This document was produced based on notes taken during the Biometric Technologies in Policing workshop of the Data & Civil Rights conference. This document represents a general summary of the discussion that took place. Not all attendees were involved in every part of the conversation, nor does this document necessarily reflect the views and beliefs of individual attendees. All workshop participants received workshop materials prior to the event to spark discussion. The primer can be found at: http://www.datacivilrights.org/pubs/2015-1027/Biometrics_Primer.pdf

Workshop Discussion Notes: Biometric Technologies in Policing

Overview

This workshop gathered individuals drawn from law enforcement, social justice movements, technology companies, academia and government to discuss the usages and effects of biometric data collection, biometric databases, and legal and privacy concerns over biometric usages by law enforcement and in judicial proceedings, as well as parallel developments in commercial and private settings. The conversation had a broad focus. Biometrics refers to the types of bio-markers, such as DNA, that are associated with specific individuals, as well as to a range of technological tools used for biometrics collection and analysis, and these tools can be applied to a wide range of applications and goals. Among the participants, a number of concerns were shared over the current and future use of biometric techniques. Primary among these was a consideration of inequality or disparate impact that such technologies might produce. The workshop was also concerned with current inaccuracies in biometric work, the complicated provenance (military, commercial, otherwise) of biometric tools, as well as the "mission creep" of biometrics in public or civil applications. After performing introductions and allowing participants to highlight key areas of concern, the session was divided into a discussion of two themes: 1) the design/development of biometric tools, and 2) the social and cultural impact of biometrics.

Design and Development

One of the largest challenges in discussing the design of biometric tools is that these tools are quite often designed in one context before migrating to another. Numerous tools have been designed for explicit military use, before being imported for civilian use. The same tools intended for enemy combatants can become the basis of criminal justice applications, which must necessarily have a different set of design values. Even within individual institutions, tools developed for one application can frequently be used for additional purposes. One participant described a DMV system which used facial recognition to fight identity theft; this system could also be adapted to the distribution of government benefits. Another participant described Iceland's collection of genetic information from its population and pointed out:

biometric data like gait recognition can be used to diagnose health issues, but can also become the basis for stereotyping or prejudice.
That many biometric tools are developed by 3rd party vendors can produce another point of vulnerability. Different tools for different spheres (state, commercial, military) might be developed using the same underlying techniques and data structure. This similarity can make it all the easier to combine and cross reference data from these otherwise separate data streams – one of the greatest threats to conditions of anonymity or privacy. Such a weakness, several steps removed from the site of the technology's design, prompts a consideration of the relationship between design and justice. Can justice be baked into (or *out* of) a technology's design? And if so, how do we know what definitions of "justice" are currently being designed for, and how is the relative success of that design being measured?

Answering questions about design values also requires a consideration of biometric ownership and privacy more generally. What happens when we think of biometric data as being the property of the individual that produces it? Participants argued that such an "ownership" model of biometrics was ineffective, and that biometric concerns must always be rendered across a group, population, or network. Privileging the autonomy of the individual decision above all else might not actually be the best way to get to biometrics that produce good rather than harm.

One possibility for improving the design of biometric tools is that an FDA-like organization could work at the federal level to mandate a level of "healthy" impact for biometric technologies. Intervening at the level of design may only be half the battle, as the implementations of the tools may end up far from the original or intended context. As it stands, too many implementers or decision makers have little to no understanding of the inner workings or broad impacts of individual biometric tools and this would have to be changed before current systems are further developed and implemented. Ultimately, this will require an expanded conversation about the changes wrought by biometrics to conditions of privacy. What, for instance, is the status of abandoned DNA? Should its collection be constituted a search? A theft? Furthermore, can such questions be re-articulated away from the discourse of law enforcement and toward the issue of public health?

Social and Cultural Impact

The current state of biometric use implies a number of possible future impacts about which participants were concerned. As data becomes more standardized and interoperable it becomes more useful, but also more powerful and more capable of escaping its intended application. This can become the condition for harm to surveilled communities – communities which, if current evidence is any indication, are most likely to be low-income communities of color.

