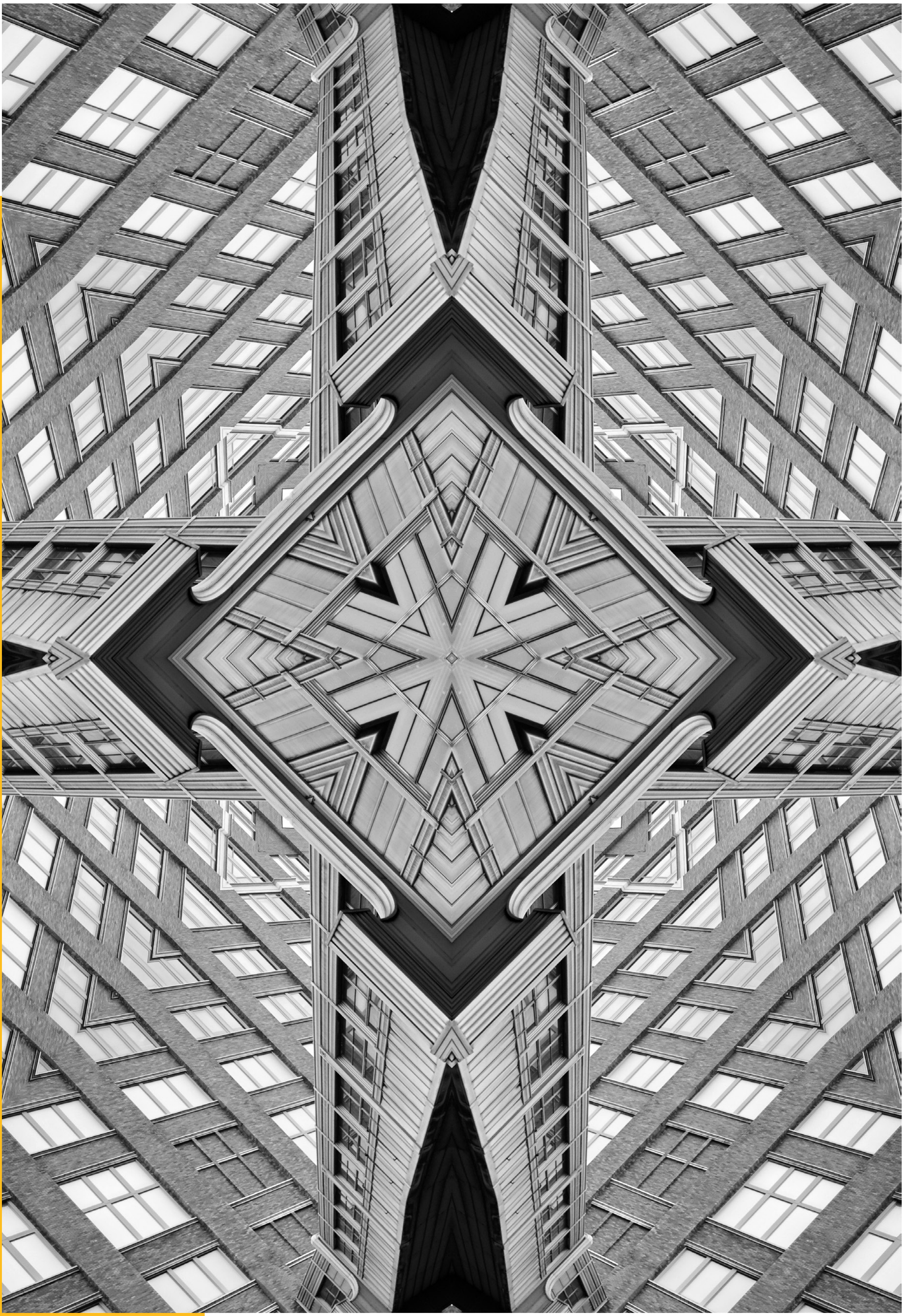
ORF OBSERVER RESEARCH FOUNDATION

Occasional Paper



ISSUE NO. 416 OCTOBER 2023

Ethical and Regulatory Considerations in the Collection and Use of Biometric Data

Shravishtha Ajaykumar

Abstract

Surveillance as a tool of governance holds more relevance today than ever before, as information technology grows by the day and collects more biometric data. Biometric data—either first-generation (static biological data) or second-generation (dynamic socio-spatial biological data)—is extracted from the biological and social aspects of individuals and used in surveillance for purposes of national security, civic responsibility, and business administration. As this data is intertwined with human experience, its collection and use provokes concerns around individuals' right to privacy. This paper discusses the ethical considerations of privacy in the collection and use of biometric data, as well as the associated regulatory requirements.

Attribution: Shravishtha Ajaykumar, "Ethical and Regulatory Considerations in the Collection and Use of Biometric Data," *ORF Occasional Paper No. 416*, October 2023, Observer Research Foundation.

Introduction

As technological innovations become more intertwined with people's daily lives, the fields of technology, biosciences, biodata, and biometrics begin merging. The surveillance of individuals[a] has been the subject of extensive research, starting with Foucault,[1] who considered security and biopower to go hand-in-hand.[2] This is especially evident in regions where not just States but also Big Tech companies like Google and Meta are considered as 'sovereigns'.[3] This biopower has come under scrutiny in recent years by regulatory agencies in certain parts of the world, resulting in a greater degree of accountability and awareness of individuals' right to privacy.[4]

The role of surveillance demands a discussion amid technological innovation, algorithmic bias, and increased monitoring.[5] In certain countries, biometric data is covered by privacy regulations. For example, the Digital Personal Data Protection Act, 2023 (DPDPA 2023) covers biometric data in India.[6] The law, however, like similar data privacy acts in other countries, tends to overlook the different types of biometric data, the vulnerabilities of individuals, and the protections required for these vulnerabilities.

This paper views biometric data in relation to surveillance as a tool of governance, specifically to control migration and enforce laws, and as a function of biotechnology and computational social science[b] that has extended beyond external biological features to include DNA samples, hormone mapping, and behavioural responses. The paper will discuss how ethical concerns around unregulated biometric data can be addressed through regulations.

[a] David Lyon considers 'surveillance' to include all aspects of an individual's public and private life, conducted in real time, and intended for future intentions and projects. See: David Lyon, "Theorising Surveillance"

[b] A systematic breakdown of human behaviour in response to social systems as analysed by computational and statistical research practices, used to analyse behavioural biometric data.

Introduction

Biometric Data in Civil Surveillance and Security

Biological data has begun to be integrated with technology to identify individuals based on their physical and behavioural traits, including fingerprints, retinal scans, voice mapping, DNA breakdown,[c] hormone mapping,[d] and first-generation or physical biometrics.[e] Biometrics also include human interactions with spatio-social stimuli, known as second-generation or behavioural biometrics. Depending on the state of the stimuli, data can be inferred for individuals or a social context, thus creating the subcategories of individual behavioural biometrics[f] and social behavioural biometrics.[g] Biometric data can also be used in more conventional identifiers such as radio frequency identity (RFID) tags and passports.[7,8]

Biometrics do not exist in a vacuum and are often used alongside artificial intelligence (AI) and immersive technologies like Web 3.0, especially in surveillance. These generative technologies often contain algorithmic biases evident in data storage and analysis. Unlike conventional surveillance, technology-based surveillance can connect seemingly unconnected data to form predictive patterns—this has social, ethical, and legal implications.[9]

Data storage and privacy are already regularly discussed in the field of technology policy, and this is especially evident in the way Big Tech collect and analyse information. However, including biological data increases this information's potential to become a political tool. For example, sovereign states invest in facial recognition that mirrors the use of face IDs in the private sector, such as in Apple products. Google's investment in human genome mapping[10] also highlights the increased need for storage, monitoring, and access to bioinformatics and biometric data, which translates to an increasing need for privacy regulations.

[c] Using the unique code of DNA to act as an identifier or as a base for identity matching.

[d] Measuring the hormonal responses of an individual to certain stimuli.

