Biometric Technologies in Policing

10.27.2015

ROBYN CAPLAN, IFEOMA AJUNWA, ALEX ROSENBLAT, and DANAH BOYD

Introduction[1]

Over the last decade and a half, the use of biometric technologies in policing has increased, and continues to grow. The Federal Bureau of Investigation has been in the process of creating a new biometrics database, the Next Generation Identification system (NGI) since 2008.[2] This $1 billion program, designed by defense contractor Lockheed Martin, will combine data like fingerprints, iris scans, photographs, and voice data into a searchable platform for use by federal and state agencies.[3] The FBI and the Department of Defense have also worked together in the development of the Biometric Center of Excellence (BCOE) in Clarksburg, West Virginia, which will combine the two agencies' research.[4] Biometric data is being collected by law enforcement with greater frequency and is being stored for longer periods of time, and technical and legal infrastructures are being developed or adapted to make data sharing and searching more streamlined between local, state, and federal agencies. As data collection and analysis becomes easier to do on a large scale, questions emerge about whether biometric databases should be governed in ways that anticipate future civil liberties and civil rights concerns.

At the local level, states and individual police departments are using biometric technologies in policing with greater frequency, and with little public oversight. Investigations by the Center for Investigative Reporting and the Electronic Frontier Foundation have detailed how facial recognition software used previously by the U.S. military and intelligence agencies in Iraq and Afghanistan, is now being used in San Diego to identify individuals suspected of a crime in real-time. Using the new Tactical Identification System, a mobile facial recognition technology, officers are able to snap photos of suspects using their mobile phones and search within existing criminal databases for their profiles.[5]

Biometric technologies, such as fingerprinting and DNA matching, have played a large role in policing over the last century, and biometric technologies, including those developed to fight terrorist threats, are being used domestically for purposes of law enforcement. Additionally, advances in computing have led to a wider variety of mobile DNA and other biometric data collection devices, as well as more cost-efficient solutions for storing and sharing biometric data between agencies and organizations. This rapid uptick in the development and deployment of

biometric systems in policing without oversight or regulation has led to concerns about potential abuses or misuses of such information. As individuals are entered into federal and state biometric databases – whether they have had an encounter with the criminal justice system or not – the vast expansion of biometric databases have also raised questions about the ease with which any individual can come under the auspices of the U.S. criminal justice system.

The benefits and harms of biometric data collection and usage have an evolving impact on criminal investigations and prosecutions. Biometric data – in particular DNA – may help identify those present at the scene of a crime, but it also can play a role in proving the innocence of the wrongly accused. The Innocence Protection Act, as well as non-profit organizations like The Innocence Project based out of Cardozo Law School which support the Act's aims, allow for post-conviction appeals through the use of DNA testing. The advancement of biometric testing technologies facilitates the introduction of new DNA evidence not detectable by past technologies, which has resulted in several successful attempts to appeal convictions.[6] At the same time, DNA can implicate individuals in crimes they may not have committed, or expose family members to a judicial system that could see them as suspect by virtue of their DNA's relation to that found at the scene of a crime.

What are biometrics?

Biometrics are markers used to identify or verify the identity of individuals, and are based on unique and measurable biological or behavioral characteristics.[7] Within law enforcement, the most common form of biometric data collected is fingerprints, which have been used over the last century and a half both to identify suspects and to archive individuals and their records within the criminal justice system. DNA evidence was first used in the 1980s in England and became more commonly used within forensics in the United States in the 1990s. Other biometric markers, such as facial recognition, retina scans, voiceprints, and hand geometry, have begun to play a larger role in law enforcement more recently.[8]

Recent federal and state biometrics programs are combining biometrics into "multimodal databases," which aggregate several forms (or modalities) of biometric data, such as fingerprints, photos, DNA, and iris scans (among others).[9] The FBI's NGI System is an example of one of these multimodal biometrics database, and currently contains nearly 125 million criminal and non-criminal fingerprints, as well as 24 million mug shots.[10] In 2014, the FBI announced a plan to accelerate the collection of biometric data, and have claimed that, as technology progresses, they will be able analyze anything, from a suspect's scars and tattoos, to their voice and eyes.[11] Any individual who is in the database – criminal and non-criminal alike – is given a Universal Control Number (UCN) to link these data points. The FBI has discussed assigning all individuals in the NGI a unique identifying number that could link data to DNA profiles held in the National DNA

