[119] unless the end-user has provided GDPR-style consent or gatekeepers rely on a limited set of other legal bases for processing under the GDPR.[120] It is uncertain whether and to what extent biometric technology will be impacted by the DMA's restriction on data combination and cross-use of personal data. This requires further regulatory guidance because certain *potentially* prohibited practices relating to the use of biometric data could be beneficial for identification and verification purposes, especially in the context of fraud prevention and public security. EU stakeholders should consider whether steps should be taken to ensure that data combination and the cross-use of personal data are permissible for security and fraud prevention purposes.[121]

C. United Kingdom

The United Kingdom's General Data Protection Regulation (UK GDPR) provides the same protections as the EU GDPR with respect to special categories of data. The UK Information Commissioner's Office (ICO) has published guidance on special categories of data under the UK GDPR, including biometric data,[122] and in an October 2022 press release, expressed concern about biometric applications in high-risk settings.[123] There, the ICO warned organizations to assess risks of using emotion analysis technologies, which may in some cases rely on biometric data, noting that the risks presented ("bias, inaccuracy, and…discrimination") outweigh the benefits.[124]

Also in 2022, the ICO simultaneously published reports on biometric technology insights and foresights. The insights report detailed the current landscape and legal contexts for biometric technologies,[125] while the foresights report examined the near-term privacy considerations of deploying biometric technologies in a number of sectors.[126] It also identified key issues in biometric systems, including:

- The need to clarify key terminology and definitions surrounding biometric technologies and data.
- The increased use of biometric technologies for classification and where this sits under existing data protection legislation.
- The need for compliance with transparency and lawfulness requirements when processing ambient data.
- The need to understand and appropriately manage high-risk biometric technologies, such as some (but not all) applications of emotion recognition AI (e.g., use of personal data to analyze subconscious behaviors and responses).[127]

116 The use of real-time remote biometric identification systems by law enforcement will be permitted under certain narrow exceptions. *See id.* at Article5(h).

117 *See id.* at Article 26. *See also id.* at Annex III.

118 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (DMA).

119 *Id.*, DMA Article 5(2).

120 Specifically, GDPR Article 6(1)(c), (d), and (e): compliance with legal obligation, vital interest protection, or public interest legal grounds respectively. DMA Article 5(2).

121 *See* CIPL Discussion Paper, "Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences," (May 2023), at 16-19 (Case Studies of Data Combination and Data Cross-use for Security and Fraud Prevention and ensuing discussion).

122 *See* "What is special category data?" UK Information Commissioner's Office (ICO).

123 "'Immature biometric technologies could be discriminating against people' says ICO in warning to organisations," ICO (26 October 2022).

124 *Id.*

125 Innovation and Technology—Biometrics: insight, ICO (26 October 2022).

126 Innovation and Technology—Biometrics: foresight, ICO (26 October 2022).

127 *Id.*, at p. 3.

In February 2024, the ICO released new guidance on the use of biometric data in biometric recognition systems.[128] The guidance introduced a new term to the ICO's lexicon—"biometric recognition"—to describe the processing of biometric data to "uniquely identify someone," and it provided various examples to illustrate data protection concepts that are relevant to biometric recognition. The guidance seeks to provide more clarity to organizations regarding the distinctions between personal data, biometric data, and special category data, as well as the distinct compliance requirements that arise based on what kind of data is being processed. Importantly, the guidance stressed that the use of biometric recognition systems requires a lawful basis and an Article 9 condition for processing special category data.

The ICO expects to publish guidance covering biometric classification or categorization systems by the end of 2024. Furthermore, the ICO has prioritized biometric technology as a key area of focus for regulatory sandboxes[129] and conducted extensive focus groups with the British Youth Forum and a Citizens' Biometrics Council.[130]

D. Other Noteworthy Jurisdictions

Several other countries have initiated actions related to biometric data privacy, including:

Australia

In November 2021, the Australian Information Commissioner and Privacy Commissioner found that Clearview AI had breached Australia's Privacy Act 1988 by collecting sensitive information without consent and through unfair means, among other violations. In doing so, the Commissioner found that the privacy impacts of Clearview AI's biometric system were not "necessary, legitimate and proportionate" in terms of their public interest benefit. Clearview AI was ordered to cease collecting facial images and destroy existing images and biometric templates of people in Australia.[131] Although Clearview AI subsequently challenged the Commissioner's decision on jurisdictional grounds, the Administrative Appeals Tribunal of Australia found that Clearview AI had an "Australian link" and was therefore bound by the Privacy Act 1988.[132]

The Australian Government has also proposed to modernize its data privacy law, which includes updates addressing the use of biometric data and biometric technologies.[133]

Brazil

Brazil includes "biometric data" within the definition of sensitive personal data under its data protection law—Lei Geral de Proteção de Dados (LGPD)—but the statute does not define the term.[134] Under the LGPD, biometric data must be processed with an individual's consent unless the processing falls within one of seven specific situations.[135]

Canada

In May 2022, the Office of the Privacy Commissioner of Canada released an Interpretation Bulletin on Sensitive Information, which identified biometric information as "sensitive in almost all circumstances, as it is intrinsically, and in most instances permanently, linked to the individual. It is distinctive, stable over time, difficult to change and largely unique to the individual."[136] The Bulletin further listed facial biometric information as particularly sensitive "as it may allow for the identification of an individual through comparison against a vast array of images available on the internet or via surreptitious surveillance."[137]

128 ICO, Biometric data guidance: Biometric recognition (February 2024).

129 Regulatory Sandbox, "Our key areas of focus for the Regulatory Sandbox," ICO.

130 ICO, Biometrics technologies; *see also* Events, "Biometric Technologies and data protection," ICO (1 November 2022).

131 "Clearview AI breached Australians' privacy", Office of the Australian Information Commissioner, 3 November 2021.

132 Clearview AI Inc. and Australian Information Commissioner, AATA 1069 (8 May 2023).

133 *See* Privacy Act Review Discussion Paper (Oct. 2021) and Privacy Act Review Report 2022. *See also* Government Response to the Privacy Act Review Report.

134 Brazilian General Data Protection (LGPD, English translation), Article 5(II).

135 *Id.*, LGPD Article 11(1).

136 "Interpretation Bulletin: Sensitive Information," Office of the Privacy Commissioner of Canada (May 2022).

137 *Id.*

At the time of this writing, the Canadian Parliament is considering Bill C-27,[138] which would replace the private sector privacy regime currently set forth in the Personal Information Protection and Electronic Documents Act (PIPEDA) with a new Consumer Privacy Protection Act. It would also create the Artificial Intelligence and Data Act (AIDA), which, according to amendments proposed by the Minister of Innovation, Science and Industry in a November 2023 letter,[139] would classify an artificial intelligence system that processes biometric information as a "high-impact system."

China

China includes "information on biometric characteristics" within the definition of sensitive personal information under the Personal Information Protection Law (PIPL). PIPL does not define "biometric characteristics"; however, it does require consent for the handling of such data.[140] PIPL also ostensibly limits deployment of biometric applications to purposes that are specific and sufficiently necessary.[141]

Japan

Japan's Personal Information Protection Commission (PIPC) released a draft report in January 2023 to provide clarity on rules governing private sector collection and use of biometric and facial recognition technologies.[142] The report does not adopt specific guidelines or cover biometric technology applications by the public sector.

Kenya

Kenya's Data Protection Act of 2019 defines "biometric data" as "personal data resulting from specific technical processing" and includes biometric data within the statutory definition of sensitive data.[143] Notably, the Kenyan law does not include the identification element within the definition of "biometric data."

Kenya's Data Protection Regulations[144] provide that a data controller or data processor may collect personal data **indirectly** from "biometric technology, including voice or facial recognition."[145] They also provide that the processing of biometric or genetic data is considered to result in "high risks to the rights of freedoms of a data subject,"[146] thereby requiring the completion of a data protection impact assessment.

Singapore

Singapore's Personal Data Protection Commission (PDPC) released a *Guide on Responsible Use of Biometric Data in Security Applications* in May 2022. The Guide reviews unique risks of biometric recognition technology, examines best practices for governing biometric data, and analyzes biometric data obligations as related to the Personal Data Protection Act (PDPA).[147]

South Africa

South Africa includes a definition for "biometrics" in its comprehensive personal data privacy law ("a technique of personal identification…") but does not define the term "biometric information," despite referencing the term.[148]

138 An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts.

139 Canada. Innovation, Science and Economic Development Canada, Letter to the Chair of the Standing Committee on Industry and Technology on Bill C-27 (November 28, 2023), available at

140 Personal Information Protection Law of the People's Republic of China (2021), English translation by Rogier Creemers and Graham Webster.

