An Ethical Look at Investigative DNA

by Carolyn Harvey

May 2020

On April 24, 2018, Joseph James DeAngelo, Jr., was apprehended by Sacramento County Sheriff's deputies after DNA pinpointed him as the Golden State Killer, the chief suspect in rapes and robberies spanning from the 1970s to the 1990s throughout California (Hare & Taoushiani, 2019). What makes DeAngelo's case different, though, is that not only his DNA was used to name him. DNA of other people collected from GEDmatch, an open-access DNA database, was used by police investigators to help identify DeAngelo as the suspect for arrest. Investigators used GEDmatch data along with other public records to build family trees of the Golden State Killer suspects, ultimately nabbing DeAngelo as their man.

While many people congratulated the investigators for capturing the menace who victimized the citizens of California for so long, many others wondered if a line had been crossed: In their investigation, police had accessed private DNA for public business without a warrant. Further, they had implicated an unknown number of innocent people in a criminal investigation. What are the ethics of police investigations of crimes using online, open-access DNA databases, without the DNA donors' knowledge or consent?

DNA for Crime Control

Because DNA contains genetic information that is unique to each individual person[1], it is very useful as a tool to solve crime. When an assailant leaves genetic material behind at a crime scene, DNA can be extracted and profiled. DNA found at crime scenes is routinely compared to DNA in national databases maintained by the FBI. The DNA Identification Act of 1994 (42 U.S.C. §14132) authorized the establishment of a national DNA index, and the Federal Bureau of Investigation spearheaded the use of DNA in criminal investigations in the United States. The FBI established and currently operates CODIS (the Combined DNA Index System) as well as the Convicted Offender Index and

[1] Except in the instance of identical twins.

carolynstoverharvey@yahoo.com

NDIS (the National DNA Index System). The federal DNA database use is restricted to those who need it to carry out their job duties, and is currently the only investigative DNA resource available to federal investigators. The Federal DNA Database Unit (FDDU) of the FBI currently organizes and oversees the federal DNA databases, including CODIS and NDIS (CODIS and NDIS Fact Sheet).

CODIS and NDIS accept DNA from law enforcement agencies at all levels from all 50 states. Laboratories that submit DNA to CODIS and NDIS must follow strict accreditation guidelines established by federal law. Laboratories must be accredited by a nationally recognized nonprofit forensic science professional association. DNA samples processed in federal labs can only be used in certain circumstances set forth in federal law, including in judicial proceedings and criminal defense purposes. Familial DNA searches, like the investigative DNA searches in the Golden State Killer hunt, are not performed in NDIS (CODIS and NDIS Fact Sheet).

Another way that police obtain DNA is by lawfully obtaining samples from people who are arrested. The National Conference of State Legislatures reports that 30 states, as well as the federal government, currently have laws on the books that require DNA samples to be taken from individuals who are arrested or charged with certain crimes, with no conviction necessary. Each state with these laws on its books has different mandates for what type of charge requires a DNA collection (felony or misdemeanor), and whether minors must provide a DNA sample. Some states require a probable cause hearing, and some require automatic expungement of the DNA collection if the arrestee is not charged or is otherwise not convicted of a qualifying crime (National Conference of State Legislatures).

Until very recently, if CODIS, NDIS, and state-specific law enforcement databases produced no match, it was a dead end for investigators. Investigators had to wait for perpetrators to be apprehended for another reason and entered into the databases, and then cross-matched to their sample. Noting the advancement of DNA technology, lawmakers in some states initiated policies or laws that allowed investigators to access investigative DNA in other ways. According to the FBI,

carolynstoverharvey@yahoo.com

"Arkansas, California, Colorado, Florida, Michigan, Texas, Utah, Virginia, Wisconsin and Wyoming currently perform familial searching," but without the use of CODIS resources (CODIS and NDIS Fact Sheet). This is the policy that enabled a team of California investigators to finally identify DeAngelo. They were operating completely within the law.