Index System (NDIS), the national DNA database that holds DNA profiles contributed by federal, state, and local participating forensic laboratories.[12]

Biometric systems being deployed by law enforcement agencies extract biometric data from individuals through a variety of methods, such as cameras, fingerprint scanners, and DNA analyzers.[13] New data collection methods, once used by the U.S. military to fight wars abroad, may provide police with a greater capacity to collect biometric data surreptitiously and unobtrusively. For instance, long-range iris scanners – some of which can grab an image from as far as 40 feet away – are currently being tested for use by local law enforcement agencies.[14]

Expanding Biometric Databases

Debates about the potential harms and benefits of biometric data collection by police often center on the rapid expansion of federal and state databases, as well as the widening of the criteria for inclusion and length of time the data is being stored. Collection of biometric data is not restricted to any one government agency, and is occurring at the local and state level, as well as through federal agencies such as the Department of Homeland Security, FBI, DEA, NSA, TSA and others, as well as through private companies. Data is also increasingly being shared between these different levels of government, and between agencies. Technical and legal barriers to making biometric data shareable and interoperable, are disappearing through the implementation of new database technologies, regulations, and data sharing relationships.

Photos and fingerprints are inputted into the FBI's NGI database through a variety of channels, and individuals could find they have a presence in a criminal justice database whether they have had a direct encounter with law enforcement or not. The FBI developed the NGI, in part, as a way to retain civil fingerprint submissions, along with accompanying biographic data, into an identity record.[15] The FBI has noted the benefit of retaining these civil fingerprints alongside the criminal database is that it provides an "'ongoing' background check that permits employers, licensors, and other authorized individuals to learn of criminal conduct by a trusted individual."[16] This data is then accessible to the Department of Justice, state, local and tribal agencies, as well as federal entities.

The advancement of biometric programs has given rise to concerns about the conditions under which an individual's biometric data can or should be entered into these databases. Depending on the state, biometric data, including DNA, can be collected at different moments of someone's entry into the criminal justice system, with some states allowing data collection at the moment one becomes a suspect and others waiting until an individual has been charged or convicted of a crime.[17] States vary at the type of offence that can warrant data collection – misdemeanors, felonies, or violent felonies – and whether biometric data, such as facial photos, taken for non-law enforcement purposes, can be made searchable for law enforcement purposes. The result of these

expanding criteria is that biometric databases are rapidly expanding both federally and within states.

For instance, the FBI's NGI system is growing faster than originally projected. Though estimates report the number of photos in the system at approximately 24 million, reports from 2014 said the FBI had planned to grow this number to 52 million by 2015.[18] Many states are already participating in the NGI, or are making their databases interoperable to make data sharing easier and more efficient. Los Angeles County is building a new "multimodal biometric identification system" which would be the largest biometric repository outside the FBI, holding records on up to 15 million individuals. Other states, like Michigan and Maryland signed Memoranda Of Understandings with the FBI to share and access facial recognition data through the NGI, and all states are participating through sharing fingerprints.

States expanding their biometric data collection programs are widening the criteria for whose DNA or other biometric data will be entered into state and federal databases. The Supreme Court ruling Maryland v. King, extended the conditions under which police officers could collect DNA from suspects not-yet-charged or convicted.[19] For instance, Rhode Island has a new DNA sampling law (2014) for violent crimes which now requires that anyone arrested for a violent crime must provide a DNA sample to police, though the sample will not be placed in a statewide database until the accused is arraigned, or if they fail to appear for an initial court hearing. Prior to Maryland v. King, courts in Rhode Island held that DNA could only be collected from those convicted of a crime. Almost all states are collecting DNA from at least some arrestees, while some states, such as California, have been challenging the practice by appealing to their state constitutions.