141 *Id.*; see also Megan Gates, "China's New Data Privacy Law Goes Into Effect," ASIS International (5 November 2021).

142 Toko Sekiguchi, "Japan clarifies private sector facial recognition use rules, stops short of new rules or guidelines," mlex (12 January 2023).

143 Data Protection Act, 2019, Part 1(2).

144 Data Protection (General) Regulations, 2021 (DPG Reg).

145 *Id.*, DPG Reg. 6(e).

146 *Id.*, DPG Reg. 49(1)(c).

147 Guide on Responsible Use of Biometric Data in Security Applications, Personal Data Protection Commission and Security Association Singapore (2022).

148 Protection of Personal Information Act, Chapter 1.

V. Evaluating Challenges in the Regulatory Landscape

As discussed above, biometric technology has distinctive properties that can pose substantial risk, ranging from false positives and negatives, to fraud, to violations of individual rights. At the same time, the use of biometric technology holds significant potential for unlocking important benefits. In regulating the use of biometric technology, key stakeholders must consider three principal challenges: (1) reconciling definitions, scope, and terminological differences across jurisdictions and industry, (2) applying an appropriate legal basis to the processing of biometric data, and (3) understanding the fast-evolving nature of biometric technologies.

Lawmakers, policymakers, regulators, and organizations must strike the right balance between protecting individuals from high-risk biometric applications and enabling innovative, beneficial, and low-risk uses of biometric technologies.

A. Definition, Scope, and Terminology Challenges

One major challenge regarding biometric technology, particularly across various data protection laws, is the use of different terminology and the varying scope of coverage.

One major challenge regarding biometric technology, particularly across various data protection laws, is the use of different terminology and the varying scope of coverage. The majority of data protection laws regulate only biometric data that is intended to be used to identify an individual, providing non-exhaustive lists of what is considered a biometric characteristic. Some exclude data such as photographs from the definition of biometric data, distinguishing a photograph of a face from an algorithmic face template derived from a photograph of a face.

While many laws generally follow the GDPR approach (which includes the identification element along with a non-exhaustive list of biometric characteristics), that is not the case universally, as seen by the Texas CUBI law,[149] which does not limit its scope to applications that identify a particular person. Texas's approach is burdensome and short-sighted because it treats low-risk applications the same as high-risk applications. Further, some laws, like Brazil's LGPD and China's PIPL, do not define "biometric data" or "biometric" information despite including such terms in their definitions of sensitive personal data. This lack of clarity, especially without corresponding guidance from regulators, creates uncertainty and risk for organizations.

Additionally, some laws provide prescriptive lists detailing what kind of biometric characteristics fall under the scope of the law, while others provide non-exhaustive lists. Again, under Texas law, a "biometric identifier" is limited to a "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry"[150] whereas under California law, "biometric information" includes physiological, biological, or behavioral characteristics.[151] California law goes on to explain that:

149 Discussed *supra*, in Section IV.A

150 Tex. Bus. & Com. Code § 503.001.

151 Cal. Civ. Code § 1798.140(c).

> Biometric information includes, *but is not limited to*, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.[152]

While discrete lists of covered data types have the benefit of providing certainty, they also risk becoming obsolete as technology continues to evolve. Laws that include lists of what constitutes a biometric characteristic should also include provisions that allow for nimble updates of those lists, as appropriate. Regulatory sandboxes and other co-regulatory tools can play an important role in facilitating effective guidance regarding the scope of the law and encouraging compliance from developers and deployers.

Future laws and regulations should strive toward greater consistency on definition, scope, and terminology—with the inclusion of an identification element, as discussed above—to help facilitate certainty and uniform guardrails for responsible and innovative deployments, thereby fostering trust in responsible biometric technologies. Lawmakers and regulators should align their terminology and definitions with standards organizations, like the ISO, which is heavily relied on by industry. Such alignment can encourage interoperability and beneficial data exchanges.

B. Applying an Appropriate Legal Basis to the Processing of Biometric Data

A second challenge relates to lawful **grounds for processing biometric data**. If covered biometric data is considered sensitive data, then the rules in global data privacy laws for sensitive data would apply. These rules are stringent and impose additional legal requirements and restrictions, irrespective of the actual purpose of use and the risks and benefits involved. For example, the GDPR prohibits the processing of sensitive data unless the processor has secured explicit consent from individuals or the processing is necessary for one of the purposes listed under Art. 9(2).[153] Many of these purposes would not apply to the processing of biometric data in most contexts,[154] leaving consent as the only realistically available legal ground, even when biometric systems are used for verification purposes.

While consent is an important means for individuals to control the use of their data and will be justifiable and necessary in some cases of biometric data use, it is not always the most effective way to protect individuals and mitigate the risks associated with biometric technologies. For example, explicit consent is not a viable option for processing biometric data in the context of fraud prevention, yet many financial institutions rely on biometric technologies that process behavioral biometric data, like keystroke dynamics, to verify whether a user interacting with a financial application is legitimate.[155] Without a suitable legal basis for processing biometric data for fraud prevention purposes, certain legitimate and beneficial uses of biometric technologies could be unavailable.

Rather than applying the broad restrictions of "sensitive data" to biometric data, legislators and policymakers should consider establishing a risk-based, nuanced approach to the lawful processing of such data. Under such an approach, organizations would need to demonstrate accountability and comply with relevant data protection principles, *viz.*, fair processing, purpose limitation and compatible use, transparency and privacy notice requirements, accuracy and adequacy requirements, data protection risk assessment requirements, data security, privacy and security by design, international data transfers restrictions, individual rights of access, objection, correction, deletion, etc. Arguably, the application of relevant data protection principles will have more impact on individual rights and on responsible biometric technology development and deployment than the application of an express consent requirement.

152 *Id.* (emphasis added).

153 GDPR Article 9(2).

154 *Id.* For example, where processing is necessary for carrying out obligations in the field of employment and social security law; where processing is necessary to protect the vital interests of the data subject; or where processing is necessary for the establishment, exercise, or defense of legal claims.

155 "What Is Behavioral Biometrics?" LexisNexis; "Protecting Customer Journey With Behavioral Biometrics", LexisNexis.

Biometric technology is evolving quickly, and, as the UK ICO and others have pointed out, use cases and best practices are still emerging. Biometric applications span a wide variety of contexts and sectors, which make standard approaches to data protection difficult to implement. A one-size-fits-all approach could result in over-regulation (thereby eliminating beneficial uses) or under-regulation (which could promote infringements on individual privacy and other rights).

C. The Effect of the Rapidly Evolving Nature of Biometric Technology

Biometric technology is evolving quickly, and, as the UK ICO and others have pointed out, use cases and best practices are still emerging. Biometric applications span a wide variety of contexts and sectors, which make standard approaches to data protection difficult to implement. A one-size-fits-all approach could result in over-regulation (thereby eliminating beneficial uses) or under-regulation (which could promote infringements on individual privacy and other rights). As discussed above,[156] some biometric technologies, such as those that use one-to-one matching, can be innocuous and drive large benefits when deployed responsibly; others, such as those that have a legal or similarly significant effect on individuals, require concentrated efforts to mitigate risks, increase security, and improve transparency. As a result, CIPL notes:

- There is a need for a deeper and more informed global policy discussion on the definition and scope of biometric data and biometric technology. Where the definition of biometric data and the scope of its application are limited and precise, it will be easier to consider case-by-case implementation and facilitate compliance in a variety of use cases. If the definition and scope are broad, there will be a need to consider additional factors—such as the purpose and use of the data along with the consideration of risks, harms, and benefits.
- Understanding the intended use and purpose of biometric applications is highly relevant; it should be the foundation for any organization's privacy impact assessment and/or compliance review of biometric technology. It is also highly relevant for the policymakers and legislators who draft the laws and regulations, as the appropriateness and effectiveness of the laws will depend on the specific applications and use cases.
- Assessing potential risks and benefits is essential for organizations to ensure that biometric technologies are built with privacy, security, and safety in mind. Importantly, a risk-based framework requires a nuanced approach to regulation, creating different obligations based on the level of risk to individuals and encouraging regulators to provide appropriate guidance, oversight, and enforcement based on the level of risk.
- Transparency, purpose limitation, individual rights, and redress are crucial for building trust with end users of biometric technologies.
- Organizational accountability is critical for facilitating responsible development and deployment of biometric technology. Lawmakers and regulators should specifically endorse **demonstrable** accountability measures, given the sensitivities around the development and use of biometric technology.[157]

156 *See supra*, Section III.G

157 For more on organizational accountability, *see infra*, Section IV.B

VI. Recommendations for a Risk-Based Approach

The rapid evolution of biometric technology together with its potential challenges and opportunities requires a risk-based approach to minimize harms and realize benefits. As Daniel Solove argues, "data is what data does,"[158] and this is especially the case with technologies that rely on biometric data processing. A biometric system that relies on a large amount of biometric data stored on a single server presents very different risks from a biometric system that processes biometric data on a user's device, at the user's request, and never (or only temporarily) stores that data on an organization's server. Still, policymakers and legislators should also consider a wide range of societal considerations when addressing biometric applications. CIPL thus believes that a comprehensive approach to regulating biometric technology requires a risk-based approach that addresses three distinct prongs: (1) laws and regulations, (2) organizational practices, and (3) regulators' actions.

