FORHUMANITY

BIOMETRIC DATA

HUMANITY'S MOST PRECIOUS DATA

FEB 2022 // PREPARED BY RYAN CARRIER, INBAL KARO, JO STANSFIELD, SUNDAR NARAYANAN

THE UNSTOPPABLE RISE OF BIOMETRIC SYSTEMS

Biometric systems have rapidly become an everyday feature of our lives. Facial recognition in public spaces, fingerprint scanning in phones and entry systems, mood recognition from voice analysis in customer service - biometric systems are so common, they are almost taken for granted. Cases in point are the recent attempted applications of facial recognition in UK School Cafeterias and by the IRS trying facial recognition for account access to “simplify” and “facilitate efficient” engagement. But biometric systems are far from innocuous, and their prevalence shouldn’t mask the danger they pose. In fact, ForHumanity believes, the treatment of Biometric Data is insufficiently governed, everywhere in the world, in all systems, and in all legal jurisdictions. This includes jurisdictions with seemingly robust data protection laws, such as the UK and EU with GDPR. This law, like many other Biometric Data laws, misrepresents the vital importance and, the true intrinsic nature of Biometric Data.

While biometric data is of course Personal Data, it is more dangerous and sensitive than most types of data relating to humans. This is true for three main reasons:

1. **The immutable nature of many Biometric Data items** makes them more intrinsic to people's being than most other data, and so results in enormous risk to people from breach, theft, misuse and misappropriation.
2. **The richness of information extractable from biometric data** makes drifts in scope, nature, and purpose extremely common and potentially almost endless, and
3. **The conspicuous nature of many biometrically scannable identifiers** (say, our faces or gaits) makes such data potentially very public, and has already led to a significant breach of privacy whenever people are in public places, physically or virtually.

There are many uses of Biometric Data already in commercial implementation. While this is usually considered benign, there is an extreme asymmetry with respect to the benefits of the use of such data, given the risks outlined above, which is rarely characterized with transparency and disclosure. If the risk/reward profile was more widely recognised, it is our belief that uses of Biometric Systems would be held to higher standards, and fewer usages of frivolous Biometric Systems would occur. Further, if the law required sufficient levels of governance, protection and oversight be applied to uses of Biometric Data, then the "cheap and easy" solution would begin to lose its luster.

Current adoption of Biometric Systems is built on a flawed risk/reward profile. The reward is skewed to the system operator and the risk is almost exclusively on the side of individuals subject to these systems. As of now, many biometric systems are being tailored to maximize profitability or efficiency, without enough regard to the possible - and often probable - harms that humans may incur, including often unproven and potentially unprovable conclusions reached by these systems about us.

ForHumanity has deep concerns regarding the accuracy, validity, and assumed causality of many Biometric Systems. Many of the inferences (e.g race, mood, personality characteristics, mental state) are very hard to test against a ground truth, as they are often hazy even when being defined by humans and are frequently based on scant scientific evidence. Furthermore, most of these systems are poorly adapted to edge cases, like the disabled, neuro-divergent or other at-risk protected categories and intersections thereof. In consequence, ForHumanity requires a risk-based approach to accepting Accuracy, Validity, Reliability, Robustness, Resilience (AVR3). Biometric Systems call for especially high transparency, high disclosure, and an assumption of high risk.

ForHumanity is a non-profit public charity. We are an all volunteer organization with more than 850 people from more than 55 countries around the world. Our collective mission is to "examine and analyze downside risk associated with the ubiquitous advance of AI, Algorithmic and Autonomous Systems and where possible to engage in risk mitigations in these systems to ensure the best possible result...ForHumanity".

As a result, our perspective is predetermined for us and we focus solely on the risk from Biometric Data in its many manifestations. We hope that this paper will accomplish three tasks:

1. Raise awareness regarding the current state of distorted risk/reward profiles in Biometric Data systems
2. Highlight our process for introducing governance, oversight, accountability and trust related to Biometric Systems
3. Assist this burgeoning industry with a framework of audit criteria, mapping and comprehensive infrastructure of trust.