[e] Static biometrics derived from physical attributes.

[f] Measuring individual responses to (in most cases) device stimuli.

[g] Measuring individual responses to social and spatial stimuli.

Introduction

Biometric surveillance is significant in frontline policing at the national and global levels. INTERPOL has deployed multiple databases and projects to convert global crime monitoring to frontline policing. These include Project First (Facial, Imaging, Recognition, Searching and Tracking), which employs biometrics to identify criminals.[11] INTERPOL also uses its biometric databases to assist INTERPOL National Central Bureaus and frontline law enforcement authorities in global policing goals.[12]

Countries also use biometric data independently to assist in policing. However, the lack of regulation in this field has led to concerns around disregard for human rights and loss of privacy through misuse and nonconsensual use of data and misidentification. For example, Greece's biometric policing program, announced in 2020, has been observed to discriminate against migrants and racial minorities.[13]

Outside of government, private sector organisations also use biometric data to allow user databases to be more accurate for individuals to access goods and services. However, there is scope for biometric data to be exploited and even become obsolete. Facial recognition, for instance, can alter with ageing and contribute to mismatches in biometric datasets.[14] Biometric data is also vulnerable to hacking and can lead to individuals losing their privacy, and their access to public spaces and welfare services.[15]

Current Uses of Biological Data

Genetic fingerprinting was developed in the 1980s by Alec Jeffreys and has since assisted in crime detection, access, authentication, and databasing.[16] China has the largest government-held DNA database, with 68 million samples, followed by the United States (US), with over 17 million samples and the United Kingdom (UK), with over six million.[17] The private sector also has a significant database, with companies providing genetic and ethnicity tests using DNA samples; AncestryDNA, which claims to hold over 22 million DNA samples, has surpassed, in terms of the quantum of data held, the DNA databases of most countries and state powers.[18,19]

Biometric verification and authentication benefit identity authentication in the public sector, especially in financial services, law enforcement, and welfare goods and services. Biometric data is also used to augment authentication and privacy by incorporating such data into forms of access control, such as passwords and identity cards.

Implementing these technologies aids efficiency. For example, facial recognition technology is widely used in smart-gates at airports, allowing individuals to navigate immigration processes without depending on immigration officers. In addition, fingerprint scans and voice recognition technology are used to verify individuals' identities to access banking, healthcare, and documentation over devices like smartwatches, phones, and computers. Optical scanners for retinal IDs are also becoming standard practice. Additionally, intelligence organisations, border control, and immigration services frequently use DNA fingerprinting and other biometric data to identify and contain immigration.[20]

Drawbacks of Biometric Data Use

Older forms of biometric data collection, such as the physical collection of fingerprints, have existed for centuries. However, the utility of this data in a larger, transferrable, and searchable database for use in fields like defence and law enforcement is relatively new. The categorisation of identities in surveillance has increasingly depended on biometrics and bioinformatics.[21] Today, there is an increase in the scope of biological data collected and digitised to form interconnected databases, including transnational data from India, China, the UK, and the US.[22]

Current Uses of Biological Data

The momentum for this development can be traced to governments and government-related authorities wanting to monitor immigration and avoid lapses in national security. There is also increasing interest in collecting and processing biometric data outside of defence and security, especially in healthcare and law enforcement.[23]

Biometric samples are becoming increasingly equipped to represent gender, ethnicity, and health background accurately.[24] Hormone mapping, DNA fingerprinting, and other forms of biometric data can help create a digital representation of an individual.[25] However, this transformation of various physical aspects into digital code, field values, images, graphs, and scores implies interminable possibilities for the data to be categorised, retrieved, and used to infer individual identities and actions,[26] raising privacy concerns.

Further, the collection of DNA samples can contribute to discriminatory practices like racial profiling. While the science behind DNA profiling is generally reliable, there is scope for partial and incorrect matches.[27] Although DNA samples and other biometrics can categorise individuals into certain ethnicities, there are significant margins for error. These biometrics could contribute to potential race-based bias in human operators and augment existing biases in biometric data analysis technologies such as AI. To mitigate this issue, individual privacy must be maintained regarding racial identity, ethnic background, and disabilities, unless relevant to the case.

While DNA samples may provide indications of the racial and ethnic background of an individual, categorising human genomes into a few races is challenging. Recent advancements have increased the scope of reliable race and ethnic accuracy in forensic DNA mapping, but there has also been a simultaneous incongruent increase in racial profiling in law enforcement, which raises ethical concerns around this technology.[28,29]

Biometric systems and innovations, therefore, contain limitations that risk individuals' privacy and imperil ethical governance.[30]

a. Participation gaps

A number of challenges have been identified in registering biometric information. These gaps are noted when subjects who are required to submit biometric data cannot do so for varying reasons—such as a physical disability, a medical condition, or cultural and religious beliefs—or the devices used for inputting such information need to be updated or revised.[31]

This has been seen in the case of national identity cards, including India's Aadhaar, which have a standardised collection process for a large population. The collection may require the obligatory input of data that may not be fulfilled by those who are injured or have disabilities like missing fingers or damaged irises.[32]

b. False authentication

Biometric systems with incomplete databases or incorrect records may lead to false authentications.[33] People with similar DNA, such as family members, can be misidentified in databases. Examples of false authentication and rejection include facial recognition technology and its racial bias, which matches distorted images of people from marginalised races.[34]

c. Spoofing

The risk of identity theft has increased with the introduction of biometrics. If certain vulnerabilities are compromised or databases are leaked, there is scope for spoofing and replicating biometric characteristics that can put individual identities at risk. As biometric data cannot be altered, once this information is compromised, it is not possible to re-enter or alter the entry by changing characteristics such as fingerprints or retinal scans. Biometric information could also lead to function creep, i.e., the use of such technology and data[h] for a secondary, usually unauthorised purpose.[35]

[h] The expansion in use and utility applications for a technology beyond its intended use, especially when this contributes to a potential invasion of privacy.

In a study conducted in the European Union (EU), 25–30 percent of adults reported being victims of online identity theft.[36] With biometric data becoming more easily accessible, rendering deepfake technology, morphed images and voice mapped imitations are further enabling function creep.[37]

The US's Federal Bureau of Investigation (FBI) has also reported increased use of deepfake-based identity theft in employer scams. In 2020, over 16,000 people in the country reported being victims of scams that resulted in a loss of personally identifiable data, including biometric and financial data, and a loss of over US$59 million.[38] In another instance, the CEO of an energy firm in the UK fell victim to identity theft when his vocal recognition was stolen using AI-gen voice mapping to verify a fraudulent transfer of US$243,000.[39]

d. Covert collection

Covert collection involves the collection of biological data without the involved or responsible consent of the individual. For example, children's DNA samples have been collected in hospitals without guardians' authorisation or knowledge.[40] Such cases have ethical concerns, as the data can be misused for studies and analyses beyond the original purpose, or even for commerce.[41]

Secondary information can also be extrapolated from the collected data. Biometric data cannot be isolated from human existence or anonymised.[42] Even raw and rudimentary biometric data can reveal secondary information, such as health concerns, biological family lineage, ethnicity, and other genetic attributes, which individuals may not consent to provide; they may even result in false matches and incorrect assumptions around race and ethnicity.[43]

e. Non-consensual collection

Consent is usually transactional in cases of information privacy, i.e., individuals have the agency to choose which information to submit and to withdraw, depending on the services.[44] However, with biometric data, the possibility of consent is often removed, especially concerning immigration

Current Uses of Biological Data

and law enforcement. With biometrics like DNA samples, collection requires active participation and consent is usually needed. For other forms of biometric data, like facial recognition and secondary biometric data, it is possible to collect data covertly from a distance, thus increasing vulnerabilities.[45]

Data breaches of biometric databases used by employers, banks, and defence firms have led to concerns around the non-consented collection of biometric data by firms, misuse of data and unethical data sharing.[46] This data includes Facial Recognition Technology (FRT), socio-spatial movements, device keystrokes, eye-movement tracking, and other interactive actions that a consumer or citizen may not overtly consent to submit. Facial recognition, for example, is often covertly collected for civil surveillance, as in the case of Japan.[47] Individuals often need to submit biometric information to security companies to access their workspaces. Often, individuals cannot confirm the privacy of this data.