A. Prong One: Laws and Regulations Must Adopt a Risk-Based Approach

Generally speaking, a risk-based approach enables tailored and contextual protections against the actual risks of specific use cases. Any law or regulation must account for both possibilities—benefits and risks—without overregulating uses with minimal risks or underregulating uses with substantial risks.

Indeed, not all collection or processing of biometric data is intended for identification. For example, an autonomous vehicle may use gait recognition technology to identify whether an object is a pedestrian without identifying who that person is and without maintaining the data for any potential future identification. While gait recognition technologies can be applied to identify individuals in other settings, gait recognition technology in the autonomous vehicle context is low risk because it is used to confirm only whether an individual is present, without identifying who that individual is and without storing that data for potential future uses.

In the context of biometric data and technology, a risk-based approach enables low-risk uses, improves mitigations for higher-risk use cases, and facilitates informed decisions on whether to limit or ban high-risk applications that cannot be effectively mitigated. Ideally, risk assessments identify the potential risks of harm to individuals from proposed uses of a given technology and weigh those risks against not only the countervailing benefits to individuals and society, but also the opportunity cost of not using the technology. Of course, effective risk assessments are dependent upon a general consensus of the harms to be identified and mitigated and the benefits to be enabled. Regulatory consultations and initiatives may be needed to help build consensus and facilitate a sufficient level of legal certainty for organizations. The process of conducting robust risk assessments on biometric applications can also build consensus by identifying points of disagreement on the competing equities and creating conditions for addressing such disagreements.

158 Daniel Solove, "Data is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data" (11 January 2023).

Limited versions of the risk-based approach have been applied in existing laws and regulations, both in the context of biometric data laws as well as in privacy laws more generally. For example, by limiting the definition of biometric data for heightened compliance requirements to include only data that is intended to be used to identify an individual, the GDPR and most U.S. state privacy laws have acknowledged that uses of biometric technology for identification purposes pose a greater risk to individuals than uses not designed for identification. Indeed, not all collection or processing of biometric data is intended for identification. For example, an autonomous vehicle may use gait recognition technology to identify whether an object is a pedestrian without identifying who that person is and without maintaining the data for any potential future identification. While gait recognition technologies can be applied to identify individuals in other settings,[159] gait recognition technology in the autonomous vehicle context is low risk because it is used to confirm only whether an individual is present, without identifying who that individual is and without storing that data for potential future uses. A full-fledged and proper risk-based approach would take such considerations into account by examining each use case and identifying and assessing the risks.

CIPL recommends that laws and regulations with heightened compliance requirements should target biometric systems intended to be used to identify individuals and exclude systems not used for identification purposes. The intent requirement should consider whether developers and deployers of biometric technologies take reasonable measures (e.g., technical, organizational, and contractual) to ensure that the processing of biometric characteristics cannot be used for identifying purposes. Laws and regulations should also explicitly exclude certain types of data (e.g., photographs, video footage, audio recordings) from the definition of biometric data.

Beyond identification-related risks, a risk-based approach can also identify biometric technologies or applications that pose unique challenges to individual rights and may therefore require greater scrutiny, additional mitigation measures, or further guidance. For example, the risks attributable to the deployment of biometric technologies for identification purposes in public spaces—namely, bias, discrimination, or inaccuracy in the technology and potential misuse by law enforcement—has generated a number of sector-specific regulations, standards, and guidance papers.[160] This increased regulatory focus arises from those recognized harms.

B. Prong Two: Organizations Must Adopt a Risk-Based Approach

Importantly, a risk-based approach does not absolve organizations from responsibility or limit the legal obligations provided by law; rather, it fosters compliance.

Importantly, a risk-based approach does not absolve organizations from responsibility or limit the legal obligations provided by law; rather, it fosters compliance. It enables organizations to prioritize compliance and accountability controls and measures in areas that create high risks for individuals (and subsequently high risks for organizations). As noted in CIPL's earlier work on the risk-based approach in the context of artificial intelligence and other emerging technologies:

> The focus on impacts and risks to individuals does not diminish the obligation to comply fully with data protection law, but it can help determine the allocation of scarce resources by both organizations and regulators; it can help assure that appropriate attention is paid to those uses of data that pose greater risks; it can help justify the use of more burdensome or time-consuming mitigation processes when the potential harmful outcomes warrant it; and it can help determine the precautionary or remedial processes that should be in place.[161]

159 "How gait recognition technology can be used at a protest," Privacy International (5 May 2021); Kang "Chinese 'gait recognition' tech IDs people by how they walk," AP (6 November 2018).

160 "Biometric Standards for Law Enforcement," NIST; *see also* A Policy Framework for Responsible Limits on Facial Recognition: Use Case: Law Enforcement Investigations, World Economic Forum (November 2022).

161 Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice, Second Report: Hard Issues and Practical Solutions, CIPL (17 January 2020).

An organization's use of a risk-based assessment can justify a decision not to use biometric technology in certain settings.

An organization's use of a risk-based assessment can justify a decision not to use biometric technology in certain settings. For example, Axon, the largest U.S. provider of police body cameras, examined the consequences of deploying facial recognition technology in body-worn cameras. When an assessment showed that the potential risks of misidentification exceeded the potential benefits, the company stopped deploying the technology in that setting.[162] Alternatively, where a risk-based analysis reveals low risk or identifies mitigations and safeguards to limit risk, it can be used to justify and promote innovative and beneficial use cases.

A risk-based approach must be coupled with organizational tools, described below, to improve data governance and mitigate risks. Such tools should provide increased transparency and a means for effective redress. They should also identify alternatives to the use of biometric technologies in certain circumstances. They will require organizations to deploy of a variety of safeguards and generally promote a focus on demonstrable organizational accountability.

Providing greater transparency around the collection and use of biometric data in most contexts is a key component for building trust in biometric systems, particularly in more sensitive settings. Lack of transparency has sometimes posed challenges for building stakeholder confidence around biometric technology deployments.

1. The Role of Transparency and Consent

Providing greater transparency around the collection and use of biometric data in most contexts is a key component for building trust in biometric systems, particularly in more sensitive settings. Lack of transparency has sometimes posed challenges for building stakeholder confidence around biometric technology deployments. For example, individuals may not know or realize that biometric characteristics may be used to generate additional data, such as iris scans revealing health information. Others may not realize that photographs posted on social media could be used for facial recognition purposes. By providing greater transparency about the use of biometric systems and the collection of data, particularly when an application is high risk, organizations can mitigate potential concerns and highlight the benefits of certain use cases. Transparency about available redress mechanisms and algorithms used to promote accuracy and mitigate bias is also essential.

Transparency will differ based on the context of the biometric application, the purpose of the data collection, the storage (or deletion) of data, and the potential impact on individuals. Transparency notices may include information about the types of data collected and the purpose or use of such data. They may also provide information about individual rights (like the right to opt-out) and redress options. While context-dependent, transparency can help build trust in an emerging field.

2. The Importance of Redress or Alternatives to the Use of Biometric Systems

As with uses of other emerging technologies, organizations developing or deploying biometric technologies should consider how to provide effective and proportionate avenues of redress for individuals claiming to be harmed. Redress allows individuals "to contest and change an outcome they believe is inaccurate, unfair, or otherwise inappropriate."[163] Avenues of redress should be clearly noted for individuals, as they may not always be readily apparent.