CLASSIFICATION OF BIOMETRIC DATA

Figure 1. Types of Biometric Data: Physiological; Physical behaviour; Digital interactions; and associated metadata

Images credits
Alan Warburton / © BBC / Better Images of AI / Quantified Human / CC-BY 4.0
Max Gruber / Better Images of AI / Clickworker 3d-printed / CC-BY 4.0

The definitions of biometric data vary greatly between various laws and regulations. For example, GDPR's definition does not include DNA data as Personal Data until it is attached to a "natural person". We consider this a false distinction, as DNA is more personal, more us, than our name, address, IP address or social security number. More importantly, it is immutable. Where almost every other element of "Personal Data" can be changed if it falls into the wrong hands, our Biometric Data cannot without extraordinary processes, if at all.

ForHumanity's found most laws, and guidance on Biometric Data to be too narrow, poorly defined, insufficiently futureproofed, and filled with loopholes that are already being exploited. Our comprehensive Biometric Data definition includes: ForHumanity's found most laws, and guidance on Biometric Data to be too narrow, poorly defined, insufficiently futureproofed and filled with loopholes that are already being exploited. Our comprehensive Biometric Data definition includes:

- Any **scans of biometric identifiers**, through physical scanning, digital mechanisms, and processing of secondary files (such as photographs). These include, among others, scans of face, gait, voice, keyboard strokes, and many more. See Figure 1 for further examples.

- Among these, we include as Biometric Data also **data that is not associated with some more "classic" identifier**, such as a name or an ID number. We argue that the fact that this data (say, a face scan) is capable of personally identifying individuals is sufficient to be considered sensitive personal information to the highest degree. In fact, this data is arguably even more identifying of a person than their name or address. .

- In combination with the Biometric Data, its metadata (such as time or location of a given scan) also requires the highest protection, as it can give rise to powerful inferences about that person. We therefore include **associated metadata** in our definition of Biometric Data

- Any **inferences or deduced information** from the biometric scans are also a type of Biometric Data. Many types of information extracted from biometric scans would be considered sensitive personal information (or Special Category Data, depending upon the jurisdiction) to the highest degree. The Biometric Data that can be extracted from the sample may increase over time as new technology becomes available.

As we have previously mentioned, it is important to treat Biometric Data as highly sensitive personal data and therefore require it be held to the highest security standards. According to our broad definition, this is true not only of the databases which match Biometric Data with other personal identifiable data (such as names, state identification numbers) but also databases of the biometric scans themselves, and the metadata associated with those scans.

CLASSIFICATION OF BIOMETRIC SYSTEMS AND THEIR USES

There are many types of biometric systems, and more are being invented all the time. To discuss them comprehensively one must make a classification that captures not only those systems that exist today but also those that will come to pass in the future, and enables us to analyze them broadly.

To that end we suggest that biometric systems must be analyzed in three parts:

1. **What is scanned** (e.g. fingerprint, gait, keystroke, face);
2. **What information is extracted** (e.g. identification, mood, thoughts, medical metric); and
3. **What is done with that information** (e.g. access, arrest, nudge).

In addition to these three processes, there is the meta-level of **information flow within the system**: what data will be stored and for how long, how and where information will flow, and how it is protected.

We submit on the following page a broad, but not comprehensive, mapping of different types of biometric systems, mapped along each of these processes (Figure 3).

In addition to these three processes, there is the meta-level of information flow within the system: what data will be stored and for how long, how and where information will flow, and how it is protected.
We submit below a broad, but not comprehensive, mapping of different types of biometric systems, mapped along each of these processes.

At the heart of our approach, we believe that any consent to the use of a biometric system, or the governance of such a system when it is not consent-based, must explicitly include all three of these processes, as well as the data flow. For example, while police use of facial scanning for identification of known criminals might be approved, this does not allow the police to use the same footage for other purposes (say, identifying passers by), or the same scans for extracting other information (say, mood of said criminals). **Consent or governance must explicitly cover what will be scanned, what information may be extracted from those scans, and what may be done with this information; in addition, it must cover which of this information will be stored for how long.** When any of these changes - what we refer to as mission creep - new consent or approval is required.

In addition to other forms of mission creep, ForHumanity has witnessed myriad instances of Biometric Data capture that is then “reapplied” in the name of Academic Research and the creation of very large datasets for model training. These rationalizations of mission creep are dangerous. First, there are the ethical considerations not only of the basis upon which the data is acquired, but also on the societal-wide benefits, the process by which this is measured and determined and by whom these conclusions are reached. Consent may be readily granted for meritorious research transparently and clearly disclosed. Currently, this domain is opaque, ungoverned and unaccountable.

