Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
Thoughts around and contributions to an A.I. Bill of Rights as requested by The White House Office of Science and Technology (OSTP) proposal to develop a "bill of rights" to protect American citizens against the potentially harmful consequences of A.I. or, more specifically, biometric data (facial recognition, voice analysis, heart rate tracking, etc.).

November 2021.

The original United States Bill of Rights spells out Americans’ rights in relation to their country. It purports to guarantee civil rights and liberties to the individual and sets rules for due process of law. Given the codified function of white supremacy and its many tendrils, not all people benefit equally from the bill of rights.

This effort is spearheaded by Stephanie Dinkins, Professor & Director of the Future Histories Studio (FHS) part of the DISCO Network, Department of Art, Stony Brook University, with input from FHS researchers, members of AI.Assembly, related artists, and Stony Brook University Campus Community members.
Prologue

People who live with the threat and discomfort of knowing the rights and liberties set out by the Bill of Rights are still not equally applied or protected.

“...a rights framework offers a wrongheaded approach to mediating the relationship between technology (created by human beings) and vulnerable populations within our society (also human beings). The history of international human rights establishes the global rights infrastructure as an aspirational rhetoric with significance in law, custom, and politics, but hardly as a safeguard against the continuing violence that is meted out against vulnerable and/or historically victimized populations within nation-states or against the violence (economic, political, and social) facing vulnerable and historically victimized peoples and lands around the world. As written above, the question separates "A.I. systems" from their human creators and the human economic interests that are inevitably tied to their existence and perpetuation. As we have yet to find a "bill of rights" either within the USA or around the world, the Universal Declaration of Human Rights (UDHR) or International Conventions of Civil, Political Rights, (ICCPR) and International Convention of Economic, Social and Cultural Rights (ICESCR), that adequately protects human beings from other human beings, why is the rights framework being deployed in the obfuscatory way in relation to A.I.? I would suggest that the lessons of the human rights and civil rights history around the world offer useful insights into mediating the shifting relationships between human beings and technology and that these would be useful sites of allegory, theory, and empirical analysis.”

– Abena Ampofoa Asare, Associate Professor, Modern African Affairs & History, Department of Africana Studies, Stony Brook University
In response to The White House Office of Science and Technology Policy (OSTP) call to engage the American public in the process of developing a Bill of Rights for an Automated Society, we offer the following requirements and rights for consideration.

Honored personhood and the Right to Opt-Out

As individuals and related communities, we require the same rights concerning biometric data as they would their person, personal information, and data created via personal digital tools.

As individuals and related communities, we have the right to opt-out of providing biometric data in both public and private spaces.

Transparency/ Non-Obfuscation / The Right to be Forgotteb

In lieu of the right to opt-out, individuals and related communities must be told any time biometric data is recorded or collected by private, public, and governmental entities and organizations.

- Standard of interaction- Individuals must be notified when data of any type related to their being is collected at each point of collection. This is especially true of more passive biometric technologies such as voice and iris recognition.
- Reasons for data collection must be explained and publicly announced in clear, generally understandable language. Notification must be available in a central repository and at the site of collection.
- The method of data collection, storage location and duration of resulting data, and instructions for redress must also be shared.
As individuals and related communities, we have the right to be forgotten.

- When data is collected, it cannot be kept in perpetuity. Unless proactively consented to data provided consensually, must be destroyed within a reasonable timespan. One week could be defined as “reasonable.”
- The burden to forget is the responsibility of the organizations, governments or persons collecting the data. This right to be forgotten must be written into the original code/system and enacted automatically on a preordained schedule.

As individuals and related communities, we require that government use of biometric data, and A.I. more generally, will not be obfuscated or laundered through the use of non-governmental organizations.

For example, if the United States employs Amazon to develop broad surveillance, they are not absolved because it was a contractor the did the work. Likewise, if the police purchase data sets from a phone company, the police should be bound by all rules as if they were obtaining the information themselves.

As individuals and related communities, we require that algorithms and datasets used to support biometric systems must be transparent. All A.I. used on any public must utilize datasets that reflect the public (with respect to demographics, such as gender and race) on which it will be used to train the A.I.

As individuals and related communities, we require that consent to provide biometric data not be coerced as a condition of usage of a product, service or technology.

**Privacy & Redress**

As individuals and related communities, we require that biometric data created by personal technologies such as wearable sensors, mobile phones, home-based care and communications technologies and bodily implants may not be accessed, used without consent, or triangulated with data from other sources.
As individuals and related communities, we require that biometric data collected about them will not be used in research without consent. When consented to profit-sharing, arrangements must be made.