Additionally, organizations should consider whether and how to provide reasonable alternatives to individuals who do not want to or cannot use certain biometric applications. Indeed, providing such alternatives may also be part of effective redress. For example, if facial recognition technology prevents a passenger from boarding an airplane, the passenger should be able to provide another form of identification for human review. Similarly, where patrons of Disney's amusement parks choose

162 First Report of the Axon AI & Policing Technology Ethics Board, Axon AI and Policing Technology Ethics Board (June 2019).

163 Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice, Second Report: Hard Issues and Practical Solutions, CIPL (17 January 2020) at p. 22.

not to use Disney's biometric-based "Ticket Tag" service,[164] Disney provides patrons with the option of showing a photo ID that matches the name on their park ticket.[165] Importantly, individuals who chose to opt-out of biometric collection should be able to do so freely and without explanation or difficulty in most circumstances. At the same time, opt-outs should not be permitted in certain contexts (such as low-risk biometric data processing that is used for fraud prevention or know-your-customer purposes).

3. The Need for Safeguards

The sensitive and unique nature of some biometric data necessitates robust organizational and security controls, particularly when biometric identifiers are collected and stored in a way that can identify individuals. For starters, organizations should document the origin and purpose of biometric data collection (i.e., data provenance) and maintain their documentation. When organizations process biometric data, they should also consider the appropriate technical, physical, and organizational safeguards to protect that data from unauthorized access or theft. This could include the storage of numerical identifiers rather than biometric data, as in the example of the Disney Parks, mentioned above.[166]

Organizations that rely on biometric technology for secure verification can, in some cases, deploy privacy enhancing technologies (such as trusted execution environments) at the hardware level of the end-user.

It could also entail robust security measures and state-of-the-art encryption with strong access controls. Organizations that rely on biometric technology for secure verification can, in some cases, deploy privacy enhancing technologies (such as trusted execution environments) at the hardware level of the end-user. As an example, Apple allows iPhone users to unlock their devices with face or finger biometric data. The user-provided biometric data required for these functions is not processed on Apple servers; rather, it is processed locally, on the user's device, in a trusted executive environment that Apple calls a "Secure Enclave."[167] The Secure Enclave temporarily stores biometric data for processing purposes and then discards it.

Promoting a risk-based approach to the deployment of biometric technologies goes hand-in-hand with demonstrable organizational accountability. CIPL's work on organizational accountability in the context of to data protection, privacy, and AI is equally relevant in the context of biometric technology.

As discussed above, a risk assessment[168] is an important tool for determining which safeguards are necessary and appropriate. An assessment evaluates the risk-level of a given technology or data use and helps identify controls and mitigation measures to address these risks.

Government-led standards initiatives can also help promote safeguards and bolster public trust regarding biometric applications. For example, the UK's Digital Identity and Attributes Trust Framework (DIATF) is a certification scheme, currently in the beta stage, that aims to facilitate trust between users, purchasers, and developers of digital identity solutions.[169] Such standards and certifications signal to the public that their information is protected, and they allow businesses to make informed choices regarding vendors, especially when overseen by a regulator (as is the case with the UK DIATF).

164 Ticket Tag, used at the entrance of Disney theme parks and water parks to facilitate ease of re-entry, takes an image of a patron's finger, converts the image into a unique numerical value, and immediately discards the image.

165 "Privacy At The Walt Disney World Resort, The Disneyland Resort, And Aulani, A Disney Resort & Spa: Frequently Asked Questions," Walt Disney Company.

166 *Id.*

167 Apple, "Face ID and Touch ID security", 18 February 2021.

168 Also known as data protection impact assessments (DPIAs) or privacy impact assessments (PIAs).

169 Policy Paper, "UK digital identity and attributes trust framework", Department for Science, Innovation and Technology and Department for Digital Culture, Media & Sport.

4. A Focus on Accountability: The CIPL Accountability Framework

Promoting a risk-based approach to the deployment of biometric technologies goes hand-in-hand with demonstrable organizational accountability. CIPL's work on organizational accountability in the context of to data protection, privacy, and AI is equally relevant in the context of biometric technology. The seven elements of CIPL's Accountability Framework—Leadership and Oversight; Risk Assessment; Policies and Procedures; Transparency; Training and Awareness; Monitoring and Verification; and Response and Enforcement—are designed to ensure a holistic approach to organizational practices and compliance measures.[170] The framework assesses whether an organization's practices are sufficiently comprehensive and whether new governance programs should be developed.[171]

Figure 1: CIPL Accountability Framework – Universal Elements of Accountability

170 The Case for Accountability: How It Enables Effective Data Protection and Trust in the Digital Society, CIPL (23 July 2018).

171 What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework, CIPL (May 2020). Please also note that, in the context of the use of facial recognition by law enforcement, there are other proposed frameworks for acceptable uses and limitations – *see* Model Face Recognition Use Policy proposed by Georgetown Law scholars Clare Garvie, Alvaro Bedoya, Jonathan Frankle.

C. Prong Three: Regulators Must Adopt a Risk-Based Approach

Lastly, a risk-based approach requires regulators to perform their duties—guidance, oversight, and enforcement—based on risk.

Risk-based laws and regulations require up-to-date regulatory guidance, especially for emerging technologies and "high-risk" biometric applications. Regulatory guidance should specify categories, types, and examples of harm to be considered in impact assessments. Importantly, guidance should consider not only the architecture of the technology, but the user as well. Specifically: Is the biometric system undisclosed or user-initiated? What is the relationship of the user to the system? What is the purpose of processing?

Designation of uses as high-risk should be rebuttable in order to:

- enable organizations to take account of the highly contextual nature of biometric applications, and
- give them the opportunity to demonstrate that the use of a specific biometric application does not present a high risk.

Further, regulator-endorsed certifications and codes of conduct can play an especially important role in promoting accountable and trustworthy biometric systems. Both certifications and codes of conduct help facilitate compliance. To encourage voluntary participation by organizations, participation in either kind of framework with appropriate safeguards should play a mitigating role in regulatory enforcement actions.

CIPL recognizes the need for organizations to share information proactively with regulators about biometric technology advancements and cutting-edge research, especially when emerging practices can mitigate known harms and risks and facilitate beneficial uses. CIPL further believes that regulators play an important role in encouraging such engagement. Regulatory sandboxes—which promote regulatory feedback and involvement—help ensure responsible and accountable development and use of biometric technology. Sandboxes enable trustworthy uses of new technologies and should be encouraged for large-scale, critical, public and private sector deployment, especially in its early stages.[172]

172 ICO, Regulatory Sandbox Final Report: Onfido (September 2020).

VII. Conclusion

Biometric technologies carry varying risks and yet are deployed responsibly in many sectors and contexts with individual privacy and security in mind. As law and policymakers develop regulatory frameworks for these rapidly evolving technologies, stakeholders should understand and be able to distinguish the principal applications of biometric systems—i.e., recognition, verification, and classification—as well as the different levels of risk and benefits associated with each particular use case. A risk-based approach is indispensable for navigating these differences and delivering the right outcomes. Importantly, the definition of biometric data triggering heightened compliance requirements should target data that is used to identify individuals and should exclude data that will not be used for identification purposes. Further, any regulatory framework for biometric technology should enable and require organizations to locate their specific use cases on a risk-benefits matrix and implement necessary and appropriate mitigations.

In sum, appropriate regulation does not address whether biometric technology, in general, should be deployed or prohibited. Rather, it addresses whether a specific use can be justified by its benefits versus the residual risk of harm after applying targeted mitigations. As biometric technologies advance, so, too, will potential mitigations. A risk-based approach will provide a future-proof solution that avoids both over-regulation (i.e., preventing low-risk uses that benefit society) and under-regulation (i.e., permitting uses with an unacceptably high level of risk).

Appendix A

Biometric Data Legal Definitions

The tables on the following pages highlight how biometric data, biometric identifier, or biometric information are defined in the European Union and by various state-level laws throughout the US.