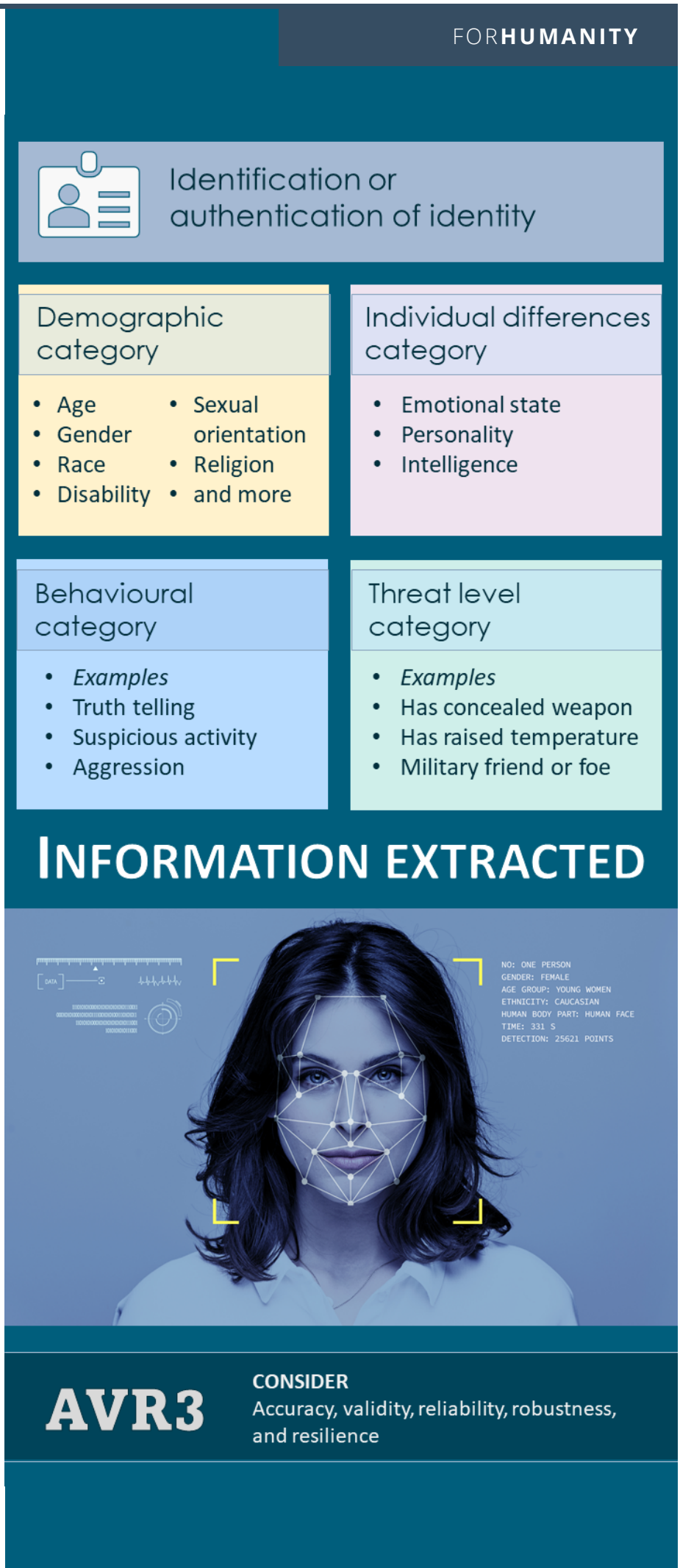
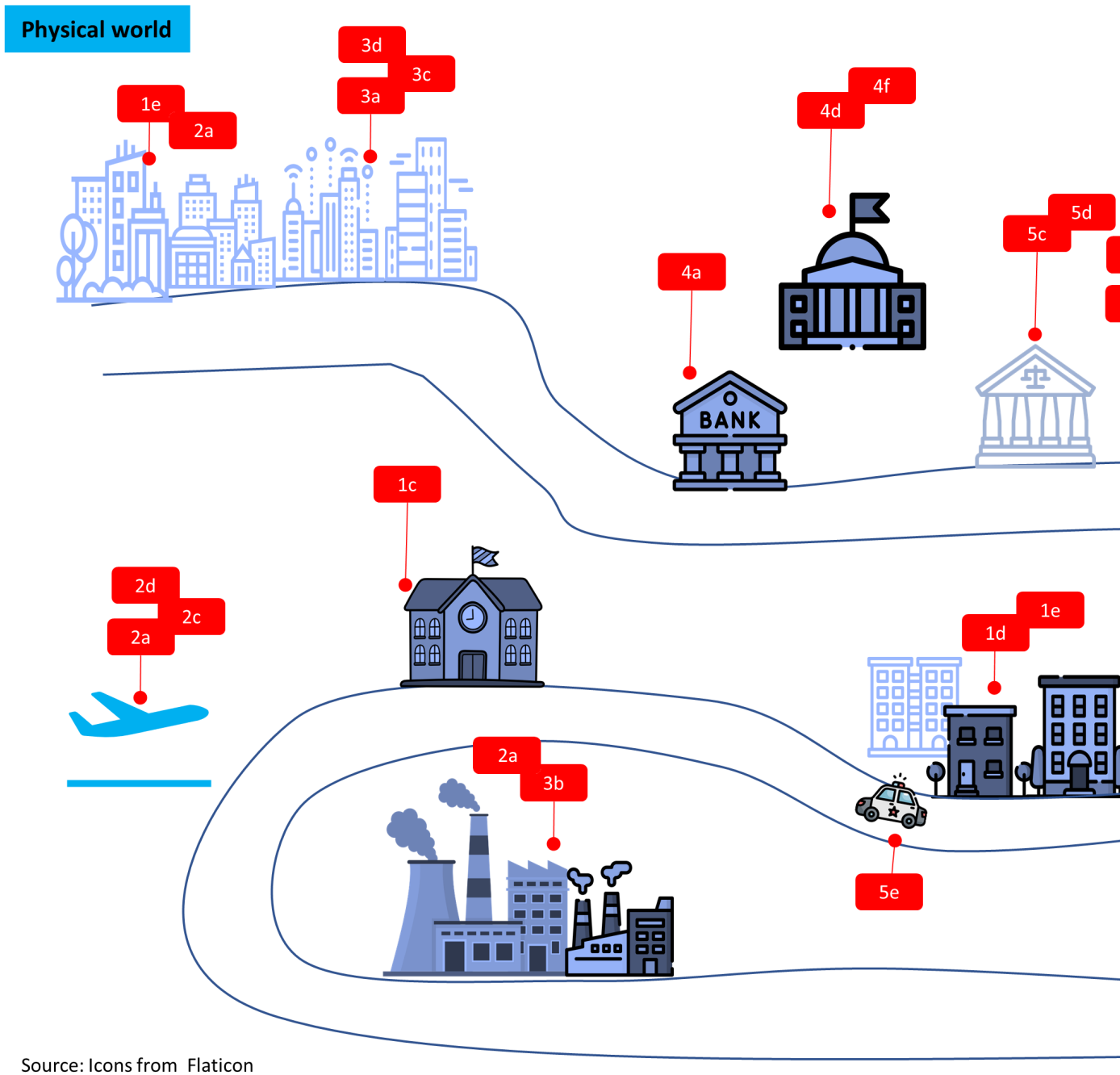