Law enforcement groups are also implementing programs to collect as much data as possible during routine policing work. For example, in towns like Orange County in Los Angeles, California, police are asking suspects to turn over genetic information as a bargaining chip in exchange for reduced charges or dismissal of charges. This practice, known colloquially as "spit and acquit" is being used to expand biometric databases.[20] Suspects provide a sample – an oral DNA swab – which goes into a database maintained by Orange County (currently separate from the FBI's). The "spit and acquit" program has so far been limited to drug cases involving possession for personal use charges.[21]

Any biometric data that is collected from the scene of a crime (or that exists as part of a cold case) is then compared to data already existing within a database. A sample need not be an exact match to the database to implicate an individual – and is rarely so.[22] Larger databases make these technologies more effective, as their power rests in the capacity of law enforcement to use biometric data to make a 'match' to solve existing or cold cases. Because citizens acting within the law are not required to submit their DNA, fingerprints, or iris images to the State, this need to match images with existing stored data creates an incentive to greatly expand biometric databases

to include as many people – citizens and foreigners – as possible. The desire to have as much data as possible also incentivizes the sharing of biometric data held by different state agencies – as well as between government and private entities.[23]

DNA and biometric data can be entered into databases accessible by law enforcement voluntarily, such as through driver's license databases, as well as for government job applications. In other cases, biometric data and DNA can be submitted to law enforcement databases voluntarily throughout the course of investigations. This is the case for missing persons cases, during which DNA will be turned over voluntarily by family members, and then entered into NDIS databases. Those accused of crimes can also submit DNA or biometric data, which can then be used to match them against an existing database. For instance, in Varriale v. State, the defendant voluntarily provided his DNA to clear him of a rape, which was then used to match him to an unsolved burglary. The Court of Appeals found that retaining the DNA and using it for other purposes (in this case a search) did not violate the defendant's Fourth Amendment rights.[24]

Limitless Data Sharing

Before 9/11, the government had practices to silo data and info within each agency. Since then, the government has enacted several measures to allow information sharing within and among federal intelligence and federal, state, and local law enforcement agencies.[25] Currently, the DHS, FBI, and Department of Defense's biometrics databases are interoperable.[26] Many states have also signed Memorandums of Understanding (MOUs) or are in discussion to sign MOUs to make their biometric data interoperable with the FBI's NGI system.[27]

Some states are analyzing their expansive, non-criminal photo databases – comprised of pictures taken for driver's licenses, for example – using facial-recognition technologies, and many allow other government agencies to search and/or request these photos. At least 26 of these states allow state, local, or federal law enforcement agencies to search — or request searches — of photo databases in an attempt to learn the identities of people considered relevant to investigations.[28] In contrast, Washington, Oregon and Minnesota, have erected legal barriers preventing police from using facial-recognition technology in their driver's-license registries. New Hampshire's legislature passed a law prohibiting motor vehicle officials from collecting any biometric data. Montana has a facial-recognition system to help prevent fraud in its drivers license registry, but officials are still debating whether to allow police any kind of access to it.

In addition to data collected by governments, there are also biometric databases being produced by private enterprises. Companies like Facebook, Google, and Apple now collect and analyze biometric data, either through photos and facial recognition software, or the more recent fingerprint scanning used to authenticate users to, for instance, access their iPhones. Companies

like 23andMe and Ancestry.com collect and store DNA data, and that data can be sold or accessed by third parties.[29]

The federal government does not appear to have formal data sharing arrangements with private companies collecting biometrics; however, there have been successful attempts by law enforcement to gain access to biometric data held privately.[30] As of right now the FBI has said that photos on social media accounts cannot be submitted to the NGI. However, law enforcement has used other channels to get access to biometric data held by companies like Facebook through appealing to the Stored Communications Act.[31] Law enforcement can gain access to biometric data held by private companies through other means. For instance, in a case in Idaho, police were able to run DNA found at a crime scene in 1996 against a database owned by Ancestry.com. After finding 41 potential familial matches, they were able to obtain a warrant to gain access to "all information including full names, date of births, and other information pertaining to the original donor."[32]

Legal Issues in Biometric Data Collection and Sharing

There are very few legal limitations on what biometric data government agencies can collect and share. In 2013, in Maryland v. King, the Supreme Court held that "when officers make an arrest supported by probable cause to hold for a serious offense and bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment."[33] The Justices concluded that biometric testing, while a suspect is in custody, meets the "reasonableness" standard of the Fourth Amendment because law enforcement has a legitimate government interest in processing and identifying arrestees and using that information to set (or deny) bail. Ultimately, the Court ruled that an arrestee's interest in keeping her biometric information private does not outweigh the legitimate government interest in obtaining that biometric information. What this means in practice is that the police can and do collect biometric information (fingerprints, as well as, DNA samples) from anyone arrested for any reason.