TABLE 1: Targeted Biometric Data Laws

Jurisdiction	Law	Definitions	Source
Illinois, USA	Biometric Information Privacy Act (BIPA)	**"Biometric identifier"** means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.	740 ILCS 14/10
Illinois, USA	Biometric Information Privacy Act (BIPA)	**"Biometric information"** means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier **used to identify an individual**. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.	740 ILCS 14/10
Washington, USA	Washington State Biometric Identifiers	"Biometric identifier" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is **used to identify a specific individual**. "Biometric identifier" does not include a physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996.	Wash. Rev. Code 19.375.010 (1)

TABLE 2: Comprehensive Personal Data Privacy Laws

Jurisdiction	Law	Key Definitions	Source	Is biometric data "sesitive data"?
European Union	General Data Protection Law (GDPR)	"Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, **which allow or confirm** the unique identification of that natural person, such as facial images or dactyloscopic data	GDPR Article 4(14)	Yes. Under the GDPR, the "processing of biometric data for the purpose of uniquely identifying a natural person" is generally prohibited unless the processing falls into one of ten specified categories. See Article 9, GDPR.
California, USA	California Consumer Privacy Act (CCPA)	"Biometric information" means an individual's physiological, biological or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), **that is used or is intended to be used, singly or in combination with each other or with other identifying data, to establish individual identity.** Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.	Cal. Civ. Code § 1798.140(c)	Yes. "Sensitive personal information" includes, "the processing of biometric information **for the purpose** of uniquely identifying a consumer."
Colorado, USA	Colorado Privacy Act Rules (Code of Colorado Regulations)	"Biometric Data" as referred to in C.R.S. § 6-1-1303(24)(b) means Biometric Identifiers that are **used or intended to be used, singly or in combination with each other or with other Personal Data, for identification purposes.** Unless such data is used for identification purposes, "Biometric Data" does not include (a) a digital or physical photograph, (b) an audio or voice recording, or (c) any data generated from a digital or physical photograph or an audio or video recording.	4 CCR 904-3-2.02	Yes. "Sensitive data" includes, "genetic or biometric data **that may be** processed **for the purpose** of uniquely identifying an individual."
Colorado, USA	Colorado Privacy Act Rules (Code of Colorado Regulations)	"Biometric Identifiers" means data generated by the technological processing, measurement, or analysis of an individual's biological, physical, or behavioral **characteristics that can be processed for the purpose of uniquely identifying an individual**, including but not limited to a fingerprint, a voiceprint, scans or records of eye retinas or irises, facial mapping, facial geometry, facial templates, or other unique biological, physical, or behavioral patterns or characteristics.	4 CCR 904-3-2.02	*Id.*

Jurisdiction	Law	Key Definitions	Source	Is biometric data "sesitive data"?
Connecticut, USA	Connecticut Data Privacy Act	"Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics **that are used to identify a specific individual.** "Biometric data" does not include (a) a digital or physical photograph, (b) an audio or video recording, or (c) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.	Conn. Gen. Stat. § 42-515(3)	Yes. "Sensitive data" includes, "the processing of genetic or biometric data **for the purpose** of uniquely identifying an individual."
Delaware, USA	Delaware Personal Data Privacy Act (DPDPA)	"Biometric data" means data generated by automatic measurements of an individual's unique biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics **that are used** to identify a specific individual. "Biometric data" does not include any of the following: (a) a digital or physical photograph (b) an audio or video recording, (c) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.	6 Del. C. § 12d-102 (3)	Yes. "Sensitive data" includes, "genetic or biometric data."
Florida, USA	Florida Digital Bill of Rights (effective July 1, 2024)	"Biometric data" means data generated by automatic measurements of an individual's biological characteristics. The term includes fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or characteristics **used to** identify a specific individual. The term does not include physical or digital photographs, video or audio recordings or data generated from video or audio recordings, or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.	Fla. Stat. § 501.702(4)	Yes. "Sensitive data" includes, "genetic or biometric data processed for the purpose of uniquely identifying an individual."
Indiana, USA	Indiana Consumer Data Protection Act (effective Jan. 1, 2026)	"Biometric data"" means data that: (a) is generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, images of the retina or iris, or other unique biological patterns or characteristics; and (b) is used to identify a specific individual. The term does not include: (a) a physical or digital photograph, or data generated from a physical or digital photograph; (b) a video or audio recording, or data generated from a video or audio recording; or (c) information collected, used, or stored for health care treatment, payment, or operations under HIPAA.	Indiana Code § 24-15-2-4	Yes. "Sensitive data" includes, "genetic or biometric data that is processed **for the purpose** of uniquely identifying a specific individual."

Jurisdiction	Law	Key Definitions	Source	Is biometric data "sesitive data"?
Iowa, USA	An Act Relating to Consumer Data Protection (effective Jan. 1, 2025)	Biometric data - means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is **used to identify a specific individual**. Biometric data does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment or operations under HIPAA.	Iowa Code § 715D.1(4)	Yes. "Sensitive data" includes, "genetic or biometric data that is processed **for the purpose** of uniquely identifying a natural person."
Montana, USA	Montana Consumer Data Privacy Act (effective Oct. 1, 2024)	"Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are **used to identify a specific individual**. The term does not include: (i) a digital or physical photograph; (ii) an audio or video recording; or (iii) any data generated from a digital or physical photograph or an audio or video recording, unless that data is generated to identify a specific individual.	Mont. Code § 30-14-2802(3)	Yes. "Sensitive data" includes, "the processing of genetic or biometric data **for the purpose** of uniquely identifying an individual."
New Hampshire, USA	Senate Bill 255 (signed March 6, 2024; effective Jan. 1, 2025)	"Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns, or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.	N.H. Rev. Stat. Ann. § 507-H:1(IV)	Yes. "Sensitive data" means personal data that includes data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status; the processing of genetic or biometric data **for the purpose** of uniquely identifying an individual; personal data collected from a known child; or, precise geolocation data.
New Jersey, USA	Senate Bill 332 (signed Jan. 16, 2024; effective Jan. 16, 2025)	"Biometric data" means data generated by automatic or technological processing, measurements, or analysis of an individual's biological, physical, or behavioral characteristics, including, but not limited to, fingerprint, voiceprint, eye retinas, irises, facial mapping, facial geometry, facial templates, or other unique biological, physical, or behavioral patterns or characteristics **that are used or intended to be used**, singularly or in combination with each other or with other personal data, to identify a specific individual. "Biometric data" shall not include: a digital or physical photograph; an audio or video recording; or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.	NJ P.L. 2023, c.266	Yes. "Sensitive data" includes, "genetic or biometric data that may be processed **for the purpose** of uniquely identifying an individual."

Jurisdiction	Law	Key Definitions	Source	Is biometric data "sesitive data"?
Oregon, USA	Oregon Consumer Privacy Act (OCPA)	"Biometric data" means personal data generated by automatic measurements of a consumer's biological characteristics, such as the consumer's fingerprint, voiceprint, retinal pattern, iris pattern, gait or other unique biological characteristics **that allow or confirm** the unique identification of the consumer. "Biometric data" does not include: (a) a photograph recorded digitally or otherwise; (b) an audio or video recording; (c) data from a photograph or from an audio or video recording, unless the data were generated for the purpose of identifying a specific consumer or were used to identify a particular consumer; or (d) facial mapping or facial geometry, unless the facial mapping or facial geometry was generated f**or the purpose** of identifying a specific consumer or was **used to** identify a specific consumer.	Or. Rev. Stat. § 646A.570(3)	Yes. "Sensitive data" includes, "genetic or biometric data."
Tennessee, USA	Tennessee Information Privacy Act (effective July 1, 2025)	"Biometric data" (a) means data generated by automatic measurement of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retina or iris, or other unique biological patterns or characteristics that are **used to identify a specific individual**; and (b) Does not include a physical or digital photograph, video recording, or audio recording or data generated from a photograph or video or audio recording; or information collected, used, or stored for healthcare treatment, payment, or operations under HIPAA;	Tenn. Code Ann. § 47-18-3302(3)	Yes. "Sensitive data" includes, "the processing of genetic or biometric data **for the purpose** of uniquely identifying a natural person."
Texas, USA	Texas Data Privacy and Security Act (effective July 1, 2024)	"Biometric data" means data generated by automatic measurements of an individual's biological characteristics. The term includes a fingerprint, voiceprint, eye retina or iris, or other unique biological pattern or characteristic that is **used to identify a specific individual**. The term does not include a physical or digital photograph or data generated from a physical or digital photograph, a video or audio recording or data generated from a video or audio recording, or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).	Tex. Bus. & Com. Code § 541.001.(3)	Yes. "Sensitive data" includes, "genetic or biometric data that is processed **for the purpose** of uniquely identifying an individual."