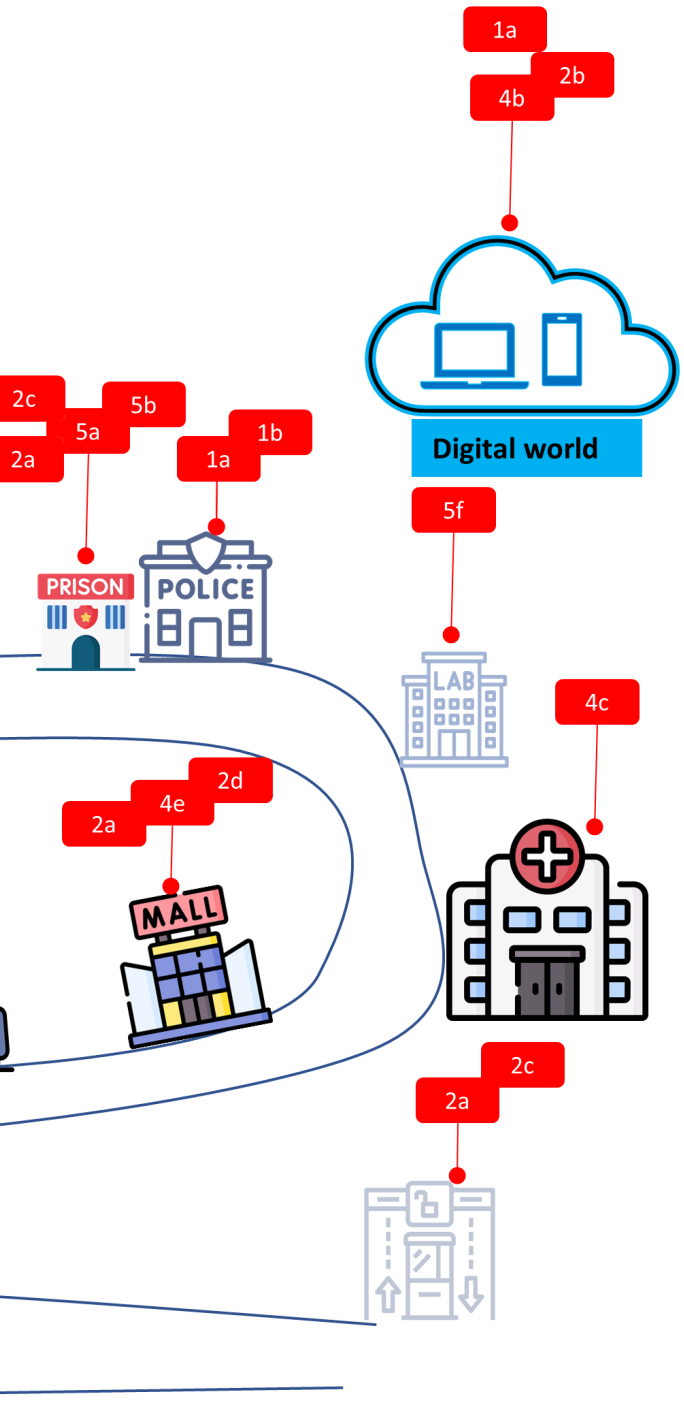
Figure 2.
Information extracted from a biometric scan: Demographic categories; Individual differences categories; Behavioural categories; and Threat level categories.
Consideration must be given to the accuracy, validity, reliability, robustness, and resilience of the extraction