Data sharing between government agencies, and between government and private entities may also be justified through United States legal theory. The Third Party Doctrine has been upheld by several Supreme Court rulings, and it stands for the idea that anything that an individual has shared with another party no longer holds an expectation of privacy such that it is not a "search" (under the 4th Amendment definition) for the government to collect that information. In the 1979 decision of Smith v. Maryland, the Supreme Court noted: "this Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." The Smith ruling had as its precedent another Fourth Amendment case decided three years earlier, United States v. Miller, that involved warrantless government access of a suspect's

bank records, in which the Supreme Court ruled that bank customers possessed no standing to contest government subpoenas to access customer records.[34]

What the Third Party Doctrine means in an age of inexpensive biometrics information collection technology, is that as more individuals opt-in to share their biometric information, either with the government for immigration purposes, or with corporations, for employment purposes, that information becomes vulnerable to capture by law enforcement without the need for a search warrant. The third party doctrine remains unchallenged – although, in United States v. Jones, Justice Sotomayor recently expressed her unease with the doctrine in the context of the digital age where personal information proliferates online because we are forced, by necessity and by convenience, to reveal a large amount of information about ourselves to third parties online, or by virtue of using digital technologies such as cellular phones, such as in the case of United States v. Graham.

There are significant other concerns that emerge from this limitless data sharing. For instance, if inaccurate data is shared across databases, the wrong information will be disseminated throughout and could therefore be very difficult to correct, as it can be difficult to determine where the information came from originally.[35] This has happened, for instance, with the Secure Communities program where, according to the American Immigration Council, 3,600 United States citizens were arrested incorrectly due to "incorrect immigration records."[36] The standardization of biometrics can also eventually be used as linking identifiers – such is the case with the FBI's Universal Control Number. This creates a potential issue in the future if these identifiers get co- opted for other uses. An example of this has already been seen with social security numbers; initially created to track wages, they now serve a variety of bureaucratic functions.

Some legal scholars have expressed concern that the ruling in Maryland v. King does not provide specific and adequate constraints on how the collected biometric information may be used in the future. Those critics argue that allowing such large-scale collection of biometric information could lead to governmental abuses. For example, NYU Law Professor, Erin Murphy, notes that "almost none of the state or federal statutory regimes authorizing DNA collection" would prevent the government from testing DNA samples for a "violence gene" or "pedophile gene" and subsequently "incarcerating people based on a probabilistic predisposition to violence or pedophilia."[37] Other legal scholars, however, maintain that the Maryland v. King only allows biometric information to be used for "identification" purposes in the narrow sense, and that when "used in this manner and to provide a permanent record of an individual's identity, DNA is similar to photographs, body measurements, and fingerprints."[38] At this stage, there is too little legal precedent to be certain where the boundaries might be drawn.

The length of time biometrics are being stored within state and federal databases creates other privacy concerns. Currently, depending on the state or federal law, biometrics can be stored for as

many as 75 years or until the statute of limitations for all criminal violations has expired. Since we don't know the full capacity of technology in the future, it's unclear how far this data could travel and for what purpose.[39]

DNA as Evidence

The use of DNA as evidence within the adjudication process has had a complex legal history, which may become more complicated as the size of federal and state databases increase and contain more data from a wider array of individuals. Potential harms in the overreliance of DNA evidence by courts, such as false positives, the effects of traveling DNA, and fabrication of DNA evidence, could actually increase as DNA testing databases expand. This is due to the way that DNA evidence is used to solve crimes – either by comparing DNA taken directly from suspects to DNA found at the crime scene, or through taking biological data from a crime scene to match it to offender profiles in existing DNA databases. A wider array of potential matches within a database widens the pool of potential suspects and the possibility of false positives, providing a gap through which bias – now bolstered through scientific techniques – can enter into court systems. It is important to note that while they are highly technical, these biometric data are not irrefutable nor is the use of them infallible.