Jurisdiction	Law	Key Definitions	Source	Is biometric data "sesitive data"?
Utah, USA	Utah Consumer Privacy Act	"Biometric data" means data generated by automatic measurements of an individual's unique biological characteristics. "Biometric data" includes data described in Subsection (6)(a) that are generated by automatic measurements of an individual's fingerprint, voiceprint, eye retinas, irises, or any other unique biological pattern or characteristic **that is used to** identify a specific individual. "Biometric data" does not include: (i) a physical or digital photograph; (ii) a video or audio recording; (iii) data generated from an item described in Subsection (6)(c)(i) or (ii); (iv) information captured from a patient in a health care setting; or (v) information collected, used, or stored for treatment, payment, or health care	Utah Code § 13-61-101(6)	Yes. "Sensitive data" includes, "the processing of genetic personal data or biometric data, if the processing is **for the purpose** of identifying a specific individual."
Virginia, USA	Virginia Consumer Data Protection Act	"Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is **used to identify a specific individual**. "Biometric data" does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.	Va. Code § 59.1-575	Yes. "Sensitive data" includes, "the processing of genetic or biometric data **for the purpose** of uniquely identifying a natural person."
Washington, USA	My Health My Data Act	"Biometric data" means data that is generated from the measurement or technological processing of an individual's physiological, biological, or behavioral characteristics and **that identifies a consumer, whether individually or in combination with other data**. Biometric data includes, but is not limited to: (a) Imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted; or (b) Keystroke patterns or rhythms and gait patterns or rhythms that contain identifying information.	Wash. Rev. Code § 19.373.010(4)	N/A
Washington, USA	My Health My Data Act	"Consumer health data" means personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status. For the purposes of this definition, physical or mental health status includes, but is not limited to:...(ix) Biometric data;...	Wash. Rev. Code § 19.373.010(8)(a)	N/A

Appendix B:

Applications and Examples of Biometric Technology Deployment

While not exhaustive, the list below demonstrates the wide breadth of biometric applications and the potential associated benefits and risks.

1. Law Enforcement

There are multiple uses for biometric data in the law enforcement and criminal investigations context. One of the earliest applications of biometric technology was in New York state prisons, where fingerprints were first used in 1903 for authentication.[173] Police in the United Kingdom and France began using fingerprints around the same time.[174] Biometric technologies have since become a core technology used for security purposes for criminal investigations, border management, and national security.

Today, criminal investigations often rely on databases that process biometric data to identify suspected criminals based on previously stored templates. Use of biometric technology in such contexts has expanded from fingerprinting to include newer technologies such as DNA, facial recognition, iris recognition, retina scan, voiceprint, and hand geometry.[175] Many uses of biometric technology are post-event—or searching for an identity after an event has occurred. A 2022 World Economic Forum Report detailed various post-event use cases for facial recognition technologies in conjunction with the Netherlands Police. These applications included: identifying an ATM fraud criminal using video footage from the ATM machine; identifying an assailant of police officers during a riot using CCTV footage; searching for the identity of a museum thief; or fighting child abuse or finding missing persons using facial recognition.[176]

In the US, this post-event application of biometric technology often involves one of two types of databases. The Automated Fingerprint Identification System (AFIS) stores a database of fingerprint images for searching and matching.[177] More recently, federal law enforcement established an Automated Biometric Identification System (ABIS) that stores biometric data in templates for face, finger, and iris.[178] These applications generally work by comparing a biometric sample from an unknown individual against a database of stored biometric templates to identify suspects or persons of interest in law enforcement investigations. There are many AFIS and ABIS databases globally with different owners who maintain and employ the systems. For example, in the US, the Federal Bureau of Investigation maintains the federal AFIS, while the EU has its own called the Eurodac.[179]

A more sensitive application in law enforcement involves the real-time deployment of facial recognition technology. One can imagine important uses for such deployments, such as actively looking for a terrorist or an active shooter in a public space.

173 Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?, University of Minnesota Human Rights Center (2022) at p. 5.

174 *Id.*

175 US Department of Justice, Global Justice Information Sharing Initiative, "Privacy and Information Quality Risks: Justice Agency Use of Biometrics".

176 A Policy Framework for Responsible Limits on Facial Recognition: Use Case: Law Enforcement Investigations, World Economic Forum (November 2022), p. 15-17.

177 "Automated Fingerprint Identification System (AFIS) overview - A short history." Thales (27 January 2022).

178 *Id.*

179 "Eurodac," European Commission Migration and Home Affairs,

Real-time comparison against databases and communication with police forces may help generate leads and contribute to public safety. While real-time application is limited within law enforcement today,[180] there are already numerous examples of both beneficial and harmful applications, which has sparked intense debate and created heightened media and public attention. There is a great potential for inaccuracies in biometric systems to further pre-existing biases and impose tangible harm for marginalized individuals and communities (e.g., wrongful arrests, over-surveillance or policing, etc.). Because such effects of systemic bias have already been documented,[181] it is imperative to consider such risks in developing, deploying, and regulating biometric systems.

2. Public Security

Another common use of biometric technology is to ensure public security in a variety of settings, such as airports, event security, or security in other large public areas. In some cases, biometric technologies are used for the convenience of easy authentication by eliminating the need for other manual identification measures, such as checking physical IDs, asking verification questions, and more.

Airport Security: The US Transportation Security Administration (TSA) uses facial recognition to improve airport operations and security by increasing the accuracy of passenger authentication.[182] TSA describes the system as "opt-in" but some observers have criticized its implementation as unduly burdening travelers who opt out.[183] Apple has also developed a digital ID, approved by TSA, to enable more seamless airport experiences and aid in identity verification when going through security checkpoints. This technology processes biometric data—Face ID or Touch ID—to unlock and access the digital ID, which is then used in the same way as a driver's license.[184]

Event security: Biometric technology is increasingly being used to monitor operations at stadiums and other venues. More than one million attendees of the 2022 World Cup were monitored by over 15,000 cameras.[185] Some stadiums have used biometric applications to identify previously banned fans, identify suspected criminals, and monitor fan activity.[186] In November 2021, the top professional soccer league in Mexico announced the deployment of facial recognition for all stadiums in the country to create safer environments for fans, reduce recent violence at major events, and create a more efficient experience across the stadium.[187] To highlight a more harmful example, MSG Entertainment (owner of Madison Square Garden and Radio City Hall) was recently under scrutiny for potentially violating anti-discrimination laws by employing facial recognition technology to recognize and bar lawyers from its venues if they work for firms suing the company.[188] Concern over the deployment of real-time facial recognition technologies has led to the decision to have AI-powered cameras at the 2024 Olympics in France, but not facial recognition.[189]

Age verification: Biometric technology can estimate an individual's age simply by scanning the face and without any additional paperwork or documentation. This can help control access to certain services or digital tools based on child safety laws. Without biometric technology, many companies may have to collect, store, and secure sensitive government identification documents at a large scale and doing so carries significant risks to the privacy and safety of users.

180 A Policy Framework for Responsible Limits on Facial Recognition: Use Case: Law Enforcement Investigations, World Economic Forum (November 2022), at p. 17.

181 Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," Conference on fairness, accountability and transparency: PMLR, 2018.

182 "Biometrics Technology," US Transportation Security Admin.

183 "TSA's Opt-in Facial Recognition Program Doesn't Seem All That Optional in Real Life," TechDirt, January 4, 2023.

184 Zach Griff, "Apple's TSA-approved digital ID is now live in 2 states, coming soon to many more," The Points Guy (25 May 2022).

185 Vas Panagiotopoulos, "Soccer Fans, You're Being Watched," WIRED (3 November 2022).

186 *Id.*

187 "Soccer stadiums in Mexico add biometrics to ticketing process," Security Magazine (21 November 2022).