BIOMETRIC SYSTEM APPLICATIONS



Source: Icons from Flaticon

Figure 3. Applications of Biometric Systems: Surveillance; Entry Systems and Security Scans; Employment Related Systems; Access to Services; and Law Enforcement



1. Surveillance
a.Public mass surveillance b.Police surveillance c.School d.Care home e.Building security
2. Entry Systems & security scans
a.Physical b.Digital c.Full body d.Temperature
3. Employment related
a.Background checks b.Time and attendance tracking c.Skill matching d.Gig economy work
4. Access to services
a.Financial services b.Fraud prevention/ security c.Healthcare d.Voting e.Customer recognition f.National identify card scheme
5. Law enforcement
a.Prison release systems b.Prison identifier c.Sentencing decisions d.Parole decisions e.Predictive policing f.Forensic

POTENTIAL HARMS ASSOCIATED WITH THE USE OF BIOMETRIC SYSTEMS

ForHumanity's approach to harms associated with Biometric Systems includes dividing them into two categories: 1) the harms that occur when the system goes wrong, and 2) the harms that occur when the system works as planned.
While some of the potential harms of Biometric Systems may seem futuristic or far-fetched, most of those listed here are already very much the case today. ForHumanity believes that there is not enough consideration of the harms that Biometric Systems cause to humans, especially when (not) balanced against the great benefits they often bring to governments and larger corporations.