**Accountability**

As individuals and related communities, we require that companies and government agencies that deploy A.I. be held accountable for any bias or discrimination which results from the use of the A.I., as if it were done by a human being.

An example, if a bank uses A.I. to determine lending policy and the policy ends up discriminating based on race, the bank would be as liable if the lending decisions were made by people. Or if a manufacturer of self-driving cars deploys systems that do not recognize Black pedestrians at the same rate as white pedestrians, they will be liable for civil rights violations in addition to any other penalties that arise from this design flaw.

As individuals and related communities, we require those who are not US citizens, mbe granted the same rights with regard to A.I. as US citizens.

For example, if US airline companies rely on A.I. (either their own or governmental) to deny passage of a Nigerian citizen, that person should be able to challenge the denial and have access to review the algorithm and/or dataset that led to their denial.

As individuals and related communities, we require all uses of A.I. by the military should be subject to review by citizens with no ties to the military.

**Checks and balances & Trust**

As individuals and related communities, we require both human and automated checks and balances of computational surveillance and decision-making systems. Checks and balances must be enacted regularly and keep pace with the speed of technological advancement.
As individuals and related communities, we require that the public (or public representatives) have the right to review and analyze the algorithms underlying biometric technologies and algorithmic systems more generally. Datasets used to train any machine learning system must also be made available for review, augmentation and edit.

As individuals and related communities, we require that an organization akin to the FDA or CDC, be created to guide the development of biometric systems and provide centralized oversight.

Individuals, communities, and autonomous entities require public and private entities to collect biometric data to use blockchain or other traceable technologies to track and engender trust in the process of data collection and disposal.

As individuals and related communities, we require that the government is not permitted to deploy A.I. for purposes that would either be illegal or impossible for unaided human analysis.

As individuals and related communities, we require A.I. systems be regularly audited for historical and contemporary biases. Proof of audit and transparency of the process must be publicly available.

**Profiling through Data**

As individuals and related communities, we require that their biometric data never be aggregated into a composite portrait created from data collected from multiple collection sites.

As individuals and related communities, we have the right to fact-check and edit the story aggregate data tells about them.

As individuals and related communities, we have the right to legal and monetary recourse for personal information inferred and divulged from aggregated data without consent.
As individuals and related communities, we require that government institutions and agencies not be able to obtain, store or cross-reference personal information which they would not otherwise be able to keep, access or cross-reference.

For example, people coming to a lecture at a university can reasonably assume anonymity and expect not to be surveilled by the police. With facial recognition technology crossed with access to driver's license photos, the technology exists for the government to compile lists of most attendees.

**Monetization and Profit Sharing**

As individuals and related communities, we require that biometric data collected about them not be monetized or otherwise used for profit in public, private or governmental spheres.

As individuals and related communities, we require that biometric data collected about us will not be used in research without consent. When consented to, profit-sharing arrangements must be made.

**Care**

As individuals and related communities, we require biometric systems to resist the hyper-rational, binary lens of efficiency and profit in favor of technological ecologies, to care for individual entities and communities while encouraging complexity, plurality, and generosity in our data-centric ecosystems.

As individuals and related communities, we require our A.I. ecosystems, inclusive of biometrics, to be infused with a diversity of nuanced values, beliefs and representations toward the equitable distribution of resources and mutually beneficial systems of care.

As individuals and related communities, we require that biometric systems be developed with the understanding that the boundaries between sovereign consciousness, nature, power, and social reality are shifting. Our A.I. ecosystems must be developed, planned, and deployed with these ideas at the forefront.
As individuals and related communities, we require our A.I. ecosystems, inclusive of biometrics, be developed, carefully administered, and deployed to support and care for global society instead of being ruled by fear and the pursuit of profit.

EPILOGUE

Mutations, adaptations, genetic drift, hybridity, and other mechanisms allow life to explore the landscape of possibilities. Life folds back on itself in an evolution of evolution: the first cells replicated by fission; but eventually developed sexual reproduction, which vastly accelerated evolutions’ landscape exploration. Human physical labor similarly folds nature back on itself, as Marx pointed out. Expressive (i.e. semiotic; informational) value is the means by which culture can pass on adaptations without waiting for genetics: language, writing, and technology. And in its most recent recursive turn, machine intelligence folds human culture back on itself. The idea that it too contains a fundamental creativity—that A.I. will explore its own space of possibilities—means that it is all the more urgent to map out evolutionary trajectories for generative justice and ensure they are deeply embedded in these new algorithmic regimes from the start.

See Evolving Systems for Generative Justice: Decolonial Approaches to the Cosmolocal.


–Ron Eglash, Professor, Stamps School of Art & Design/ Professor, School of Information, and Audrey Bennett, Professor, Stamps School of Art & Design, University of Michigan