One large challenge to curbing the negative social impacts of biometrics is the way that early adopted technologies and tools can become ingrained in institutions. The data formats adopted by law enforcement agencies can quickly become de facto standards, and the norms surrounding appropriate use of biometrics

can quickly become the basis for legislation or regulation. Thus, any intervention into the use and reception of biometrics must be made at the same rate as the new technologies' adoption. Specifically, some means must be found to intervene between biometric tools and low-income or minority communities. It is these communities, often least equipped to parse or combat violations of their rights which fund (through tickets, fines, and sanctions) the biometric programs that are meant as the models for national adoption. Many of the activist organizations or movements within these communities – take Black Lives Matter, for instance – do not make issues of new surveillance serious areas of advocacy. The naturalization of surveillance – *the man is listening* – more often takes the form of jokes or clichés.

On the other end of the spectrum, many powerful or public figures are pro-data without a strong understanding of the technology or impact they support. The Department of Justice is instrumental in this phenomenon. One the one hand, they are currently liberal and proactive in shaping policy on privacy and biometric data collection. On the other hand, they are still fundamentally pro-data, appearing to operate under the assumption that these tools *will* be used in the future, but what remains is to set limits and norms on this use.

The DOJ, for instance, has acknowledged that law enforcement must be trained in the discriminatory nature of data tools and the possibility of baking justice and privacy into the design of their systems. However, whether this can be accomplished remains to be seen, as the very fundamental purpose of surveillance tools would seem to contradict a support of privacy. In addition, the current landscape of surveillance is quite distant from traditional legislation of privacy – the Wiretap Act of 1968, for instance, would seem to disqualify most of what is currently done with biometric tools.

In the end, the norms, rules, and regulations of law enforcement function as a type of "world building." These steps contribute to what society sees as normal, acceptable, and desirable. This leads the group to wonder how differing expectations of privacy will attach themselves to different identity groups (upper-class vs lower-class, white vs minority). What might a biometric "stop and frisk" look like? And what would be an appropriate response to such a system? To answer such questions would require the increased participation of more groups from more diverse backgrounds – perhaps a taskforce of sorts, that could evaluate technologies and ratify their use.

Conclusions

Having approached biometrics from two areas of concern (design and impact), the workshop participants collaborated on a summarized set of concerns and conclusions before imagining 1) the best possible applications of biometrics, and 2) the actionable items that could be taken forward from the workshop.

It is clear that the development of biometric technologies is always different from those technologies' actual application. Understanding just how far these technologies can drift will be important in identifying and assessing their possible uses. As much as possible, these uses should be imagined and shifted toward public

health concerns above criminal justice applications, and those charged with applying them to criminal justice (judges, etc.) must be far better equipped to understand their impact.

The impact of biometrics on society must also be understood to unduly effect vulnerable populations. Allowing technology to develop now that creates or deepens social disparities can lead to damaging future technologies. By testing biometric tools in the least privileged communities, and by attaching them to public goods or other civil services, we risk creating the worst possible model for biometrics – unfair, coercive, pervasive. What remains to be seen is whether a privileging of "privacy" will be enough to combat these risks.

Best Case Future Scenario. What might a positive version of biometric systems look like? It would need to have a mutually informed public and private stakeholders capable of having a conversation about biometrics. It would have a considerably slowed rate of biometric tool adoption to allow for unintended consequences prior to any particular roll out. The DOJ advisory community on forensic science would serve as a model for the study and consideration of biometrics. New regulatory and statutory frameworks would need to be implements at both state and federal levels. These frameworks would have to be based on a new understanding the civil rights issues involved – one that goes beyond "the right to privacy" as the guiding principle. Though, at the same time, a right to Informational Privacy would need to be established as en explicit and universal right. Finally, where biometrics were being used, systems would need to be transparent to allow for monitoring and oversight.

Action Items. Courts need to be leveraged as legal recourse for limitless biometrics collection. Hyper-visible public stunts need to be arranged to start and shape public discussion. Statutory restrictions need to be pursued and passed. The discourse on biometrics needs to be moved toward expanded privacy expectations (see Riley v. California). 4th Amendment jurisprudence needs to be improved. States need to be held accountable for new biometric systems. The interplay between biometric data sets needs to be brought into the discussion. Formal "walls" need to be set up between commercial and law enforcement data collection. Strong opt-out policies need to be enforced. The implicit conflict between open access enthusiasts and privacy advocates needs to be acknowledged and resolved. The fundamental right to privacy needs to be weighed against the range of government interests.