Some of the harms that might occur **when a system goes wrong** include:

- **Bias** - the quality of the system's application might differ between various protected category groups (and intersections thereof), such as facial recognitions' systems not being trained on darker faces. In such a situation, a certain group would suffer the effects of misidentification, denial of access, false arrests, and more. This problem requires attention and bias mitigation throughout the process, starting with the training data which often contains historical bias that needs to be rectified

- **Inaccessibility** - Disabled people are frequently inadequately captured in datasets and Biometric System development resulting from a "normal" outward statistical construct, rather than an "edge in" design approach that includes diverse input at the design, development and deployment phase, rather than the traditional post hoc, outcomes-based feedback.

- **Intractability** - Finality of decisions based on Biometric Data, without the ability to appeal decisions or change them in time, could cause great harm (for example, a car's refusing to start because its biometric scanner incorrectly deems a driver incapable of driving might leave a person unable to get to work or to pick up a child). In mitigation of this, systems must incorporate the following:

    - Right to Object
    - Right to Rectify
    - Right to Access
    - Right to withdraw consent
    - Right to have one's data deleted

- **Lack of Explainability** - a human-centric issue around dignity. Corporations and Governments exist through human constructs for organization and efficiency - they both owe the people they serve a reasoned and transparent explanation for the decisions that the tools conclude deploying Biometric Data

- **Poor Decisions** - Insufficient validity and accuracy in model construction, including incorrect conclusions or inferences that cannot be proved, and insufficient data for validation and accuracy at the protected category level

- **Failed Security** - Breach or exposure of data and potential misuse of them

Some of the harms that might occur with a **perfectly functioning, unbiased, biometric system**:

- **Disproportionality** - the loss of privacy in public spaces, where biometric surveillance might constantly run face recognition, mood analysis, behavior analysis, identification of sexual orientation, and more

- **Mission Creep** - with more and more information extractable from given samples, and with increasing possible uses of this information, biometric data given for specific purposes might be used for ones that the individual never meant to consent to

- **Manipulation of People against their Best Interests** - biometrics give deep insights into people's behavior, and these can be used for design / dark patterns that cognitively influence people

- **Data misappropriation** - data might be acquired for one purpose, and then deployed for further purposes of the acquirer beyond the consented scope and unrelated to the user

- **Excess control** including Social Scoring of people, especially the digitally marginalized, that fails to support their basic human rights

The potential harms of biometric systems are, in our opinion, wide and varied. As mentioned above, the current adoption of Biometric Systems is often built on a flawed risk/reward profile, because the reward is skewed to the corporate side and the risk is almost exclusively on the human who is subject to its operation, or of specific groups thereof. In addition, when assessing potential harm, there is rarely a process that includes diverse multi-stakeholder input, which is necessary for robust quantification and comparison of potential harms. We advocate that a comprehensive and systematic consideration of harms is a basic requisite of the assessment of every biometric system.

APPLIED RISK MITIGATION, CONTROLS, GOVERNANCE, ACCOUNTABILITY AND OVERSIGHT

ForHumanity is gravely concerned regarding a series of characteristics already present in applications of Biometric Systems:

1. Insufficient security
2. Insufficient governance, accountability and oversight
3. Insufficient validity, accuracy, reliability, robustness and resilience (notably with respect to protected categories and intersections thereof)
4. Insufficient ethical governance
5. Poorly calculated risk/reward profile (Considerations of Necessity and Proportionality)
6. Wide-spread systemic bias against protected categories and intersections thereof
7. Questionable accessibility
8. Immutable nature of Biometric Data (more personal than our name)
9. Technological self-fulfillment, choice inhibition and prejudicial treatment

Therefore, given the myriad unmitigated risks, ForHumanity's suggestions and responses with regards to Biometric Data will always require the absolute highest levels of ethical oversight, bias mitigation, privacy protection, trust enhancements and cybersecurity diligence. In addition, our definition of Biometric Data attempts to be all encompassing to ensure a future-proofed capture of all risk to people.