Biometrics in National Security

Fingerprinting has been used in most international travel and has served as an identifier in law enforcement since 1892, and for civil purposes since 1902.[48] Biometrics in national security gained more focus after the 9/11 terrorist attacks in the US, resulting in counterterrorism programmes that use biometric information and financial information for the surveillance, tracking, and prediction of attacks.

Such databasing is augmented with AI, which uses predictive analytics to create possible risk scenarios. However, the scope of misuse and the unreliability of AI due to inbuilt biases and abuse by malicious actors has led to the unfair surveillance of civil society.[49,50]

Poor design and intentional misuse of counterterrorism-related laws and measures have resulted in restrictions on human rights, including the rights to association, assembly, expression, privacy, and participation, and the criminalisation of activists. Most recently, emergency-related regulations enacted to respond to the COVID-19 pandemic amplified this trend, where racial biases and fake news led to the surveillance and disproportionate rejection of Southeast Asian immigrants seeking asylum in the US, UK, and other Global North countries.[51]

Biometric data is currently used for counterterrorism across 118 countries.[52] The United Nations Security Council's (UNSC) Resolution 2396 for member states to develop databases and use biometric data to identify threats highlights the use of biometric data in counterterrorism. The resolution also encourages the sharing of biometric data amongst other member states, organisations like INTERPOL, and private-sector participants for national security.[53] INTERPOL has also formulated Project First[i] and I-CORE,[j] which has garnered international traction.[54,55,56] Further, the UN International Organisation for Migration (IOM) has established the Migration Information and Data Analysis System (MIDAS), a biometric database that can assist in border control under the IOM's ethical guidelines.[57]

[i] Project First aims to share biometric data to assist in the improved identification and detection of terrorists.

[j] I-CORE is a program to assist border control, based on INTERPOL's I-24/7 database to identify individuals through biometrics, extended to front-line policing.

With these resolutions and guidelines, biometrics are having more use in anti-crime efforts, often assisted by unmanned aircraft systems, CCTV surveillance, and other recognition technology.[58] This includes techniques to identify individuals through algorithmic requirements, AI, and other emerging technologies. In addition, biometric technology is used to examine know-your-client (KYC) process databases to track the financing of terrorism.[59]

Despite their significant drawbacks to civilians, such uses of biometric data and technologies are justified by their assistance in counterterrorism. However, these technologies are also disproportionately used to disadvantage civil society, activists, protesters, and other dissidents, over actual terrorists.[60] This is evident in social media activism and the use of FRT in protester identification, such as in the use of FRT by the US police force to identify protestors.[61] Since AI software is already biased toward political, regional, and racial minorities, identifying marginalised groups expressing dissent is higher.[62,63]

The use of FRT also elicits distrust among protesters and citizens in the government and police forces. This distrust is especially pronounced in India, following the 2020 protests on citizenship laws, as well as in Canada, where FRT is being increasingly used in daily policing.[64,65]

Biological citizenship

The concept of biological citizenship uses biomedical information to assign social identity.[66] This collectivisation and bio-sociality[k] determine who can access social infrastructure such as rights, social welfare programs, and any other forms of physical or tangible public support. However, this also creates categorisations based on specific physical characteristics and disease vulnerabilities. While biological citizenship has been useful for increasing advocacy organisations and creating public awareness, it has also expanded the scope of racial discrimination and exclusion.[67,68] Such technologies are also used to discriminate based on race, as seen in Russia and China, to identify and disallow access to basic social infrastructure like housing.[69]

[k] The shared social community between individuals with shared biological attributes.

DNA testing and biometric classification are also often used in immigration decision-making, which often results in exclusion. For example, in family reunification through DNA testing, biological criteria are used to assign citizenship or entry into an asylum country to those with existing family members in that country. However, the same technology has unfairly categorised applicants from specific ethnic backgrounds as "undesirable".[70]

Biometrics in Civic Spaces

Biometric technologies are also utilised in civic spaces, including voter IDs, national ID cards, ration cards, banking, employment, purchase, and devices like mobiles and smartwatches, as well as other developing technologies. The use of counterterrorism technologies in standard technology for national and social identity under the purview of personal security augment the surveillance, privacy, and human rights challenges associated with biometrics.[71]

India's Aadhaar is the most extensive biometric identity system globally, devised to provide subsidies, welfare programmes, and services to the residents of the country. This system uses a 12-digit identification number for every registered individual and uses biometrics as one of the primary identifiers of individuality. The biometric process uses ten fingerprints, two ocular scans, and a photograph alongside demographic data to ensure inclusivity, without depending on caste, ethnicity, and blood type.

However, the supposed inclusivity of Aadhaar is already faulty, since the process excludes disabled persons who may be unable to provide all ten fingerprints or iris scans; the elderly or injured, who may also not be able to complete the biometric requirements; transsexual people whose demographic details and biological details may not align with their identity; as well as other marginalised groups.[72,73] These issues also limit these individuals' access to benefits such as banking and healthcare.[74] Aadhaar has also been criticised for privacy concerns, including data leakages and function creeping, identity theft, and spoofing.[75]

Biometrics in Private Spaces

Social media platforms are generally provided as a cost-free service, with their profits being attributed to advertisements, other businesses, subscription models, and, in many cases, through the collection, use, and sale of users' data to enhance other services.

While private platforms ask for users' consent when collecting data (usually as part of their terms and conditions), the lack of regulatory barriers creates concerns around information privacy. Meta-owned, Facebook, the largest social media platform, has been alleged to misuse facial recognition data. In a US$35-billion class action lawsuit, it was uncovered that users never consented to their pictures being scanned by FRT, nor was consent procured for the storage and long-term use of the biometric data.[76]

As most platforms now allow photographic and videographic submissions, facial recognition has become one of social media's most preferred data-collection methods. In addition, many platforms are expanding to use other forms of biometric data, such as palm prints.[77]

Behavioural Biometric Data

Physical biometric data is also known as first-generation biometric data and is static data that is based on the physical attributes of an individual. However, innovations such as Web 3.0 result in discussions around behavioural biometric data or second-generation biometric data.

While behavioural biometric data is not a novel form of data, it has been sparsely employed in regulation. A commonly discussed form of behavioural biometric data is the digital fingerprint, which includes personal data collected in collaboration with an individual's interaction with user interfaces. This identifier was initially developed for security purposes, under browser fingerprinting and device fingerprinting, to track individuals' activities on browsers and websites and identify malicious activity and actors.[78] Once assembled, a digital fingerprint can be accurate;

even with present generations of VPNs, restrictions on cookies, and regular cleaning of browser histories, trackers can still accurately identify and re-identify devices when a website is visited on more than one occasion.[79] Thus, privacy is a prevalent concern with digital fingerprinting. Individuals are vulnerable to organisations using information such as health data, financial data, and other sensitive information to determine candidates' suitability for college intakes, for instance, or for access to financing and health insurance.[80]

Behavioural biometric data can be further classified into two types—individual behavioural biometrics and social behavioural biometrics. Individual behavioural biometrics include keystroke dynamics, mouse dynamics, and signatures, which are used for authentication and continuous identity monitoring. The application of behavioural biometrics could be challenging due to the data quality and size of the population.[81] Social behavioural biometrics use individuals' social interactions and communications with other users.[82]

Behavioural biometrics add new dimensions to data collection and use for personal authentication, enrolment, profiling, access control, privacy, and risk security. The inability of behavioural biometrics to collect data in 'flat' forms makes it unique; unlike current big datasets, these biometrics cannot exist as isolated datasets, as the acquired data concerns activities and interactions, and, thus, requires contextual analyses to create knowledge patterns. Behavioural biometrics can be analysed using human interaction modelling, including voice recognition, eye movements, head movements, hormone spikes and dips, and other human activities in response to spatiotemporal stimuli.[83] These features aid in creating authentication systems and ensure that online and offline activity is not malicious.[84]

Behavioural biometrics, specifically social behavioural biometrics, have advantages over physical biometric data. It is usually unobtrusive, i.e., the data can be collected from a distance. Unlike physical biometrics, which may require active enrolment, data can be collected in a relatively low-cost form through CCTV cameras and existing technology and collected both offline, using surveillance technology, and online. However, these characteristics have corresponding disadvantages, as they remove the need for explicit consent from the user. Furthermore, the inability to standardise and deduplicate[l] such data can lead to authentication errors.