Commercial DNA Tests and Open-Access Databases

The commercial ancestry DNA test market developed in the early 2000s[2]. Today, there are three main players: Ancestry, 23andMe, and Helix. All of these companies allow consumers to spit into a tube, mail it off, and obtain an online report showing estimates of ethnic origins, all for entertainment purposes. People also use the sites to connect with newly discovered relatives identified through DNA matches, post on message boards to research their heritage, build out family trees, and even connect with long-lost family members. In 2019, it was estimated that commercial DNA testing companies held the profiles of nearly 26 million people (Institute for DNA Justice: Investigative Genetic Genealogy).

Some people take their research a step further by downloading their raw DNA file from the site and uploading it to an open-access online DNA database called GEDmatch, where it can be analyzed more thoroughly by amateur genealogists, among others. Per the login page at http://www.gedmatch.com, GEDmatch is a website that "provides applications for comparing your DNA test results with other people" as well as some other ancestry estimation tools (GEDmatch Login Page).

According to an article on the Pew Research Trust website, law enforcement officers across the country are following suit by using GEDmatch, hoping to strike cold case gold like the State of California did with DeAngelo, saying "Arrests have been made in dozens of cases — many that had been considered cold." The same article

[2] This is different from the direct-to-consumer genome testing, for instance, to determine if a woman has the BRCA-1 and BRCA-2 mutations that would potentially lead her to develop breast or ovarian cancer. These tests, characterized as "Cancer Predisposition Tests (CFR 21 866.6090)" are considered medical devices and are regulated by the FDA . Other genome tests that purport to determine one's general wellness, for instance, are considered novelty items that do not require FDA approval (Center for Drug Evaluation and Research, 2019).

carolynstoverharvey@yahoo.com

says that “By the end of 2019, GEDmatch’s database had been used to solve at least 70 U.S. violent crimes. Verogen, a forensic genomics company, bought GEDmatch in December [2019], and said that the use of its database as a crime fighting tool...would continue” (Van Ness, 2020). Sacramento County district attorney Anne Marie Schubert believes in the concept of investigative DNA so much, she established the Institute for DNA Justice, a non-profit with the goal to “educate the public about the value of investigative genetic genealogy (IGG) as a revolutionary new tool to identify, arrest, and convict violent criminals, deter violent crime, exonerate the innocent, [and] encourage the 26 million Americans who have taken a DNA test to become genetic witnesses” by uploading their genetic profiles to GEDmatch.com and FamilyTreeDNA.com, a similar open-access DNA database (Institute for DNA Justice: Investigative Genetic Genealogy). To Schubert, investigative DNA is the key to solving crime.

At present, there is no federal law against using DNA from open-access DNA databases in investigations. In September 2019, the Department of Justice issued the “Interim Policy on Forensic Genetic Genealogical DNA Analysis and Searching” to provide guidance to federal officers on the burgeoning topic. A final policy is expected this year. In short, the interim policy allows the following:

> In essence, a DNA sample taken from the scene of a violent crime that does not match any samples available in the FBI’s Combined DNA Index System (CODIS) will not generate a lead for law enforcement. FGG[3] provides an alternative option. However, FGG requires a type of DNA testing that Department laboratories currently do not perform, so the sample must be outsourced to a vendor laboratory. After the vendor laboratory completes a more comprehensive analysis on the sample, the resulting genetic profile is entered into one or more publicly-available genetic genealogy services and compared by automation against the genetic profiles of individuals who have voluntarily submitted their own samples. The computer’s algorithm then evaluates potential familial relationships between the sample donor and the website’s users. If an

[3] The Department of Justice’s term for investigative DNA is “forensic genetic genealogical DNA” or “FGG DNA.”

carolynstoverharvey@yahoo.com

> association is detected, it generates a lead. Subsequently, law enforcement can use that lead to advance their investigation using traditional investigative and genealogical methods.
>
> The personal genetic information is not transferred, retrieved, downloaded, or retained by the genetic genealogy users – including law enforcement. And before FGG is an option, all other available techniques, including a search of CODIS, must be exhausted (Department of Justice).

