Response to RFI on Public and Private Sector Uses of Biometric Technologies

Written by: David Danks (University of California, San Diego), Maria Gini (University of Minnesota), Odest Chadwicke Jenkins (University of Michigan), Daniel Lopresti (CCC and Lehigh University), Melanie Mitchell (Santa Fe Institute) and Katie Siek (Indiana University, Bloomington)

1. Descriptions of use of biometric information for recognition and inference: Information about planned, developed, or deployed uses of biometric information, including where possible any relevant dimensions of the context in which the information is being used or may be used, any stated goals of use, the nature and source of the data used, the deployment status (e.g., past, current, or planned deployment) and, if applicable, the impacted communities.

The characterization of "biometric technology" is incredibly broad. There are many current uses of technology that seemingly qualify as biometric on this definition, but that we believe should not qualify. Parties are strongly encouraged to consider the convergence of data streams that create biometric knowledge. For example, a cognitive tutor (or similar EdTech system) arguably counts since it uses behavior (= student responses) to infer cognitive state (= subject knowledge). More contentiously, the recommendation engine underlying Amazon counts as biometric technology since it uses behavior (= user search terms & clicks) to infer cognitive state (= preferences).

Parties are also encouraged to consider how technology that is typically not utilized for biometrics can be harnessed to abstract similar biometric knowledge. For example, in smart homes for older adults, researchers determined that it was easier to use an ultrasonic sensor in a doorway to identify people instead of a gait sensor because the ultrasonic sensor could detect a person's height with the assumption that people with varying heights live together.

We don't think that NIST has these kinds of uses in mind, as the example behaviors are all physical ones and the example cognitive and/or emotional states are all highly effective ones. But we do believe that they are focused on what most people would consider "biometric technology" when the actual definitions that they give is much broader leading to a counterproductive definition.

[1] This material is based upon work supported by the National Science Foundation under Grant No. 1734706. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

2. Procedures for and results of data-driven and scientific validation of biometric technologies: Information about planned or in-use validation procedures and resulting validation outcomes for biometric technologies designed to ensure that the system outcomes are scientifically valid, including specific measures of validity and accuracy, resulting error rates, and descriptions of the specific measurement setup and data used for validation. Information on user experience research, impact assessment, or other evaluation of the efficacy of biometric technologies when deployed in a specific societal context is also welcome.

Existing practice in academia for publishing new research has generally involved testing on standard datasets that were collected when there was far less awareness about the serious privacy and ethical issues. The community depends on these datasets, and it's not clear whether it is broadly accepted that past practices are wrong and need to be changed. Already better benchmark datasets (most obviously, the dataset built by the Gender Shades project), have been developed but the community hasn't shifted to using those datasets. It will be extremely disruptive to tell researchers they can no longer use datasets they've been depending on for years. This could slow down the careers of young faculty members, and could delay the graduation of PhD students, but the transition has to happen and it seems likely government support will be needed to help facilitate this.

The entire community, including journal publishers and conference organizers, need to come together to map a way forward. Even measuring the amount of work it will take to transition the community to new datasets that meet the new ethical standards is going to be a challenge -- someone needs to do this work, and someone needs to fund it. Beyond this, there is also the question of which biometrics are appropriate to develop, and which are not (e.g., facial recognition, at least the way it's practiced now). In addition, evaluation needs to go beyond the current narrow focus which is entirely technical ("this method is 1% better than that method") and directly include the ethical issues -- datasets and evaluation measures need to be transparent and fair, and be calibrated to identify potential risks and damages. Researchers don't have the ability to control every use of the technology that they build, but there needs to be an increased effort to identify likely (or "easy") real-world uses of the system, since that is what really matters. Systems that perform well in the lab might predictably fail in the real-world, and researchers should bear some responsibility for thinking about "obvious" misuses.

Human computer interaction researchers investigated biometrics for emotional state awareness acceptance through wizard of oz studies and small pilot studies. Researchers utilized facial recognition during clinical encounters to help healthcare providers understand “non-verbal cues” of their patients - especially when providing difficult news. They found that healthcare providers appreciated viewing the emotional sensed data ambiently and reminded them to listen better, but some were concerned it may take their concentration away from their patients. Researchers created intervention applications with facial recognition for emotion detection for people with autism. The pilot studies are small because they are technology feasibility studies, however support

for creating more robust systems that can support larger studies are needed to understand the *in-situ* efficacy of these systems.

3. *Security considerations associated with a particular biometric technology. Information about validation of the security of a biometric technology, or known vulnerabilities (such as spoofing or access breaches). Information on exhibited or potential leaks of personally identifying information via the exploitation of the biometric technology, its vulnerabilities, or changes to the context in which it is used. Information on security safeguards that have been proven to be efficacious for stakeholders including industry, researchers, end users, and impacted communities.*

There has already been some work in the security community on biometric technology, but one research area from this domain that deserves more attention is the creation and use of fake biometric data, which could be more dangerous than fake information. Particularly with regards to adversarial attacks that do not directly compromise the hardware (e.g., wearing glasses with particular patterns to deceive a face recognition system). There aren't many folks in the security community really thinking about these attacks and there are concerns about whether the Machine Learning researchers fully understand the security worries. Interestingly, there is a gap between the security community (which tends to be paranoid and worst-case) and the pattern recognition / machine learning community which develops and tests biometrics (which tends to be optimistic and average-case). The two research areas need to work closely together to achieve the proper equilibrium between the differing attitudes when developing and evaluating biometrics; government funding could help with this as well.