Our risk mitigation suggestions can be categorized broadly in the following manner:

- **Prohibitions** (excessively risky, unethical, non valid, inaccurate, or illegal practices) - including unconsented scraping, unconsented data capture, data on-selling
- **Robust, documented assessment** of the delicate and nuanced balance between safety/security versus bias, privacy, accuracy and validity - executed ethically
- **Strict lawfulness and consent**, with tightly defined and tracked scope, nature, context and purpose
- **Ethical oversight**, including independent third-party governance, oversight, accountability, audits and internal Ethical Risk Analysis
- **Robust, risk-based requirements for Accuracy, Validity, Reliability, Robustness and Resilience** (AVR3) at the protected category level (and intersections thereof, especially for at-risk categories) including associated liability
- **Robust Risk management** including Biometric System Governance, Ethical Risk Analysis, Testing and Evaluation Risk assessment, and Algorithmic Risk Management
- **Diverse Inputs and multi stakeholder feedback** across needs assessment, design, development, deployment and decommission phases of the Biometric System lifecycle

- **Continuous monitoring,** post-market monitoring, and adverse event tracking systems

- **High disclosure and transparency** (presence of, disclosure of process)

- Strict **data minimization**

- Required and immediate **encryption**

- **Immediate deletion** (with robust definition of deletion) when Necessity is terminated

Independent Audit of AI Systems is a holistic approach that ensures Governance, Oversight and Accountability for Biometric Systems certified audit compliant. Certification governs Ethics, Bias, Privacy, Trust and Cybersecurity, maximizing risk mitigation to adverse human impacts from these systems. Some key contributions to risk mitigations are listed below:

- **Diverse inputs and multi stakeholder feedback** - specific risk input process required at design, development, deployment and decommissioning phases of Biometric Systems. Critical for maximized risk mitigation.

- Standing and empowered **Ethics Committees** managing myriad risks associated with instances of Ethical Choice embedded consistently in socio-technical systems deploying Biometric Data. Objective and trained in algorithm ethics, soft law navigation and Ethical Choice risk management to produce an Ethical risk Analysis

- **Code of Ethics and Code of Data Ethics** documented and public, issued by a standing and empowered Ethics Committee delineating the shared moral framework ethical principles and Relevant Legal Frameworks by which the organization will evaluate instances of Ethical Choice including the documentation of an Ethical Risk Analysis and the Residual Risk from questions of Ethical Choice. Then holding the process accountable with independent audit of compliance with criteria on Ethics.

- **Governance, Accountability, Oversight by design** - integrated with Enterprise Risk Management and assured with AI Governance Assessment dedicated to the Biometric System

- **Independent Audit** - by trained and certified independent auditors with expertise in audit compliance for each individual Biometric System using system specified audit criteria design from a human perspective to minimize risk when compliant