Behavioural biometrics is already utilised in the preliminary stages of national security projects. One such instance is the Future Attribute Screening Technology (FAST) Project by the US's Homeland Security Advanced Research Project Agency and Science and Technology (S&T) Directorate Human Factors/Behavioral Sciences Division.[85] The FAST project, which began in 2008, aims to improve the screening process at checkpoints for entry into the country, using behaviour-based screening to identify possible malicious intent. The project also seeks to advance technologies that can automate such judgements and incorporate these technologies after volunteer testing.[86]

A similar project has been launched in the EU, called the Automatic Detection of Abnormal Behavior and Threats in Crowded Spaces (ADABTS), which uses behavioural biometrics to protect against crime, terrorism, and riots.[87] The ADABTS project is aimed at enhancing imagery surveillance and security screening operations by automatically detecting abnormal behaviour with possible malicious intent; the system only outlines suspicious behaviour, human operators take further steps. The ADABTS also interacts with the EU AI Act, as it does not depend on identifying the individual through real-time biometrics, but instead, compares the individual to a list of "threatening" behaviours. These distinguishing methods rely on signal-processing algorithms that detect predefined threat behaviours and deviations from normal behaviour.[88]

Digital fingerprinting and behavioural biometrics have begun to be incorporated as data-based identifiers by national governments and corporate entities.[89] The crossover of data collection by private entities and use by governments needs to be governed.

[l] The process of running data against all other data occurrences to ensure that there is no duplicate entry.

Ethical Concerns

The use of biometric technologies for various security purposes warrants discussions around the associated ethics given the limited checks and balances. For example, if biometric databases have a 99.9 percent reliability in isolating terrorists, in a population of one million, this could result in 100 false identifications. Such false negatives could compromise national security and result in the loss of individuals' privacy and integrity.

Biometrics can assist in tagging, tracking, and localising (TTL) using uncrewed vehicles. The data can be used by machine learning (ML) systems and AI systems to extrapolate data that is yet to be voluntarily submitted.[90] Vital Intelligence platforms can also collect facial scans of individuals through drones and identify people suffering from diseases such as COVID-19 and Ebola. Drones with Vital Intelligence can also identify individuals with other biometric traits like gait, heat levels, and facial structure.[91] Such innovations can be used to deploy vaccines and healthcare kits to affected individuals in war zones; however, much like any other technology, it has a dual-use dilemma and needs to be regulated.

Biometric data is also more difficult to anonymise. Moreover, including DNA mapping and racial biases in genetic sciences augments the racial bias in technologies such as AI and ML. Applying these technologies in the private sector allows businesses to access unauthorised data. They could also lead to law enforcers conducting unfair arrests and detentions, and to automated weapons targeting certain races and ethnicities over others in the interest of national security.[92] Further, second-generation biometrics allow for observational learning that eliminates the need for consent unless explicitly stated in the regulation.

Thus, biometric technology raises questions around privacy and human rights. The United Nations Commission on Human Rights has reiterated the need to regulate the monitoring of data and metadata, the underlying concept of which is extendable to biometric data, which is arguably more sensitive to exploitation.[93,94,95]

a. Private sector participation

Outside of national security, private sector organisations also need to be held accountable for the ethical collection, storage, and use of biometric data. These also need to be governed by explicit regulation. To aid this process, businesses should identify the human rights most likely to be impacted by an enterprise's activities and devise effective ways to prevent and mitigate the ethical implications.

b. Voluntary, willing, and repeated consent

The difference between first- and second-generation biometrics lies in the awareness of the data being collected. The required physical contact in first-generation biometrics enables an individual to consent to the submitted data. In the case of surveillance with second-generation biometric techniques, data capture and processing are distant, and possibly covert, removing the requirement for willful consent at the time of data submission or collection.

c. Behavioural attributes

Another ethical concern regarding second-generation biometric data is the process of analysis. The behavioural aspect of collection requires the analysis to be standardised and associated with individuals based on social norms. These norms differ socially, culturally, and even individually, increasing the scope for misjudgment rather than depending on self-identification. Moreover, the automation of this process furthers the possibility of misjudgment beyond human error.[96]

Addressing Ethical Challenges

Since collecting and using biometric data experience the same concerns as other information, the associated challenges can be addressed by ensuring compliance and conducting regular risk assessments.

Risk assessment

The risk assessment for human rights highlights due diligence on the part of businesses and involves conducting risk assessments that examine actual and potential human rights impacts, both direct and indirect, of business operations. Risk assessments should include all phases and aspects of business activities and monitor how the nature and scope of the risks may change over time. For example, data handling should include collection, retention, processing and sharing, and data disposal. Due diligence responsibilities should also cover all phases of technology development and deployment, including in relation to the sale or transfer of the product and after-sales support and maintenance.[97]

Compliance

Risk assessment needs to complement compliance measures. Governments and private organisations should adopt policies that establish minimum standards for existing legal and policy frameworks, including regulatory safeguards required by home countries or other government or public authorities. As part of their due diligence process, companies must also assess potential business relationships, including public authorities, to identify, prevent, and mitigate potential human rights impacts before entering contractual relationships. In addition, business enterprises must ensure that their operations are guided by international human rights law, including the 'respect, protect, remedy' framework established under the United Nations Guiding Principles on Business and Human Rights.[98]

Updating technologies for privacy

In addition to technological innovations for collecting and analysing such data, technologies and software need to be regularly updated to maintain privacy. For example, biometric systems can be developed to include liveness detection, which is used to distinguish between live and recorded biometric samples. This technology can differentiate between a live image and a 2D or 3D-printed representation of a person's face and can counter spoofing. However, a biometric solution may still be at risk of spoofing, function creep, and other attacks, thus requiring multi-level technology barriers to aid privacy.[99]

Global Regulatory Landscape

Biometrics are being globally incorporated in governance and business. However, regulations and legal guarantees around the same are still developing. The vast potential for new forms of knowledge production, policymaking, implementation, targeting, and the development of prevention strategies, while welcome, will also give rise to new forms of surveillance that may not be entirely benign.

Private sector organisations are not always liable to local governing structures and tools. If biometric data is collected and stored by organisations that are registered in locations without appropriate government tools, data and individual privacy may not be protected even though global norms label biometric data as an important right that requires protection.

Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights discuss an individual's privacy rights.[100,101] However, the language used is vague, resulting in their applicability to many fields other than just biometric data. Thus, there is an increasing need for explicit policies to protect biometric data.

India

The Information Technology Act, 2000 (IT Act) classifies biometric data as sensitive personal data[102] and covers the collection, disclosure, and sharing of such information. India also has the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, according to which, biometric data collected under its database is considered as 'sensitive data' under the IT Act.[103]

India has also made attempts at data privacy legislation—the most recent iteration of which was in 2022—under which sensitive data has been merged with personal data, and biometrics is only mentioned as an example.[104] Further, this legislation assumes consent based on participation rather than informed and willful consent, furthering the problem of privacy with integrity.

United Kingdom

The proposed EU AI Act, applicable in the EU and the UK, defines biometric data for authentication and identification.[105] However, the act overtly only considers biometric data to include face scans, with FRT as the underlying governed technology, whereas other forms of biometrics are not mentioned in the Act. While this is one step ahead of India, its exclusion of different forms of biometrics, especially vocal-recognition and second-generation biometrics, is concerning, as these alternative biometrics are becoming increasingly common in national security, civic spaces, and personal devices.

