Nicholas Brown

Professor Garcia-Murillo

IST618

November 11, 2019

DNA Storage and Tracking in the Information Age

Introduction

In April 2018, local law enforcement in collaboration with the FBI arrested Joseph James DeAngelo on multiple counts of murder, rape, and burglary bringing closure to dozens of families and victims (Zhao, 2018). Dubbed 'the Golden State Killer', DeAngelo was finally being held accountable for a series of crimes dating back to the mid 1970s. Despite the collection of evidence containing DNA by government agencies at the time of the crimes, it was not until over 40 years later that collaboration between government, higher education, and the private sector enabled his capture. Investigators were able to utilize a genealogy database ran by GEDmatch in combination with DNA matching algorithms developed at Stanford University to track down DeAngelo's family members eventually pinpointing him as a relevant suspect. DeAngelo's case highlights the tremendous power that the merging of government and commercial DNA analysis services present. Though the benefits of government and private collaboration are obvious in this case, there are many situations in which people's fundamental human rights to privacy and security could be endangered as the line between government and commercial services begin to blend. Furthermore, this case shows how we have lost control over our genetic makeup as even a distant relative, like a third cousin, could provide DNA for analysis which forfeits our very **personhood** and **control** over our genetic information.

US Government DNA Collection

In 1998 the FBI launched a software platform called CODIS (Combined DNA Index System) to facilitate the comparison of DNA profiles found at crime scenes with known criminals and cases (U.S. Department of Justice, 2001). According to the FBI's CODIS Statistics webpage "CODIS contains over 14 million offender profiles, 3.7 million arrestee profiles, and nearly 1 million forensic profiles as of October 2019". The DNA data collected by both state and federal law enforcement includes people who are not only convicted, but simply arrested for a crime. In other words, nearly 3.7 million people who have been accused of a crime have been forced to give up their DNA to the US government without any due process.

Government DNA Collection Advantages

The benefits of CODIS to society are rather narrow with official sources typically highlighting only two legitimate uses. Primarily, CODIS is used to match crime scene DNA to identify suspects in a criminal case; this benefits society by increasing public safety at the cost of a criminal offender's privacy. The second use of CODIS is to help identify missing persons. For example, if a body is found which cannot be identified, DNA can be sent to a CODIS lab where it can be matched to DNA which was submitted at the time of a person's disappearance. Again, this allows members of society who have experienced loss to gain some closure.

Government DNA Collection Disadvantages

Despite the benefits to society there are multiple drawbacks to government collection of DNA. One major downside is an increase in false convictions, especially involving previous offenders. According to an article published by Rutgers University professor Kimberlee Sue Moran there is greater risk of DNA contamination as "technology has facilitated single-cell profiling meaning

that there is the potential for nearly every piece of evidence to produce a mixed profile" (2018). What this means is that a single cell from a crime scene can now be analyzed for DNA. This would have a tremendous impact on those who are in the CODIS database already. For example, if someone in CODIS touches an object in a store, and that object is then used by another party to assault someone, there will be a CODIS match and evidence to convict them simply for being near something. Indeed, this has already happened in a case known as the "Phantom of Heilbronn" where a factory worker had accidentally gotten her own DNA on evidence swabs. When these swabs were tested, her DNA was discovered at over 40 crime scenes (Gasiorowski-Denis, 2016). Contamination caused German police to believe she was an accomplice to a multitude of crimes including murder. With DNA evidence so frequently admitted in court and taken as undeniable proof, how often are people wrongly convicted?

Private DNA Collection

Today, there are two primary motivations for a person to send their data to a private DNA analysis lab. The first reason is to understand their genetic makeup to identify their ethnic heritage and any possible markers for future health conditions. This type of analysis has many benefits as one can send in a small sample and within a matter of days or weeks know if they are at risk for certain health conditions in addition to better understanding their ethnic background and heritage. This type of analysis provides the greatest amount of **secrecy** and **control** over one's DNA and the information derived from it; a stark contrast to the second motivation which is to find relatives and specific ancestors through DNA profiling. Take the case of Dr. Kenneth L. Leetz who published his experience with DNA matching services in the American Journal of Psychiatry. Kenneth's daughter had used a DNA matching service to find

relatives and ancestors when she discovered she had a half-sister. Kenneth had been an anonymous sperm donor in medical school and was now deanonymized as a child created from his donation was notified of a familial match. Kenneth had felt guilt and other "unanticipated emotions derived from choices made four decades ago with no foreknowledge of how the cloak of anonymity might be pulled away by the future technologies of the Internet and commercial DNA ancestry tests" (2018). These genetic matching services had completely revoked Dr. Leetz's **right to be left alone** amongst other fundamental privacy rights. Even worse it was not Dr. Leetz who had willing given up his DNA, it was his adult daughter who he had no legal right to keep from submitting her DNA.