Evidence shows that biometric data, such as DNA, is subject to collection and laboratory errors and pro-prosecution bias, and is often presented in ways that may overstate scientific certainty.[40]

A number of cases illustrate the consequences false positives can have on individuals caught up in the criminal justice system. For instance, in some cases where DNA has traveled through environments – through cells and fluids – its presence has resulted in innocent people being implicated in crimes despite not being present at the scene of the crime.[41] In one case, a homeless man spent five months in prison because his DNA was found at the scene of a crime that had been committed while he was laying unconscious in a hospital.[42] Investigators eventually discovered his DNA had been transferred to the scene of a homicide through EMTs and medical equipment. In the case of DNA and fingerprints, the length of time and the condition under which biometric data is collected can also affect the strength of the match, and these degraded samples are more likely to produce false positives than if full profiles can be retrieved from the scene of a crime. The presence of data from multiple individuals can also affect the degree to which evidence can be perceived as conclusive.

When samples are degraded, experts analyzing biometric data like DNA evidence can often disagree over the results. A survey conducted by the National Institute of Standards and Technology in 2013 asked analysts from 108 labs to look at a three-person mixture and determine whether a suspect's DNA was present.[43] The study found that analysts disagreed as to whether the suspect's DNA was included in the sample, with 70% of analysts saying the suspect might be

present, 24% saying the data was inconclusive and just 6% saying the suspect's DNA was not in the sample (which was the right answer). These types of disagreements can often be used in court to cast doubt in the theories being presented by either the prosecution or the defense.

Civil Rights Concerns

The collection of biometric information from social activists, particularly those who lead the Black Lives Matter movement, has raised some alarm about the impact of biometric information collection on minorities.[44] Some scholars have noted that if databases contain a majority of biometric information from minority arrestees, since minorities are arrested at higher rates than whites, then minorities will be disproportionately impacted by practices like "familial matching."[45] A typical database search for DNA collected from a crime scene or suspect aims to find an exact match between a known person and the DNA sample, whereas familial searching merely looks for partial matches in order to discover potential relatives of the source. Some legal scholars have argued against familial matching for a variety of reasons, including those related to equality, accuracy, privacy, and racial discrimination.[46]

One proposal to counter this problem is the creation of a universal database where everyone's biometric information is collected and archived. Professor Andrea Roth has argued, "the solution, one that would avoid the severe racial inequities in current databases, maximize DNA's crime-solving power, and ensure a robust privacy debate, is a universal citizen database."[47] A major disadvantage of this suggested solution is that, given the prevalence of data breaches,[48] such a universal database of biometric information that includes genetic information could open the door for the database to be co-opted for genetic discrimination and other discriminatory practices.[49] Data breaches involving biometric data are particularly dangerous because the identifier cannot be replaced. DNA and biometric data is also discarded by us everywhere we go, leaving open the possibility that, if a match to our DNA exists within a database, we could be tracked by government entities more easily.

Law enforcement is currently capturing an ever-increasing amount of video records through police-worn body cameras, surveillance systems, and dash cameras. Although facial recognition and image detection software is not mature enough to easily identify people in this footage, these technologies are emerging and will be available shortly. This raises significant civil rights concerns about automated data collection during protests or of people who lack housing. Facial recognition technology is being deployed with greater frequency by both public and private actors, and yet there are currently no federal laws that specifically govern its use.[50] Two states, Illinois and Texas, have laws against using these technologies without informed consent – laws that have enabled individuals to bring action against companies, like Shutterfly, that use biometric technologies to analyze and identify individuals within photographs uploaded to the site.[51] These laws, however,

target commercial uses of facial recognition software. It is still unclear how government-uses of similar technologies would be treated under the law.