The United States

The Illinois, Texas, and Washington state laws govern biometrics in the US. Illinois became the first state to pass a biometric data privacy law, the Biometric Information Privacy Act (BIPA), in 2008, allowing for a private right of action, and holds the statute till date. The BIPA places compliance requirements and barriers on repurposing biometric data collectors.[106] However, much like the laws in the UK, it does not include second-generation biometrics in the definition of biometric data.

Texas and Washington also have broad biometric privacy laws, but neither creates a private right of action like the Illinois Act. Other states have passed information privacy bills, but they all follow the scope of the BIPA and exclude second-generation biometrics.[107]

Australia

Australia has outlined a set of Information Privacy Principles under the Privacy and Data Protection Act 2014. These principles cover biometric data and the interaction of biometric data and systems with privacy concerns.[108] The Office of the Victorian Information Commissioner (OVIC)[m] covers biometric data that includes static physical data and behavioural data, including keystroke dynamics and individuals' gait or signature.

[m] The primary regulator and advisor to the Victorian Government in Australia on the collection, use, and dissemination of data.

Australia also launched a critical infrastructure centre to oversee biometric data and protect classified information (including biometric data) under an agreement established with France.[109]

While OVIC has highlighted the importance of biometrics in relation to the existing Privacy and Data Protection Act, OVIC's mention of behavioural biometric data can be expanded to include social behavioural biometric data before daily use of this form of computational social science is normalised.

Japan

The biometric recognition system in Japan does not involve live facial recognition and uses existing images of those who have been previously arrested.[110] Thus, while law enforcement in Japan does not currently report using behavioural and live biometrics, biometric data is still stored in databases.

Japan's Act on the Protection of Personal Information, updated in 2017, includes physical biometric data under the protections allowed for personal data. The forms of biometric data included are static physical imagery, facial recognition, palm and fingerprint scans, iris scans, vocal prints, and DNA.[111]

In its most recent iteration, updated as of March 2023, biometric data is also protected under data that cannot be anonymised, or 'pseudonymised data'. Such data has protections for the use and identification of individuals by businesses but does not have protections for public sector use. Further, as in other regulations globally, the acts do not cover behavioural biometric data.

South Africa

South Africa launched its Protection of Personal Information Act in July 2020, which includes biometric information.[112] As per the Act, biometric data includes any data that can identify an individual through physical,

Global Regulatory Landscape

psychological, or behavioural means, which include blood type, fingerprints, DNA, iris scans, and voice recognition.[113] The Act ensures that any data that has been “de-identified”, which requires the anonymising of information, which cannot be “re-identified” for civil purposes. However, biometric data can identify individuals at all levels of law enforcement and national security. While the Act includes behavioural biometric data, it does not provide any special protections for such data.

Brazil

Brazil’s General Law for the Protection of Personal Data (LGPD) covers anonymised and sensitive data with protections for the individual. However, biometric data is covered only under sensitive personal data.[114] Further, under its definitions, while genetic data is highlighted separately from biometric data, behavioural biometric data needs to be explicitly mentioned.

Globally, biometric data is used by private-sector corporations, public-sector organisations, and law enforcement agencies. However, most regulations in the field only protect biometric data partially, if at all.

Explicit definition and subtypes of biometric data

As in the context of India and several US states, there is no explicit mention of biometric data outside of general data. However, in all cases, biometric data falls under sensitive data. However, there is still a need to quantify the protection of biometric data, both primary and secondary, and the associated bio-informatics.

It is thus necessary for national governing authorities to explicitly mention biometric data at the government and national levels, especially in terms of required consent in biometric data collection, and conduct compliance measures and checks to hold participating parties accountable. These should be extended to second-generation biometrics, especially considering the advent of FRT.

Standardised privacy-preserving biometric schemes (PPBS)

Standardisation of PPBS should be enforced at a national and international level. These methods can include biometric encryption,[n] cancellable biometric databases with biohashing,[o] and cancellable biometric databases with non-invertible transformed outputs.[p,115]

Individual systems of privacy protection also have drawbacks and can be combined with secure computational PPBSs such as homomorphic encryption,[q] which combines the abovementioned methods and creates privacy while ensuring data validity and verification.[116]

[n] This can be of two types—key binding, where a randomly generated secret key is encrypted using biometric features, and key generating, where a key is rendered from the biometric database.

[o] Biohashing is a two-step verification process that includes a randomly generated key and a user-created key that must be used to access the full biometric inferable data.

[p] Non-invertible transform results in a 'transformed' feature set that is difficult to trace back to its original and individual form.

[q] Homomorphic verification extracts the data and encrypts it with a key. This key, when entered, measures the validity of the data by means of a distance matrix to verify the information retrieved without accessing the original dataset and data submitted, therefore maintaining privacy.

The International Organization for Standardization (ISO), under ISO/IEC JTC 1/SC 37, has established standards around the need for biometric storage, protection against false authentication attacks, and the need for verification.[117] However, to truly implement these, governments will require regulation around standardising sensors to detect attacks and ensure PPBSs at the organisational and government levels.

Usage of clearance and checkpoints

Different forms of data, i.e., primary biometric data, secondary biometric data, and the informatics derived from them, need to be defined with varying levels of protection for sharing and use. Furthermore, these subdivisions in the governing documents need to include the clearance level and checkpoints to ensure that the inferred data and datasets cannot be misused. Such checkpoints can include trained human supervision until the error rates of automated systems are reduced. Legislations governing biometrics should include all forms of data, including second-generation biometrics, and create mechanisms for purpose limitation and repurposing barriers so that innovations in the field are not only governed by technical barriers and private-sector compliance. These mechanisms should also be held accountable at a national level.

Legal guarantees and authorised governing bodies

While regulations are necessary, legal guarantees are essential in the case of exploitation. For example, individuals should be allowed to withdraw data if the purpose of the data is extended beyond their consent. Further, if these regulations are removed and submitted information must be complied with, governing bodies should hold organisations accountable. This includes establishing a governing body to oversee biometric data protection regulation and compliance.

Statute of limitations on collection

All collected biometric data, depending on the intention and purpose limitation outlined at the point of collection, should be destroyed and discarded effectively after the decided-upon time. In cases of national security, law enforcement, and immigration, where biometric data may need to be maintained for a longer duration, the data can be updated to include changes in fingerprints or individual gait, representing physical and biometric data that may alter with age or injury. However, data collected for access and authentication cases in the public and private sectors should be discarded after a predetermined period. The UK National Health Service, for example, has claimed that they hold DNA data for a period of five years in some cases, before it is destroyed.[118]

Grades of protection

Similarly, depending on the authority using the data and the purpose for which it was collected, the data can have different grades of protection, allowing more individual autonomy and purpose limitation in private-sector collection.

Conclusion

As the forms of biometric data and their use and tools expand, the parameters for their human rights and privacy-compliant use continue to evolve accordingly. Bridging the gap between technological developments and legal and policy responses is a constant challenge for governments and has associated problems that may not have overarching solutions.

Biometric data collection has been used for racial profiling and unethical enforcement of state power. Lack of privacy, loss of access and authentication rights, and exclusion of people with disabilities are additional risks associated with biometrics. However, current forms of legislation are inadequate to address these disadvantages. With advancements in biometrics, including FRT, voice recognition, and behavioural biometrics, there is a need to enhance these legislations to pre-empt technological advancements and adoption in daily use and ensure that ethical challenges are addressed, as opposed to waiting for social and ethical disruptions before creating compliance checks and regulatory barriers.

A human rights-conscious approach also necessitates due attention to implementing strong protections for data-sharing and use. Reduced foreseeability of future implications also means that consequences of data use may not have been foreseeable when data was collected. This challenges the adequacy of informed consent as the basis for processing personal data, fairness and transparency in collection and processing, purpose limitation, and accountability in data handling. It further highlights the importance of assessing data use lawfulness and human rights compliance at every stage.