4. *Exhibited and potential harms of a particular biometric technology: Consider harms including but not limited to: Harms due to questions about the validity of the science used in the system to generate the biometric data or due to questions about the inference process; harms due to disparities in effectiveness of the system for different demographic groups; harms due to limiting access to equal opportunity, as a pretext for selective profiling, or as a form of harassment; harms due to the technology being built for use in a specific context and then deployed in another context or used contrary to product specifications; or harms due to a lack of privacy and the surveillance infrastructure associated with the use of the system. Information on evidence of harm (in the case of an exhibited harm) or projections, research, or relevant historical evidence (in the case of potential harms) is also welcome.*

There are a couple different facets to consider when viewing this problem. Some of this seems to be a matter of education. Researchers generally know when to trust and not trust a certain biometric, but those actually using biometrics in the field may place far too much trust in them and have no understanding at all of their failure modes. That can be very dangerous to society. Biometrics are also easily abused: developed for one specific purpose and validated in that context, but then applied for another purpose that may seem similar, but where there are significant differences that make the biometric inappropriate. When used for identification purposes, there may be false presumptions of uniqueness based on “conventional wisdom” as opposed to science. For example, in

the early stages of DNA fingerprinting there were overly broad statistical assumptions about uniqueness that had not yet been proved because not enough real-world data had been collected yet. This resulted in people being identified with an extremely high probability of having committed a certain crime. Juries can't understand the intricacies of statistics. It's unlikely that individual researchers will have data that is both broad enough and deep enough to understand the impacts on "edge cases" -- in this case, individuals or groups who are highly underrepresented in their data. There are huge questions that are hard to answer, such as who decides what margins of error are acceptable? And what recourse do individuals have when biometrics make an error that harms them? While questions such as these are basically impossible for individual researchers to answer, there is more that researchers can be doing to mitigate the risks. Researchers can't prevent all misuse, but they could potentially build into their system a "check" of whether the input had been significantly modified in various ways, and simply refuse to run on heavily manipulated images or video.

In addition, using biometric data for emotional inference is problematic and potentially harmful because the definition of specific emotions is based on the developers' interpretation, cultural norms, and the data set used. A cultural example would be nodding one's head from side to side - which may mean they disagree in some cultures, but in others it may mean they agree. An accessibility example would be someone with autism spectrum disorder not showing emotions as would be expected and thus a system misinterpreting their biometrics. Systems would need to process multiple and sometimes private data streams from an individual to appropriately interpret an individual's emotions, however this could introduce more privacy issues and personal harms.

6a. *Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case: Information regarding stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies;*

Some individual researchers are working with stakeholder groups to tackle this issue, but it is usually to understand the needs of the biometric tech *owners/users*, rather than the needs of the *targets* of the biometric tech. There is a question of whether these engagement processes should/could lead to realization that a type of biometric tech ought not be researched or built? While it is impossible to prevent research on specific topics, certain biometric technologies could be forbidden by law. All industries and researchers engaging in biometric data and inference systems should have a compensated advisory board of public members (researchers, stakeholders including target users and humans who generate the data streams) who review upcoming studies, technologies, data, and discuss the implications. The industries and researchers should have to publicly respond to concerns of the advisory board. In addition, the associated research communities should also develop their own "ethics boards" who are well-versed in such issues, but this may prove challenging for organizations that are largely organized and run by volunteers.

Finally, federal funding agencies who fund biometric research and industry members who create biometric technologies should organize a unified, compensated review board that meets annually to review biometric research and technology developed and deployed to see if these types of systems are beneficial to society and potential harms and make recommendations to the relevant parties including federal policy makers.

6c. *Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices;*

Likewise, it will be important to investigate the current standard practices of the research communities who collect and use standard datasets for developing new biometrics. As noted earlier, support will likely be necessary to help research communities to transition away from their existing datasets to new datasets that are more fair and less biased. Many of the other important issues mentioned here (disclosure, consent, review, security, sharing, storage, monitoring) fall on volunteers who are already overburdened and will probably require funding support to transition to better practices.

Biometrics are data from individuals - individuals who have limited bargaining power over the value of their data. We must rethink how individuals' data is collected, used, shared, and distributed to not only ensure there are no harms, but also to negotiate with industries on the use and financial gains of this personal data. The Computing Community Consortium (CCC) wrote a whitepaper in regards to this topic - Modernizing Data Control: Making Personal Digital Data Mutually Beneficial for Citizens and Industry.