Ethical Concerns

Despite appearing to be a clear-cut victory for society, the case of DeAngelo poses some serious ethical questions about the collaboration of private and government DNA databases. The most important **ethical dilemma** faced by proponents of DNA analysis is that the progress of technology allows police to catch a single murderer, it simultaneously enables mass human rights violations like genocide. The combination of private DNA ancestry analysis with government tracking databases is the perfect tool for racial or ethnic cleansing. To date the FBI has provided the CODIS software to over 50 countries (FBI, 2016). If Nazi Germany used IBM's technology to organize the genocide of millions of Jews (Dillard, 2003); could any of these countries use a combination of CODIS technology and private analysis to do the same by finding and eliminating people with certain racial marker? This is already happening in China where the Uighyr, Han, and Tibetan minorities have had their DNA collected and analyzed for racial markings. In a terrible repeat of history, it is American companies who are selling the software

and analysis to the Xinjiang and Chinese government (Wee, 2019). American's need to consider how these technologies will be used if they are to make the ethical decision on whether or not to pursue this technology.

Current Regulation and Possible Improvements

The complexity of DNA analysis means that very few people who use services like 23andMe or AncestryDNA fully understand the implications of having their DNA analyzed and placed in a database. Currently, DNA analysis services operate almost entirely under what Peter Swire calls self-regulation. According to Swire, self-regulation relies on "shared community norms and ethical values", it is these shared norms and values that will keep the people at a company from making decisions which could negatively impact their reputation (Swire, 1997). This type of regulation is not possible in a country as diverse in values as the United States. According to a pew research study conducted from November 2014 to January 2015, 40% of American citizen felt it was okay for the government to monitor their communications compared to 57% who felt it was unacceptable (Pew Research Center, 2016). With Americans divided on the most basic privacy issues, how could self-regulation ever work? The most effective solution to current problems would be a twofold approach. First, DNA testing must be regulated by a government agency and export embargoes placed on countries which do not possess a very good human rights record. An approach similar to that of the one used for regulating nuclear technologies could be a good framework. Secondly, American's must have a legal right to their DNA and the information it contains. It should be considered both their intellectual and physical property where anyone who possesses it without express permission from the owner should be held legally accountable. Ideally, the US government would amend HIPAA to include DNA

analysis companies. The drawbacks of this solution would be increased red tape for anyone wishing to start or operate a DNA testing company, however, there are many industries with regulation who are still able to thrive while maintaining compliance. It is only through government regulation that the multitude of negative consequences of DNA analysis can be controlled.

Word Count: 1,507

Bibliography

Zhao, C. (2018, April 27). How was the Golden State Killer caught? DNA from relative on genealogy website was key. Retrieved November 11, 2019, from https://www.newsweek.com/how-was-golden-state-killer-caught-dna-relative-genealogy-website-was-key-903590.

Department of Justice. Audit Report: The Combined DNA Index System, Audit Report: The Combined DNA Index System (2001). Washington DC. Retrieved from https://oig.justice.gov/reports/FBI/a0126/final.pdf

CODIS - NDIS Statistics. (2016, June 8). Retrieved from https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics.

Combined DNA Index System (CODIS). (2016, May 6). Retrieved from https://www.fbi.gov/services/laboratory/biometric-analysis/codis.

Gasiorowski-Denis, E. (2016, July 6). The mystery of the Phantom of Heilbronn. Retrieved from https://www.iso.org/news/2016/07/Ref2094.html.

Moran, K. S. (2018). Damned by DNA — Balancing personal privacy with public safety. Forensic Science International, 292. doi: 10.1016/j.forsciint.2018.09.011

Dillard, J. F. (2003). Professional services, IBM, and the Holocaust. Journal of Information Systems, 17(2), 1+. Retrieved from https://bi-gale-com.libezproxy2.syr.edu/essentials/article/GALE%7CA114128501?u=nysl_ce_syr

Leetz, K. L. (2018). An Unanticipated Outcome of a DNA Ancestry Test. American Journal of Psychiatry, 175(12), 1167–1168. doi: 10.1176/appi.ajp.2018.18050555

Wee, S.-lee. (2019, February 21). China Uses DNA to Track Its People, With the Help of American Expertise. Retrieved from https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html.

Swire, Peter. (1997). Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce.. SSRN Electronic Journal. 10.2139/ssrn.11472.

The state of privacy in America. (2016, September 21). Retrieved from https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.