Shravishtha Ajaykumar *is Associate Fellow at ORF's Centre for Security, Strategy and Technology.*

Endnotes

1 Michel Foucault, “The Will to Knowledge: The History of Sexuality Volume 1,” *Penguin* (1998) https://www .google.co.in/books/edition/The_ History_of_Sexuality _1/5xSfDwAAQBAJ?hl=en&gbpv=1&dq=The+Will+to+Knowledge:+The+History+of+Sexuality+Volume+1&printsec=frontcover.

2 Michel Foucault, “The Will to Knowledge: The History of Sexuality Volume 1.”

3 L. Tilley, “Biopower,” *Global Social Theory*, 13 March, 2021, https://globalsocialtheory.org/concepts/biopower/.

4 A Ceyhan, “Surveillance as biopower,” *Routledge Handbooks Online*, 27 April 2012, https://www.routledgehandbooks.com/doi/10.4324/9780203814949.ch1_1_c.

5 David Lyon, “Theorising Surveillance.”

6 “Digital Personal Data Protection Act, 2023” *Ministry of Law and Justice, Government of India*, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

7 “Deployment of Biometric Identification and Electronic Storage of Data in MRTDs,” *International Civil Aviation Organisation* (2021), https://www.icao.int/publications/documents/9303_p1_cons_en.pdf.

8 “Biometrics.” *Global Biotechnology Insights,* https://www.globalbiotechinsights.com/glossary/308/biometrics.

9 David Lyon, “Theorising Surveillance.”

10 Will Knight, “Google Has Released an AI Tool That Makes Sense of Your Genome.” *MIT Technology Review*, April 2, 2020. https://www.technologyreview.com/2017/12/04/147305/google-has-released-an-ai-tool-that-makes-sense-of-your-genome/

11 INTERPOL, “Interpol’s Project First Was Recently Deployed to Cameroon CM to Record the Biometric Data of Prison Inmates Convicted of Terrorism-Related Offences. 500+ Suspected Foreign Terrorist Fighters Were Identified during the Mission, and Interpol Blue Notices Were Issued Accordingly,” *Twitter*, January 4, 2022, https://twitter.com/INTERPOL_HQ/status/1478284716650475523.

12 “Biometrics for Frontline Policing,” *INTERPOL,* https://www.interpol.int/en/How-we-work/I-CORE-our-vision-for-change/Biometrics-for-Frontline-Policing.

13 “Greece: New Biometrics Policing Program Undermines Rights,” *Human Rights Watch*, January 31, 2022, https://www.hrw.org/news/2022/01/18/greece-new-biometrics-policing-program-undermines-rights.

14 Battista Biggio et al., “Poisoning Adaptive Biometric Systems” *Lecture Notes in Computer Science*, *Springer* (2012), https://doi.org/10.1007/978-3-642-34166-3_46.

Endnotes

15 G. H. Sai et al., "Biometric Security in Internet of Things Based System against Identity Theft Attacks," *International Conference on Computer Communication and Informatics* (2023), https://doi.org/10.1109/ICCCI56745.2023.10128186.

16 Rana Saad, "Discovery, Development, and Current Applications of DNA Identity Testing," *U.S. National Library of Medicine*, April 2005, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1200713/.

17 Whittall, "The Forensic Use of DNA: Scientific Success Story, Ethical Minefield," *Biotechnology Journal. U.S. National Library of Medicine*, February 18, 2011, https://pubmed.ncbi.nlm.nih.gov/18348243/.

18 Margaret O'Brien et al., "Who has the largest DNA Database" *Data Mining DNA*, February 3, 2023, https://www.dataminingdna.com/who-has-the-largest-dna-database/.

19 Justin Jaffe et al., "Best DNA Test for 2023: Ancestrydna vs. 23andMe and More." *CNET,* https://www.cnet.com/health/medical/best-dna-test/#:~:text=AncestryDNA%20says%20its%20database%20contains,the%20DNA%20test%20kit%20services.

20 William R Wood, "Viral Power: Interview with Arthur and Marilouise Kroker," *Critical Sociology*, March 8, 2017, https://www.academia.edu/31780587/Viral_Power_Interview_with_Arthur_and_Marilouise_Kroker.

21 Irma Van der Ploeg, "The Illegal Body: `Eurodac' and the Politics of Biometric Identification - Ethics and Information Technology," *SpringerLink, Kluwer Academic Publishers,* https://link.springer.com/article/10.1023/A:1010064613240.

22 Morgan J Tear et al., "The Importance of Ground Truth: An Open-Source Biometric Repository," *LSE Research Archives,* March 2016, https://eprints.lse.ac.uk/66631/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Tear%2C%20M.J_The%20importance%20of%20ground%20truth_Tear_The_importance_of_ground_truth.pdf.

23 David Lyon, "Theorising Surveillance."

24 Crystal Huynh et al., "Forensic Identification of Gender from Fingerprints," *Analytical Chemistry,* October 13, 2015, https://pubs.acs.org/doi/abs/10.1021/acs.analchem.5b03323.

25 Crystal Huynh et al., "Forensic Identification of Gender from Fingerprints"

26 David Lyon, "Biometrics, identification and surveillance," *Bioethics*, October 14, 2008, https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-8519.2008.00697.

27 Shravishtha Ajaykumar, "DNA Technology Regulation Bill, Data Privacy, Dependence, and Bias," *Observer Research Foundation,* December 20, 2022, https://www.orfonline.org/expert-speak/dna-technology-regulation-bill/.

Endnotes

28 Chow-White et al., “Do Health and Forensic DNA Databases Increase Racial Disparities?” *PLoS Medicine, U.S. National Library of Medicine*, October 2011, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3186804/.

29 Filipa Quieros, “The Visibilities and Invisibilities of Race Entangled with Forensic DNA Phenotyping Technology,” *Journal of Forensic and Legal Medicine, Elsevier*, August 12, 2019, https://www.sciencedirect.com/science/article/pii/S1752928X19300873.

30 Alan Gleb et al., "Identification for development: The biometrics revolution," *Center for Global Development,* March 2, 2013, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2226594.

31 Alan Gleb et al., "Identification for development: The biometrics revolution."

32 Smriti Parsheera, “Participation of Persons With Disabilities in India’s Aadhaar Project,” *SSRN,* September 28, 2020, https://ssrn.com/abstract=3700984.

33 Alan Gleb et al., "Identification for development: The biometrics revolution."

34 Trenton W. Ford, “It’s time to address facial recognition, the most troubling law enforcement AI tool,” *The Bulletin,* November 10, 2021, https://thebulletin.org/2021/11/its-time-to-address-facial-recognition-the-most-troubling-law-enforcement-ai-tool/.

35 Bert Jaap-Koops, “The Concept of Function Creep,” *Taylor & Francis*, March 16, 2021, https://www.tandfonline.com/doi/full/10.1080/17579961.2021.1898299.

36 Kalvet et al., “Risks and Societal Implications of Identity Theft,” *Electronic Governance and Open Society: Challenges in Eurasia. Communications in Computer and Information Science, Springer* (2019), https://doi.org/10.1007/978-3-030-13283-5_6.

37 Akshay Agarwala et al., "Manipulating faces for identity theft via morphing and deepfake: Digital privacy," *Handbook of Statistics: Deep Learning, Elsevier* (2023), https://www.sciencedirect.com/science/article/abs/pii/S016971612200058X#:~:text=Morphing%20and%20deepfake%20techniques%20became,as%20interference%20in%20the%20election.

38 “FBI Warns Cyber Criminals Are Using Fake Job Listings to Target Applicants’ Personally Identifiable Information.” *FBI*, April 21, 2021, https://www.fbi.gov/contact-us/field-offices/elpaso/news/press-releases/fbi-warns-cyber-criminals-are-using-fake-job-listings-to-target-applicants-personally-identifiable-information.

39 Catherine Stupp, “Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case,” *The Wall Street Journal*, August 30, 2019, https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.