Critical Questions

1. How does collecting biometric data contribute to inequality within the criminal justice system? Are some groups being targeted more than others for data collection, such as through the Spit and Acquit program? Does the collection of biometrics exacerbate existing racial and ethnic disparities within the criminal justice system?

2. Should DNA samples be taken upon arrest or upon conviction? What should happen to DNA samples if a person is never charged, if a person is never convicted, or if a conviction has been overturned?

3. What are the potential risks of biometric data collection to individual privacy and security?

4. What role does biometric evidence play in the courtroom? How is biometric evidence perceived by judges and juries as opposed to other types of evidence?

5. How we can ensure greater transparency in the sharing of biometric data between government agencies (such as between health and criminal justice) or between private companies and government?

6. How broadly will databases be expanded? How many individuals are expected to be included within government biometric databases within the next ten years?

7. How will biometric databases be connected to other databases, such as social security? How might this change bureaucratic processes, like background checks?

8. How will biometric data collection fit into a broader system of institutionalized surveillance? What are the potential psychological and social harms of biometric data collection to particular communities being targeted?

9. How could biometric databases used for law enforcement potentially suffer from "mission creep" – or the use of this data for purposes otherwise not intended?

10. How might police departments use biometric data in the future in network mapping used to identify crime/criminals?

[1] We are very grateful for the strong contributions and insights made by Wilneida Negrón, David Robinson, Harlan Yu, Corrine Yu, Jennifer Lynch, Alvaro Bedoya, Alondra Nelson, Patrick Davison, and Angie Waller in the research and production of this primer.

2 "Interstate Photo System." *FBI.* Accessed October 1, 2015. https://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.
3 "Next Generation Identification." *FBI.* Accessed September 16, 2015. https://www.fbi.gov/about-us/cjis/fingerprintsbiometrics/ngi/ngi2.
4 "About the Biometric Center of Excellence." *FBI.* Accessed October 1, 2015. https://www.fbi.gov/about-us/cjis/fingerprintsbiometrics/biometric-center-of-excellence/about/about-the-biometric-center-of-excellence.
5 Winston, Ali. "Facial Recognition, Once a Battlefield Tool, Lands in San Diego County." *CircOnline.org*, November 7, 2013. http://cironline.org/reports/facial-recognition-once-battlefield-tool-lands-san-diego-county-5502.
6 United States v. Watson, 423 US 411 (Supreme Court 1975).
7 "Fingerprints & Other Biometrics." *FBI.* Accessed October 19, 2015. https://www.fbi.gov/about-us/cjis/fingerprintsbiometrics.
8 Amoore, Louise. "Biometric Borders: Governing Mobilities in the War on Terror." *Political Geography* 25, no. 3 (March 2006): 336–51. doi:10.1016/j.polgeo.2006.02.001.
9 "EPIC - EPIC v. FBI - Next Generation Identification." Accessed September 17, 2015. http://epic.org/foia/fbi/ngi/.
10 "FBI Using Facial Recognition despite Privacy Concerns." Accessed September 24, 2015. http://www.valleynewslive.com/home/headlines/FBI-using-facial-recognition-despite-privacy-concerns-311738091.html.
11 "Los Angeles Police to Widen Biometric Net." *Equal Future.* Accessed July 13, 2015. https://www.equalfuture.us/2014/10/01/la-widens-biometric-net/.
12 "CODIS and NDIS Fact Sheet." *FBI.* Accessed October 9, 2015. https://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis-and-ndis-fact-sheet.
13 "Biometrics: Frequently Asked Questions." *Electronic Frontier Foundation.* Accessed September 17, 2015. https://www.eff.org/sls/tech/87125/faq.
14 Meyer, Robinson. "Long-Range Iris Scanning Is Here." *The Atlantic.* May 13, 2015. http://www.theatlantic.com/technology/archive/2015/05/long-range-iris-scanning-is-here/393065/.
15 "Next Generation Identification (NGI) ? Retention and Searching of Noncriminal Justice Fingerprint Submissions." *FBI.* Accessed October 1, 2015. https://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.
16 "Next Generation Identification (NGI) - Retention and Searching of Noncriminal Justice Fingerprint Submissions." *FBI.* Accessed October 1, 2015. https://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.
17 "DNA Arrestee Laws." National Conference of State Legislatures, n.d. http://www.ncsl.org/research/civil-and-criminal-justice/dna-arrestee-laws.aspx.
18 "FBI Plans to Have 52 Million Photos in Its NGI Face Recognition Database by Next Year." *Electronic Frontier Foundation.* Accessed October 1, 2015. https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year.
19 "Police Praise R.I.'s New DNA Sampling Law for Violent Crimes; Civil Libertarians Say It Erodes Presumption of Innocence." *Providencejournal.com.* Accessed July 6, 2015. http://www.providencejournal.com/article/20150705/NEWS/150709632.
20 Jones, Elizabeth N. "'Spit and Acquit': Legal and Practical Ramifications of the DA's DNA Gathering Program." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, April 14, 2011. http://papers.ssrn.com/sol3/papers.cfm?abstractid=1809997.
21 Jones, Elizabeth N. "'Spit and Acquit': Legal and Practical Ramifications of the DA's DNA Gathering Program." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, April 14, 2011. http://papers.ssrn.com/sol3/papers.cfm?abstractid=1809997.
22 "Legal History of DNA Evidence." *TheFreeDictionary.com.* Accessed October 5, 2015. http://legal-dictionary.thefreedictionary.com/Legal+History+of+DNA+Evidence.
23 Cole, Simon A. "Fingerprint identification and the criminal justice system: historical lessons for the DNA debate." DNA and the criminal justice system: The technology of justice (2004): 63-90.
24 "Varriale v. State." *Justia Law.* Accessed October 3, 2015. http://law.justia.com/cases/maryland/court-of-appeals/2015/85-14.html.
25 Lynch, Jennifer. "From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, May 22, 2012. http://papers.ssrn.com/sol3/papers.cfm?abstractid=2134481.
26 Lynch, Jennifer. "From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, May 22, 2012. http://papers.ssrn.com/abstract=2134481.
27 "FBI Plans to Have 52 Million Photos in Its NGI Face Recognition Database by Next Year." *Electronic Frontier Foundation.* Accessed September 14, 2015. https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year.