188 Karen Matthews, "New York's AG says MSG lawyer ban may violate anti-bias laws," ABC News.

189 Kayali, "French privacy chief warns against using facial recognition for 2024 Olympics," POLITICO (24 January 2023).

3. Border Security

The US Customs and Border Protection (CBP) agency has deployed various biometric solutions to improve processes to enable border security. For example, CBP partnerships have deployed facial biometric technologies at all international airports in the US, 26 seaports, and all pedestrian lanes at northern and southwest border ports of entry.[190] The system is more than 98% accurate in authenticating travelers' identities; has processed more than 196 million travelers; and has prevented more than 1,500 individuals from illegally entering the country.[191]

4. Military Checkpoints

A controversial example of biometric technology is in the Israeli-occupied West Bank, where facial recognition technology has been incorporated at West Bank military checkpoints into Israel.[192] While Israel has argued that the screening is needed for security reasons as well as greater speed and efficiency in passing through checkpoints, many Palestinians and civil liberties advocates have sharply criticized it and other biometric data-based surveillance in the Occupied Territories as harmful and invasive.[193]

5. Airport Efficiency and Convenience

Although many deployments of biometric technology at airports and events are designed to ensure security, other uses are designed to increase efficiency and passenger convenience. According to a 2021 survey from the International Air Transport Association, 73% of airline passengers were willing to share biometric data for the purpose of improving airport experiences, up more than 25% from the 2019 survey.[194] Given the advancements in biometric technologies as well as the increasing favorability with passengers, there are a multitude of examples of biometric technology used to increase airport efficiency and convenience. Those listed below are only a small subset of these use cases:

CLEAR[195] uses biometric characteristics—irises and facial recognition—to authenticate individuals for easier entry through security at airports and major stadium venues in the US.[196] CLEAR has other applications for user convenience, including age verification for ordering alcoholic beverages and authenticating users when checking into hotels.[197]

Many airlines have tested or currently use biometric applications to enable more seamless boarding experiences. For example, Delta Airlines uses biometric technology for this purpose at certain airports in the US. Passengers can opt in to this service for their convenience and bypass the passport check otherwise required by the US government. Biometric data is not saved or stored by Delta and the images are discarded within 12 hours. [198] Other airlines—including American, United, and Spirit—have tested or implemented similar solutions. Studies have shown that biometric boarding processes can board 400 people in approximately 20 minutes, which is nearly half the time required for conventional boarding.[199]

Another emerging use of biometric technology at airports is checking luggage. In November 2021, Delta launched a partnership with TSA PreCheck to use biometric technology, and facial recognition specifically, for smooth bag checking, security screening, and boarding.[200] The goal is to require only 30 seconds for dropping off a bag at baggage claim.[201]

190 "Say hello to the new face of speed, security and safety Introducing Biometric Facial Comparison," US Customs and Border Protection.

191 *Id.*

192 Estrin, "Face Recognition Lets Palestinians Cross Israeli Checkposts Fast, But Raises Concerns," NPR (22 August 2019).

193 Elizabeth Dwoskin, "Israel escalates surveillance of Palestinians with facial recognition program in West Bank" The Washington Post, November 8, 2021.

194 Elaine Glusac, "Your Face Is, or Will Be, Your Boarding Pass," NY Times (11 January 2022).

195 CLEAR is a membership-based service often found in stadiums and airports that utilizes biometric technology to allow users to pass through security fasters faster.

196 "HOW IT WORKS: Stress-Free Airport Security Nationwide," CLEAR.

197 "BUSINESS & PARTNERSHIPS: One Platform, Countless Solutions," CLEAR.

198 "5 things to know about biometrics and Delta," Delta News Hub (6 January 2020).

199 Elaine Glusac, "Your Face Is, or Will Be, Your Boarding Pass," NY Times (11 January 2022).

200 *Id.*

201 Frederic Lardinois, "Delta Air Lines partners with TSA PreCheck to launch biometrics-based bag drops," TechCrunch (27 October 2021).

6. Device Security

Device security and access is perhaps the most commonly recognized use of biometric technology, as most smart phones are equipped with authentication settings that can enable fingerprint or facial recognition of the owner. Many phones, laptops, and other connected devices use biometric identifiers to improve device security. These are typically opt-in mechanisms that allow a user to unlock a device, directly log in to or access passwords for apps or files, make purchases using Apple Pay, Google Pay, or other virtual wallets. Home devices such as Google Home, Alexa devices, and Siri devices utilize voice recognition to verify authorized users. The use of biometric technologies has become a common practice to help secure mobile, personal, home, and work devices, while also providing convenient access mechanisms for the device owner.

7. Enterprise Security

Biometric and facial recognition technologies can help organizations improve access controls for facilities, networks, and devices. These applications support user authentication and role-based access controls to improve the security of building and network perimeters. This can support cyber resilience for organizations by adding a layer of protection against security breaches and unauthorized access. Biometric technologies have also been deployed to mitigate some of the risks inherent in the rise of remote work by enhancing authentication protocols for remote devices; on-premises security can be fortified against theft or loss of traditional access cards through the use of biometric access devices.[202]

8. Banking and Financial Services

The financial services sector has adopted biometric technologies for a number of applications to improve account and transaction security, identify and prevent fraud, and enhance customer experience.

In Japan, Seven Bank is using facial recognition on a trial basis to authenticate ATM users and ensure authorized use of the card by matching it to the owner.[203]

Many banks now require multi-factor authentication for access to online or mobile accounts. According to one source, over 90 percent of consumers prefer using biometric systems over traditional passwords because it takes less time than entering traditional passwords and feels more secure.[204]

Banks are increasingly using biometric technologies to secure building access and improve identity management of employees.

Companies in financial services are using biometric technologies to drive innovation in fraud prevention. For example, Mastercard's Biometric Card uses fingerprint technology combined with existing chip technology to, in their own words, "conveniently and safely verify the cardholder's identity for in-store purchases."[205] The card's sensor authenticates identity through a fingerprint at the time of transaction to limit fraudulent use. Another example of this is Onfido, a technology company that helps businesses verify customer identities by matching a photo-based identity document (e.g., driver's license) to a biometric verification (e.g., selfie photo or live video).[206]

202 Maria Pihlström, "Biometrics: Unlocking next-gen enterprise security," Security Magazine (2 November 2021).

203 "The Top 9 Common Uses of Biometrics in Everyday Life," NEC New Zealand (7 July 2020).

204 "9 Industries Biometrics Technology Could Transform," CBInsights (12 December 2019).

205 "MASTERCARD® BIOMETRIC CARD: Driving cardholder security and convenience," Mastercard.

206 Lubna Takuri, "Guide to identity proofing: what it is and why it matters," Onfido (10 February 2023).

9. Workplace Monitoring and Safety

While biometric technologies have assisted in enterprise security and employee identity management, they have also created opportunities for employers to increase workplace monitoring.[207]

Employers have implemented facial recognition time clocks to authenticate employees, simplify the process of clocking in, and limit time fraud.[208]

Biometric technologies can be implemented at point-of-sale systems, such as requiring employee fingerprints, to detect fraud or inappropriate access, which creates a more accurate audit log of registers.

To improve employee safety during the pandemic, some employers introduced thermal imaging for employees as they walked into the workplace, which collected temperature data to detect whether an employee had a higher temperature than the recommended parameters.[209]

Employers also have the ability to monitor productivity, emotion, or attitude at work. For example, McDonald's reportedly trialed applications of facial recognition in Japan to assess customer service, including analysis of whether employees are smiling when assisting customers.[210] This application of biometric technologies can be used in retail, restaurants, and a number of customer-facing industries, although concerns have been raised about risks related to employee privacy and autonomy.

The variety of applications in the workplace have important benefits for organizations, but it is important to have transparency about the collection and use of such data, limitations on the further use of such data beyond its initial purpose, and avenues of redress available to offset concerns about employee surveillance or infringement on employee privacy. Employers will also need to also consider potential applicability of obligations under statutes such as the California Consumer Privacy Act (CCPA), which explicitly applies to employment data.[211] In many jurisdictions, labor law will impose additional restrictions on the use of the technology to monitor employees.

10. Marketing and Customer Experience

Whether in food and beverage, hospitality, or retail, biometric technologies have the potential to improve the financial transaction experience, improve in-store advertisements and promotions, and limit theft. The examples below are only a small sample of use cases in this context.

Coca-Cola has deployed facial recognition in numerous settings around the globe, including rewarding customers who recycle in China or delivering personalized ads at vending machines to increase drink sales in Australia.[212]

Many locations for AmazonGo, Amazon's brick and mortar stores equipped with "Just Walk Out" technology, allow customers to use palm prints to pay.[213] Computer vision is used to create a palm signature, which is connected to financial and account information. This aids in customer convenience and enables more personalized offers and recommendations for future interactions.

Many online retailers, such as MAC (a cosmetic brand) or EyeBuyDirect (an online retailer for eyeglasses), allow users to virtually try on products using augmented reality and facial recognition features. This allows consumers to have a better idea of whether the product will work for them and decreases the likelihood of returns when shopping which in turn has a positive environmental impact.

207 Ifeoma Ajunwa, The Quantified Worker: Law and Technology in the Modern Workplace (2023).

208 Henry Kronk, "Facial Recognition Technology in the Workplace: Employers Use It, Workers Hate It, Regulation Is Coming for It," Corporate Compliance Insights (3 March 2021).