Endnotes

40 Lux Fatimathas, “Babies' DNA Secretly Stored in NHS Database,” *PET*, October 28, 2021, https://www.progress.org.uk/babies-dna-secretly-stored-in-nhs-database/.

41 Varsha Chiruvella et al., “Ethical Issues in Patient Data Ownership,” *Interactive Journal of Medical Research*, May 21, 2021, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8178732/.

42 Bonomi et al., “Privacy Challenges and Research Opportunities for Genomic Data Sharing,” *Nature Genetics*, July 2020, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7761157/.

43 Duello et al., “Race and Genetics versus ‘Race’ in Genetics: A Systematic Review of the Use of African Ancestry in Genetic Studies,” *Evolution, Medicine, and Public Health*, June 15, 2021, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8604262/.

44 Sara Atske, “Public Knowledge and Experiences with Data-Driven Ads.” *Pew Research Center: Internet, Science & Tech*, November 15, 2019, https://www.pewresearch.org/internet/2019/11/15/public-knowledge-and-experiences-with-data-driven-ads/.

45 Günter Schumacher, “Behavioural Biometrics: Emerging Trends and Ethical Risks,” *Second Generation Biometrics: The Ethical, Legal and Social Context*, March 2012, https://www.researchgate.net/publication/303648289_Behavioural_Biometrics_Emerging_Trends_and_Ethical_Risks.

46 Josh Taylor, “Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms,” *The Guardian*, August 14, 2019, https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

47 Japanese police using facial recognition for investigations,” The International Association of Privacy Professionals, September 17, 2020, https://iapp.org/news/a/japanese-police-using-facial-recognition-for-investigations/.

48 U.S. Department of Justice Office of Justice Programs National, “The Fingerprint Handbook,” *U.S. Department of Justice Office of Justice Programs National,* https://www.ojp.gov/pdffiles1/nij/225320.pdf.

49 Karamjeet Gill, “Prediction Paradigm: The Human Price of Instrumentalism,” *AI & Society, SpringerLink,* August 11, 2020, https://link.springer.com/article/10.1007/s00146-020-01035-6.

50 Alex Chen, “The Threat of Artificial Intelligence to POC, Immigrants, and War Zone Civilians,” *Medium*, February 18, 2019, https://medium.com/@access_guide_/the-threat-of-artificial-intelligence-to-poc-immigrants-and-war-zone-civilians-e163cd644fe0.

Endnotes

51 Samantha Artiga, "Asian Immigrant Experiences with Racism, Immigration-Related Fears, and the COVID-19 Pandemic," *KFF*, May 27, 2022, https://www.kff.org/coronavirus-covid-19/issue-brief/asian-immigrant-experiences-with-racism-immigration-related-fears-and-the-covid-19-pandemic/.

52 United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), "CTED Analytical Brief: Biometrics and Counter-Terrorism," *United Nations Security Council,* https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Dec/cted_analytical_brief_biometrics_0.pdf.

53 United Nations Security Council Resolution, "S/RES/2396(2017) Security Council," *United Nations Security Council,* https://www.un.org/securitycouncil/content/sres23962017.

54 "I-Core: Our Vision for Change," *INTERPOL,* https://www.interpol.int/en/How-we-work/I-CORE-our-vision-for-change.

55 "Netherlands Police Backs Interpol's Drive to Enhance Policing Information Exchange," *INTERPOL,*https://www.interpol.int/en/News-and-Events/News/2021/Netherlands-Police-backs-INTERPOL-s-drive-to-enhance-policing-information-exchange.

56 "Germany Supports Interpol in Its Digital Transformation," *INTERPOL,* https://www.interpol.int/News-and-Events/News/2020/Germany-supports-INTERPOL-in-its-digital-transformation.

57 "MIDAS," *International Organization for Migration,* https://www.iom.int/midas.

58 "Security Council - Counter-Terrorism Committee (CTC)," *United Nations Security Council,* May 2019, https://www.un.org/securitycouncil/ctc/content/trends-alert-%E2%80%93-may-2019.

59 "Case Study Jordan," *European Center for Not-for-profit Law,* https://ecnl.org/sites/default/files/2023-03/CASE%20STUDY%20-%20Jordan.pdf.

60 Alexandra Ulmer et al., "India's Use of Facial Recognition Tech during Protests Causes Stir," *Thomson Reuters*, February 17, 2020, https://www.reuters.com/article/us-india-citizenship-protests-technology-idUSKBN20B0ZQ.

61 Kirsten E. Roy, "Defrosting the Chill: How Facial Recognition Technology threatens free."

62 Kirsten E. Roy, "Defrosting the Chill: How Facial Recognition Technology threatens free," *Rodger Williams University Law Review* (2022), https://docs.rwu.edu/cgi/viewcontent.cgi?article=1790&amp;context=rwu_LR.

Endnotes

63 Drew Harwell, “Federal Study Confirms Racial Bias of Many Facial Recognition Systems, Casts Doubt on their Expanding Use,” Washington *Post,* December 19, 2019, https://www.washingtonpost.com/technology/2019/12/19/federalstudy-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-theirexpanding-use/.

64 Alexandra Ulmer et al., “India's Use of Facial Recognition Tech during Protests Causes Stir.”

65 “Police Use of Facial Recognition Technology in Canada and the Way Forward,” *Office of the Privacy Commissioner of Canada*, June 10, 2021, https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

66 Adriana Petryna, “Biological Citizenship: The Science and Politics of Chernobyl-Exposed Populations,” *Department of Anthropology Papers, University of Pennsylvania* (2004), https://repository.upenn.edu/cgi/viewcontent.cgi?article=1020&amp;context=anthro_papers.

67 Torsten Heinemann. “Biological Citizenship,” *SpringerLink, Springer International* (2022), https://link.springer.com/referenceworkentry/10.1007/978-3-319-09483-0_453.

68 Kevin P Donovan, “The biometric imaginary: Bureaucratic Technopolitics in Post-Apartheid Welfare,” *Journal of South African Studies* (2015), https://www.jstor.org/stable/24567044.

69 Umberto Bacchi, “Analysis-'Racist' Facial Recognition Sparks Ethical Concerns in Russia,” *Thomson Reuters*, July 5, 2021, https://www.reuters.com/article/uk-russia-tech-race-idUSKCN2EB0BC.

70 Ilpo Helen, “Biological Citizenship across the Borders: Politics of DNA Profiling for Family Reunification,” *Distinktion: Journal of Social Theory,* June 9, 2014, https://www.tandfonline.com/doi/abs/10.1080/1600910X.2014.923321.

71 United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), “CTED Analytical Brief: Biometrics and Counter-Terrorism.”

72 Deepa H. Ramakrishnan et al., “Fading Fingerprints Disconnect Aadhaar Link for the Elderly,” *The Hindu*, December 4, 2017, https://www.thehindu.com/news/cities/chennai/fading-fingerprints-disconnect-aadhaar-link-for-the-elderly/article21255867.ece.

73 “Digital ID and inclusion,” *University of South Hampton,* https://www.eprints.soton.ac.uk/442610/1/Digital_ID_and_Inclusion.pdf.

74 Ranjit Singh et al., “Seeing like an Infrastructure: Low-Resolution Citizens and the Aadhaar,” *PACM on Human-Computer Interaction*, October 2021, https://dl.acm.org/doi/pdf/10.1145/3476056.

Endnotes

75 Subhashis Banerjee et al., “Privacy Concerns with Aadhaar Identification Project,” *Association for Computation Machinery*, November 1, 2019, https://cacm.acm.org/magazines/2019/11/240384-privacy-concerns-with-aadhaar/abstract#:~:text=The%20main%20privacy%20concerns%20with%20Aadhaar%20are%3A&amp;text=Identity%20theft.,biometrics%20are%20not%20secret%20information.

76 Danny Thakkar, “Biometrics in Social Media Apps: Opportunities and Risks,” *Bayometric*, November 13, 2019, https://www.bayometric.com/biometrics-in-social-media-apps/.