[28] Timberg, Craig and Ellen Nakashima. "State Photo-ID Databases Become Troves for Police." *The Washington Post*, June 16, 2013. https://www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497story.html.

[29] For example, the terms of service for Ancestry.com permits targeted DNA-based advertising. See also: Anderson, Martin. "DNA-based advertising redefines commercial 'ad-targeting'. Sept. 16, 2015. Accessed Sept. 25, 2015, https://thestack.com/security/2015/09/16/ancestry-com-dna-advertising. and Hill, Kashmir. "Cops Are Asking Ancestry.com and 23andMe for Their Customers' DNA." *Fusion.* Accessed October 17, 2015. http://fusion.net/story/215204/law-enforcement-agencies-are-asking-ancestry-com-and-23andme-for-their-customers-dna/.

[30] Lynch, Jennifer. "From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, May 22, 2012. http://papers.ssrn.com/abstract=2134481.

[31] "FBI Plans to Have 52 Million Photos in Its NGI Face Recognition Database by Next Year." Electronic Frontier Foundation. Accessed September 14, 2015. https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year.

[32] "How Private DNA Data Led Idaho Cops on a Wild Goose Chase and Linked an Innocent Man to a 20-Year-Old Murder Case." Electronic Frontier Foundation. Accessed September 22, 2015. https://www.eff.org/deeplinks/2015/05/how-private-dna-data-led-idaho-cops-wild-goose-chase-and-linked-innocent-man-20.

[33] Maryland v. King, 133 S. Ct. 1958, 1980. Available at: http://www.supremecourt.gov/opinions/12pdf/12-207d18e.pdf.

[34] "United States v. Miller Bank Records ? Google Search." Accessed September 23, 2015. https://www.google.com/webhp?sourceid=chrome?instant&ion=1&espv=2&ie=UTF?8#q=United+States+v.+Miller+bank+records.