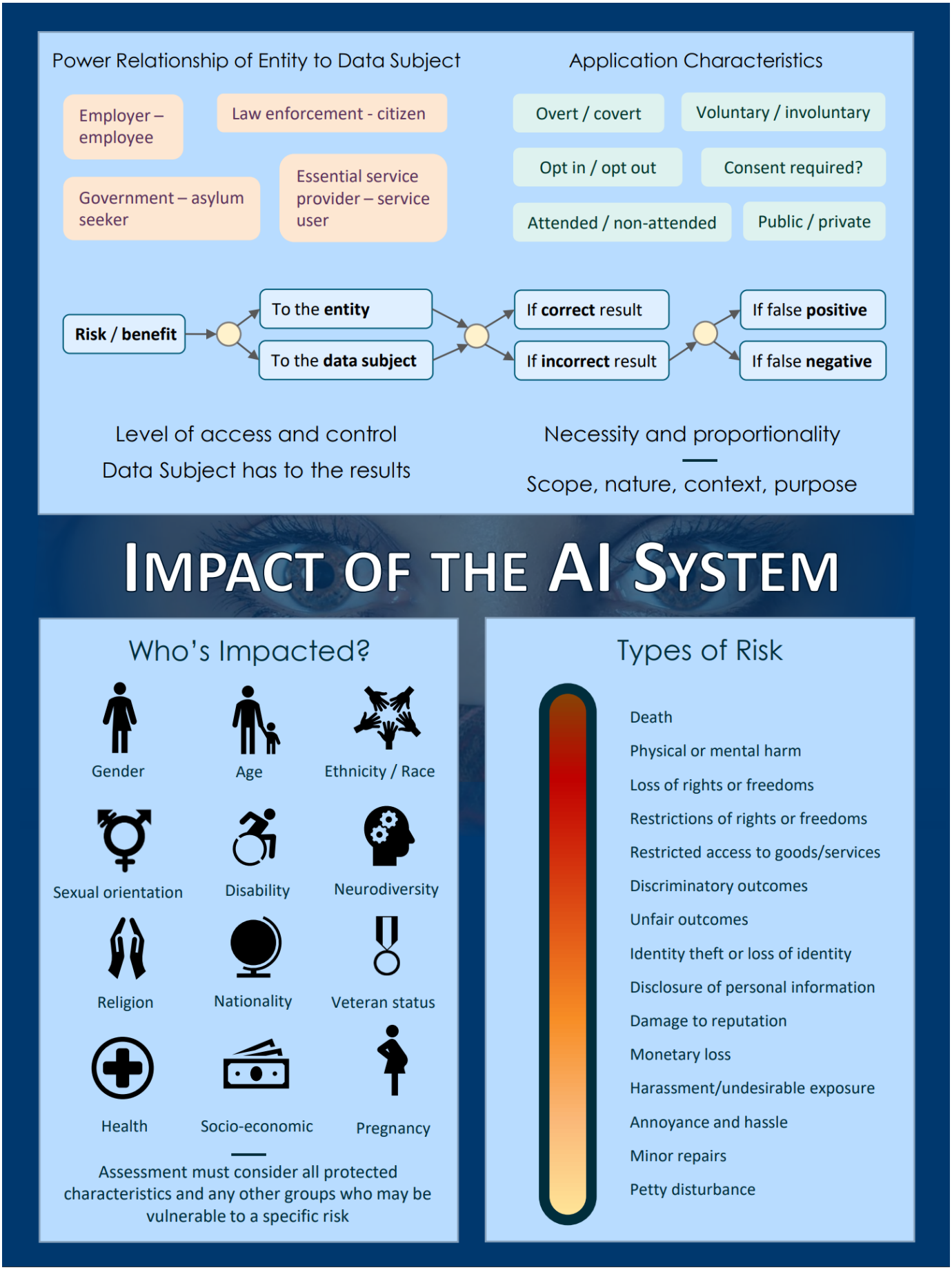
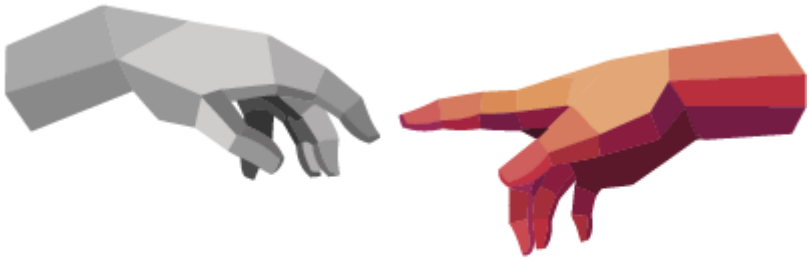


Figure 4. Impact assessment considerations for AI Systems

CONCLUSION

While public policy globally continues to neglect the critical nature of Biometric Data, ForHumanity will endeavor to raise awareness and provide risk mitigations thru Independent Audit of AI Systems and our dedicated Biometric Data audit criteria. Under current law, protections for people remain insufficient, leading to a distorted risk/reward paradigm for applications of Biometric Data Systems. ForHumanity endeavors to change this misalignment through its discussions with governments and regulators in addition to providing solutions for corporations that recognize that long term sustainable profits start are rooted in fair and ethical treatment of all people, notably when using their most precious forms of Personal Data, -Biometrics.



Ryan Carrier, *Executive Director of ForHumanity*
Inbal Karo, *ForHumanity Fellow*
Jo Stansfield, *ForHumanity Fellow*
Sundar Narayanan, *ForHumanity Fellow*

About ForHumanity

ForHumanity (https://forhumanity.center/) is a 501(c)(3) nonprofit organization dedicated to addressing the Ethics, Bias, Privacy, Trust, and Cybersecurity in artificial intelligence and autonomous systems. ForHumanity uses an open and transparent process that draws from a pool of over 850+ international contributors to construct audit criteria, certification schemes, and educational programs for legal and compliance professionals, educators, auditors, developers, and legislators to mitigate bias, enhance ethics, protect privacy, build trust, improve cybersecurity, and drive accountability and transparency in AI and autonomous systems. ForHumanity works to make AI safe for all people and makes itself available to support government agencies and instrumentalities to manage risk associated with AI and autonomous systems.