77 Chai et al., “Contactless Palmprint Biometrics Using Deepnet with Dedicated Assistant Layers - the Visual Computer,” *SpringerLink*, July 11, 2022, https://link.springer.com/article/10.1007/s00371-022-02571-6.

78 Daniel Kessler, “This Is Your Digital Fingerprint,” *The Mozilla Blog*, July 26, 2018, https://blog.mozilla.org/en/privacy-security/this-is-your-digital-fingerprint/.

79 Daniel Kessler, “This Is Your Digital Fingerprint.”

80 Douglas MacMillan et al., “Student tracking, secret scores: How college admissions offices rank prospects before they apply,” *Washington Post*, October 14, 2019, https://www.washingtonpost.com/business/2019/10/14/colleges-quietly-rank-prospective-students-based-their-personal-data/.

81 Charles Li, “Biometrics in Social Media Applications. Biometrics in a Data-Driven World,” *Biometrics in a Data-Driven World*, December 2016, https://www.researchgate.net/publication/311365307_Chapter_5_Biometrics_in_Social_Media_Applications_Trends_Technologies_and_Challenges.

82 Madeena Sultana et al., “A Concept of Social Behavioral Biometrics,” *Proceedings - 2014 International Conference on Cyberworlds* (2014), https://www.researchgate.net/profile/Madeena-Sultana/publication/271204421_A_Concept_of_Social_Behavioral_Biometrics_Motivation_Current_Developments_and_Future_Trends/links/565ff73308ae1ef929856de2/A-Concept-of-Social-Behavioral-Biometrics-Motivation-Current-Developments-and-Future-Trends.pdf.

83 Oana Andrei et al., “Interpreting Models of Social Group Interactions in Meetings with Probabilistic Model Checking,” *Proceedings of the Group Interaction Frontiers in Technology, ACM Conferences*, October 1, 2018, https://dl.acm.org/doi/abs/10.1145/3279981.3279988.

84 Madeena Sultana et al., “A Concept of Social Behavioral Biometrics.”

85 “Future Attribute Screening Technology (FAST) Project,” *Department of Homeland Security, USA*, https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf.

Endnotes

86 "Future Attribute Screening Technology (FAST) Project," *Department of Homeland Security, USA*.

87 "Automatic Detection of Abnormal Behaviour and Threats in Crowded Spaces," *Europa EU,* https://cordis.europa.eu/project/id/218197.

88 Madeena Sultana et al., "A Concept of Social Behavioral Biometrics."

89 Daniel Kessler, "This Is Your Digital Fingerprint."

90 Angus Willoughby, "Biometric surveillance and the right to privacy," *IEEE Technology and Society Magazine 36, no. 3* (2017), https://ieeexplore.ieee.org/abstract/document/8038135.

91 Dawn Zoldi, "AI, a biometric info-gathering platform, can be a battlefield game-changer," *Military Embedded Systems,* January 29, 2022, https://militaryembedded.com/unmanned/sensors/ai-biometric-info-gathering-platform-can-be-a-battlefield-game-changer.

92 Eirini Ntoutsi, "Bias in data-driven artificial intelligence," *Wiley Interdisciplinary Reviews,* February 3, 2020, https://wires.onlinelibrary.wiley.com/doi/full/10.1002/widm.1356.

93 "The Right to Privacy in the Digital Age: Report (2021)," *Office of the United Nations High Commissioner for Human Rights* (2021) https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021.

94 Nancy Liu, "Bio-Privacy: Privacy Regulations and the Challenge of Biometrics," *Routledge & CRC Press* (2012), https://www.routledge.com/Bio-Privacy-Privacy-Regulations-and-the-Challenge-of-Biometrics/Liu/p/book/9780415823395.

95 Noureddine Belgacem, "A Novel Biometric Authentication Approach Using ECG and EMG Signals," *Journal of Medical Engineering & Technology,* Taylor & Francis, April 2, 2016, https://www.tandfonline.com/doi/full/10.3109/03091902.2015.1021429.

96 "Behavioral Biometrics to Detect Terrorists Entering U.S.," *Homeland Security Newswire,* September 28, 2010, https://www.homelandsecuritynewswire.com/behavioral-biometrics-detect-terrorists-entering-us.

97 Enrico Schiavone et al., "Risk Assessment of a Biometric Continuous Authentication Protocol for Internet Services," *First Italian Conference on Cybersecurity* (2017), https://ceur-ws.org/Vol-1816/paper-06.pdf.

98 "Guiding Principles," *Office of the United Nations High Commissioner for Human Rights*, https://www.ohchr.org/sites/default/files/Documents/Issues/Business/Intro_Guiding_PrinciplesBusinessHR.pdf.

Endnotes

99 Saptarshi Chakraborty et al., "An overview of face liveness detection." *International Journal on Information Theory,* April 2014, https://arxiv.org/abs/1405.2227.

100 “Universal Declaration of Human Rights,” *Office of the United Nations High Commissioner for Human Rights,* https://www.ohchr.org/en/universal-declaration-of-human-rights#:~:text=The%20Universal%20Declaration%20of%20Human%20Rights%20(UDHR)%20is%20a%20milestone,rights%20to%20be%20universally%20protected.

101 “International Covenant on Civil and Political Rights,” *Office of the United Nations High Commissioner for Human Rights,* https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-right.

102 “The Information Technology Act, 2000,” *India Code,* https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

103 “Laws in India Governing Facial Recognition Technology,” *Legal Service India,* https://www.legalserviceindia.com/legal/article-6388-laws-in-india-governing-facial-recognition-technology.html#:~:text=The%20Information%20Technology%20Act%2C%202000,and%20sharing%20of%20such%20information.

104 “The Digital Personal Data Protection Bill, 2022,” *Ministry of Electronics and Information Technology, Government of India,* https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf.

105 "E.U. AI Act," November 28, 2022, https://artificialintelligenceact.eu/.

106 “The Illinois Biometric Information Privacy Act (BIPA),” *Illinois Government, United States of America,* https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&amp;ChapterID=57.

107 “Biometric Data Privacy Laws and Lawsuits,” *Bloomberg Law,* https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/.

108 “Biometrics and Privacy - Issues and Challenges,” *Office of the Victorian Information Commissioner,* October 6, 2022, https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/#easy-footnote-bottom-1-22905.

109 “Attorney-Generals-Department-Annual-Report-2016-17,” *Attorney-General’s Department, Government of Australia*, March 8, 2020, https://www.ag.gov.au/about-us/publications/attorney-generals-department-annual-report-2016-17/annual-performance-statement/strategic-priority-2-security.

110 “Japanese police using facial recognition for investigations.”

111 “Act on the Protection of Personal Information,” *Government of Japan,* https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en#je_ch1at2.

Endnotes

112 "South Africa's Protection of Personal Information Act, 2013, Goes into Effect July 1," *The National Law Review,* https://www.natlawreview.com/article/south-africa-s-protection-personal-information-act-2013-goes-effect-july-1.

113 "Protection of Personal Information Act Section 1 Definitions," *Government of South Africa,* August 31, 2020, https://popia.co.za/section-1-definitions/.

114 "General Law for the Protection of Personal Data (LGPD)," *Government of Brazil,* https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

115 Iynkaran Natgunanathan et al., "Protection of privacy in Biometric Data," *IEEE Access* (2016), https://ieeexplore.ieee.org/document/7420576.

116 Iynkaran Natgunanathan et al., "Protection of privacy in Biometric Data."

117 "Standards by ISO/IEC JTC 1/SC 37," *International Standards Organisation,* https://www.iso.org/committee/313770/x/catalogue/p/0/u/1/w/0/d/0.

118 Lux Fatimathas, "Babies' DNA Secretly Stored in NHS Database," *PET*, October 28, 2021, https://www.progress.org.uk/babies-dna-secretly-stored-in-nhs-database/.

Images used in this paper are from Getty Images/Busà Photography (cover and page 2) and Getty Images/Otto Stadler (back page).

OBSERVER
RESEARCH
FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org