[35] Lynch, Jennifer. "From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, May 22, 2012. http://papers.ssrn.com/sol3/papers.cfm?abstractid=2134481.

[36] Kohli, Aarti, Peter Markowitz, and Lisa Chavez. "Secure Communities by the Numbers: An Analysis of Demographics and Due Process." The Chief Justice Earl Warren Institute on Law and Social Policy, October 2011. https://www.law.berkeley.edu/files/SecureCommunitiesbytheNumbers.pdf. ; and "Report: Biometric Data Being Collected with 'Little to No Standards, Oversight, or Transparency' | Immigration Policy Center." Accessed September 15, 2015. http://www.immigrationpolicy.org/newsroom/clip/report-biometric-data-being-collected-little-no-standards-oversight-or-transparency.

[37] Murphy, Erin. "The Supreme Court, 2012 Term — Comment: License, Registration, Cheek Swab: DNA Testing and the Divided Court," 127 Harv. L. Rev. 161, 180 (2013).

[38] Kaye, David. (2013). "Maryland v. King: Per Se Unreasonableness, the Golden Rule, and the Future of DNA Databases". Harvard Law Review Forum (2013).

[39] Eubanks, Virginia. "Los Angeles Police to Widen Biometric Net." *Equal Future.* Accessed July 13, 2015. https://www.equalfuture.us/2014/10/01/la-widens-biometric-net/.

[40] Cole, Simon A. "Fingerprint identification and the criminal justice system: historical lessons for the DNA debate." DNA and the criminal justice system: The technology of justice (2004): 63?90.

[41] Worth, Katie. "The Surprisingly Imperfect Science of DNA Testing." *Frontline.* Accessed June 26, 2015. http://stories.frontline.org/dna.

[42] Worth, Katie. "The Surprisingly Imperfect Science of DNA Testing." *Frontline.* Accessed June 26, 2015. http://stories.frontline.org/dna.

[43] Worth, Katie. "The Surprisingly Imperfect Science of DNA Testing." *Frontline.* Accessed June 26, 2015. http://stories.frontline.org/dna.

[44] Ford, Matt. "The U.S. Supreme Court Goes to Ferguson." *The Atlantic.* Aug. 11, 2015. http://www.theatlantic.com/politics/archive/2015/08/the-us-supreme-court-goes-to-ferguson/401048/.

[45] Roberts, Dorothy E., "Collateral Consequences, Genetic Surveillance, and the New Biopolitics of Race" (2011). *Howard Law Journal*, Vol. 54, Pg. 567, Spring 2011.

[46] Murphy, Erin, "Relative Doubt: Familial Searches of DNA Databases" (November 2, 2009). *Michigan Law Review*, Vol. 109, p. 291, 2010. Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstractid=1498807.

[47] Roth, Andrea L., "Maryland v. King and the Wonderful, Horrible DNA Revolution in Law Enforcement" (October 24, 2013). *Ohio State Journal of Criminal Law*, Forthcoming; UC Berkeley Public Law Research Paper No. 2344918. Available at SSRN: http://ssrn.com/abstract=2344918.

[48] Newman, Lily Hay. "The OPM Hack Compromised Five Times as Many Fingerprint Records as We Thought." *Slate*, September 23, 2015. http://www.slate.com/blogs/futuretense/2015/09/23/56millionfederalemployeeshadfingerprintrecordscompromisedinopm.html

[49] Ajunwa, Ifeoma. "Genetic Testing Meets Big Data: Torts and Contract Law Issues" (October 7, 2014). *Ohio State Law Journal,* Vol. 74, 2014. Available at SSRN: http://ssrn.com/abstract=2460891.

[50] Sobel, Ben. "Facial Recognition Technology Is Everywhere. It May Not Be Legal." *The Washington Post*, June 11, 2015. https://www.washingtonpost.com/news/the-switch/wp/2015/06/11/facial-recognition-technology-is-everywhere-it-may-not-be-legal/.

[51] Roberts, Jeff John. "Shutterfly Hit with Privacy Suit over 'Faceprints,' Use of Photos." *Fortune*, n.d. http://fortune.com/2015/06/18/shutterfly-lawsuit-facial-recognition/.