Biometric Technologies in Policing

Biometric technologies are rapidly finding use in a variety of policing contexts, and their use is expected to grow as these technologies become more accurate, cost-effective and accessible to law enforcement agencies. Since 2008, the FBI has been assembling a new biometrics database, the Next Generation Identification system (NGI), since 2008. This $1 billion program will combine fingerprints, iris scans, facial recognition, voice data and other biometrics into a multimodal database, greatly expanding the amount of data searchable by federal and state agencies. Other existing biometric databases such as the National DNA Index System may be interoperable with this system. At the same time, new technologies, as well as new laws and regulations, have widened the conditions under which law enforcement agencies can collect, store, and share biometric data.

- Biometrics are markers used to identify or verify the identity of individuals and are based on unique and measurable biological or behavioral characteristics. In law enforcement, the most common biometric data have been fingerprints and DNA. Other biometric markers, such as iris scans, facial recognition, voiceprints, and hand geometry, are starting to play a larger role in law enforcement.
- State and federal biometric databases are expanding rapidly. In 2014, it was reported that the FBI had planned to grow the number of photos in the NGI from 24 to 52 million by 2015. States are tapping into the FBI facial recognition system and developing their own, sometimes accessing drivers' license photos.
- New technologies – long-range iris scanners and mobile facial recognition technology – have increased the capability of officers to identify individuals in real-time. As databases expand and become more inclusive, a greater number of individuals could be identified more easily through these and similar practices.
- Amendments made to state and federal laws, supported by *Maryland v. King*, have widened the conditions under which police officers can collect DNA from suspects. Presently, no court precedent limits facial recognition.
- There are few non-technical barriers for government agencies to share biometric data with each other. Additionally, law enforcement has sometimes gained access to privately held biometric data such as genetic data held by Ancestry.com or 23andMe.
- Civil rights advocates are concerned about the implications of biometric databases for marginalized communities, who are overrepresented in biometrics databases and may be disproportionately impacted by practices like "familial matching," wherein suspects without DNA on record are found through searches for partial matches of family members.
- Biometric data also plays a role in adjudication, where it may be perceived as more accurate than it is in practice. Evidence shows that factors such as traveling DNA (wherein DNA is carried to other places through other people, objects or environmental factors) and degraded samples can lead to "false positives."

Critical Questions

- What forms of oversight and regulation should be introduced into the development and deployment of biometric systems by law enforcement?
- Does collecting biometric data contribute to inequality within the criminal justice system? Are some groups targeted more than others for data collection?
- We are seeing a much broader collection and use of biometrics for non-criminal justice purposes – from background checks to immigration. Should we try to create limitations around how that information becomes part of the criminal justice system?
- How can we ensure greater transparency in the sharing of biometric data between government agencies or between private companies and government?
- How will biometrics data collection fit into a broader system of institutionalized surveillance? What are the potential psychological and social harms of biometric collection to particular communities being targeted?
- Because biometrics are immutable do they create specal security risks? Should we consider limitations on how the how we hold biometrics to mitigate this risk?
- Should different biometrics be regulated differently? Face recognition raises different issues than DNA – does it even make sense to lump them together?
- How concerned should we be with errors in biometric databases and analyses, and how should we address them in law and practice?
- What limits should be in place to regulate how law enforcement accesses the biometric data collected or stored by private companies?

Data&Society The Leadership Conference Upturn