209 "The Benefits of Biometric Technology for Workplace Safety," Work Health Solutions.

210 "What is Facial Recognition – Definition and Explanation," Kaspersky Lab; *see also* Megan Gates, "What McDonald's Approach to Biometrics says About the Future of Restaurants," ASIS International (December 2015).

211 California Consumer Privacy Act FAQs, updated February 15, 2023.

212 Alex Heber, "Coca-Cola Is Using Face-Recognition Technology On Vending Machines In Australia To Sell More Drinks," Business Insider (1 May 2014).

213 Sarah Perez, "Amazon expands its biometric-based Amazon One palm reader system to more retail stores," TechCrunch (1 February 2021).

Facial recognition is increasingly used in the hospitality industry to improve customer experience, provide seamless check-in and check-out processes, and deliver personalized recommendations.

Face scanning and emotion recognition allow companies to track user responses to advertisements or capture initial reactions to products in focus groups to improve market research, although these systems have been criticized for accuracy problems and not always being attuned to differences across cultures.[214]

11. Transportation and Logistics

Biometric authentication and tracking technologies in the transportation industry are being deployed to reduce theft and loss of shipments. According to the US Department of Justice in 2020, common cargo theft and lost shipment losses are estimated at $1 million a day.[215] Biometric systems are one potential technological solution for convenient authentication of drivers or carriers, enabling an accurate log of who took the cargo and ensuring that only authenticated individuals have access to facilities.[216]

12. Automotive Industry

The automotive industry also commonly makes use of biometric technologies, often for driver or pedestrian safety, or in security applications. Biometric technology, such as fingerprint and facial recognition, are increasingly used to unlock and start a vehicle without a key or key fob.[217] Another feature on the rise is driver monitoring software based on biometric data where cameras and sensors are used to monitor driver alertness. This may reduce accidents caused by distracted, tired, or drunk drivers, but can also have the potential to infringe on privacy since the data can be used for secondary purposes or reported to insurance companies. Some manufacturers have used biometric technology to promote convenience for the driver, identifying who is driving and automatically adjusting presets such as seat location, mirror positions, or radio stations.[218] A research team in University of Pennsylvania has also used individual biometric data from cyclists such as eye-tracking to study human behavior and create designs for safer roadways for cyclists and pedestrians.[219] These innovations, along with others in the space of biometric technology and autonomous vehicles, are still being explored and developed, but have potentially promising benefits.

13. Healthcare

The healthcare industry can benefit from biometric applications in numerous ways: identifying patients in emergency situations, preventing prescription or health insurance fraud, authenticating patients and authorizing payments, protecting patient files with biometric-enabled audit logs, and advancing telemedicine with fingerprint or voice authentication, emotion recognition for care, and security of patient records. Biometric applications can also be implemented in hospitals for building security, seamless employee logins, reduction of administrative tasks (such as patient sign-in). Many organizations have also explored the possibility of using biometric technology to replace current patient-matching approaches and more easily and accurately link health records across multiple healthcare providers or jurisdictions.[220]

214 Kate Crawford, "Artificial Intelligence is Misreading Human Emotion," The Atlantic, April 27, 2021.

215 "1332. Charging Theft from Interstate Shipment – Dollar Thresholds, Local Efforts," US Department of Justice Archives (17 January 2020).

216 Sivaranjith Sivaraman, "4 Futuristic Applications of Biometric Technology in Logistics," Mantra Softech (2 March 2022).

217 *See* Joann Muller, "You can unlock Genesis' new electric SUV just like an iPhone," Axios (14 October 2022); Jim Nash, "Ford's biometric sentry for people, critters inside and outside car is awarded patent," Biometric Update (24 February 2022).

218 Keith Barry, "How Driver Monitoring Systems Can Protect Drivers and Their Privacy," Consumer Reports (17 February 2022).

219 Ericka Brockmeier, "A new metric for designing safer streets," Penn Today (19 July 2021).

220 "Health Care Can Learn From Global Use of Biometrics: Examples from other industries could offer lessons for linking patient medical records," Pew Charitable Trusts (19 November 2020).

Innovations in wearable technology also process biometric data to collect patient data and continuously help improve patient outcomes by giving their doctors a more holistic picture of how certain treatments are working or how diseases might be progressing. Ongoing clinical trials are assessing the use of biometric monitoring devices for patients in various settings (e.g., diabetes patients using continuous glucose monitoring devices or oncology and neurology patients measuring physical activity or sleep quality).[221]

14. Health and Fitness

Wearables do not just find application in direct healthcare settings, but also in the health and fitness industry. The prevalence of wearables, such as Fitbit, Apple Watches, or Oura Rings, has increased in recent years for users ranging from beginners in health and fitness to advanced users such as elite athletes. These trackers can help individuals measure a number of health metrics, including step count, active hours, calories burned, pulse, sleep quality, temperature, or blood pressure. Wearables provide benefits in numerous contexts: users have a better understanding of their overall health habits, which can improve performance; healthcare providers may use results to better understand health patterns; and users can work with healthcare providers to use the wearable to track long-term goals and prevent certain health risks.[222] At same time, some observers have raised concerns about the privacy and security of data collected through these technologies.[223]

15. Education and Schools

The use of biometric technologies in schools is being explored as a way to improve efficiency, safety, and student experience. One example is to improve student safety by authenticating individuals as they come into schools to monitor for intruders. Administrative tasks such as attendance tracking could be replaced by fingerprint scanners or facial recognition, saving 3 to 5 minutes per class time.[224] Biometric technology can also be used to understand student engagement and ensure academic integrity. This can be inferred from behavioral observations and emotion recognition, which may help instructors personalize education or identify techniques to create the most effective and engaging learning environment. Biometric technologies can improve academic integrity by ensuring that student records are only authorized by those with proper credentials and authenticating students when taking exams or assessments, particularly for proctoring in online learning environments.[225] However, students and their families have raised concerns about the impact of these technologies on student privacy.[226]

16. Social Media

Many social media platforms now utilize biometric technology to authenticate account sign-in. Biometric systems have been used for tagging and sorting photos or creating and using filters on faces. There are also applications to authenticate age of user upon account creation, limit or deter bots and fake profiles, and otherwise improve the safety of the online community. However, there are harmful use cases as well. Social media platforms have become a resource for third-parties' biometric data processing, even without user knowledge or consent. Certain private companies, such as Clearview AI, have scraped billions of publicly available images from social media platforms and sold those images to both private sector companies and public government authorities.[227]

221 Carolina Graña Possamai, Philippe Ravaud, Lina Ghosn & Viet-Thi Tran, Use of wearable biometric monitoring devices to measure outcomes in randomized clinical trials: a methodological systematic review, BMC Medicine (November 2020).

222 "Fitbits of the future: What's next for biometric data in health?" Aetna.

223 *E.g., see* Marie Lamensch, "Putting Our Bodies Online: The Privacy Risks of Tech Wearables," Centre for International Governance Innovation, August 11, 2021.

224 Bob Hand, "Biometrics In Schools: 4 Ways Biometric Data Can Be Used To Enhance Learning," eLearning Industry (25 February 2018).

225 *Id.*

226 Jen A. Miller, "Biometrics in School to Yield Security Benefits and Privacy Concerns," EdTech, May 7, 2019.

227 Will Knight, "Clearview AI Has New Tools To Identify You in Photos," Wired (4 October 2021).

17. Virtual Immersive Experiences

An emerging field that relies heavily on biometric data is that of augmented and virtual reality. Augmented reality devices, typically known as "smart glasses," allow users to project images over their physical environment, whereas virtual reality devices, typically more complex headsets, replace an individual's physical reality with a virtual one. Social media or commercial tools that allow users to apply filters to real-world environments, including their face, are another example of augmented reality. In these cases, it is important to make sure users have been informed about the kinds of biometric data being collected and consent to doing so. The risk-level associated with these uses depends on whether biometric data is stored on service providers' servers and whether that data is combined with other data to make inferences. Companies that collect vast amounts of personal data may be able to use biometric data, together with other data about an individual, to make inferences about a range of topics including health conditions and potentially protected categories like political or religious affiliation.

About the Centre for Information Policy Leadership

CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at

http://www.informationpolicycentre.com/.

DC Office
2200 Pennsylvania Avenue
Washington, DC 20037
+1 202 955 1563

London Office
30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Brussels Office
Avenue des Arts 47-49
1000 Brussels
+32 2 643 58 00

24184.0424