At the time of this writing, the final policy has not been released.

To date, The Supreme Court of the United States has heard just one case that is somewhat similar to using investigative DNA to solve crime. The key issue that the court undertook in the case is the state's unreasonable search and seizure as outlined in the Fourth Amendment of the Constitution. In the 2013 case *Maryland v. King*, the court upheld the constitutionality of "routine collection and storage of DNA samples and profiles from arrestees" (Kaye, 535). Maryland police arrested Alonzo King for "menacing people with a shotgun" and processed his booking in the usual way, photographing him, taking his fingerprints, and swabbing the inside of his cheek for DNA. The DNA sample was checked against the Maryland database, whereupon it was discovered that "six years earlier, King had held a gun to the head of a fifty-three-year-old woman and raped her." Had the police not lawfully taken the sample, King would have not been identified as the suspect for the rape and assault and subsequnently tried for the crime. King was convicted of rape and appealed the conviction, arguing that the "DNA collection deprived him of the right, guaranteed by the Fourth Amendment of the Constitution, to be free from unreasonable searches or seizures," to which the Maryland Supreme Court agreed. The State of Maryland then petitioned for another review, and it went to the Supreme Court, which found:

carolynstoverharvey@yahoo.com

> (1) buccal swabbing is a search subject to the Fourth Amendment; (2) the constitutionality of this kind of search, performed on all individuals arrested for serious crimes, turns on the balance of state and individual interests; and (3) this balance favors the state when the swabbing is done (a) after charges have been filed, (b) the loci tested do not reveal sensitive personal information, and (c) statutory and administrative privacy safeguards are in place (Kaye, 541).

The key point in *King* is that there is a "categorical-exception approach" where the category is arrested individuals (Kaye, 543). In Justice Kennedy's opinion,

> "In addition, the record of the arrestee's DNA profile could be useful in solving future crimes. A database of DNA profiles of suspected terrorists is one such intelligence tool, as it can be used to inform analysts of these suspects' possible involvement in bombings or other incidents in which DNA traces are found" (Kaye, 545).

While this law didn't explicitly hold up the constitutionality of swabbing completely disinterested bystanders--King was under arrest for another crime and was in police custody at the time--lawmakers in many states have recognized the need to extend specific protections to people as it relates to police using open-access DNA databases. Ironically, while Maryland does permit swabbing of arrestees in custody, the state explicitly prohibits the use of investigative DNA in criminal investigations, as does the District of Columbia (National Conference of State Legislatures). As previously mentioned, several states have developed guidelines for using investigative DNA, while several other states have recently proposed legislation that would completely ban the practice, citing the possibility that it gives police the ability to obtain a warrant to perform a "mass search," according to Michael Melendez, a policy director at Libertas Institute, as quoted in a Pew Charitable Trust article about DNA databases (Van Ness, 2020). In

carolynstoverharvey@yahoo.com

a 2018 *Washington Post* article, former public defender Stephen Mercer, who helped initiate the legislation to ban investigative DNA in Maryland, said, “You allow that low-quality potential evidence to start being searched in these unregulated databases, you’re casting a wide net suspicion over many, many people” (Selk, 2018). This is especially germane considering an estimated 26 million Americans alone have taken at-home DNA tests (Institute for DNA Justice: Investigative Genetic Genealogy).

Other state lawmakers are seeking to limit the boundaries of investigative DNA. Ways to address this include limiting the use of investigative DNA to only felony cases, or only allowing its use when all other leads have been exhausted. Yet others are attempting to regulate what consumer-focused DNA companies can release to law enforcement without a consumer’s consent (Van Ness, 2020).

In an effort to advocate for their industry, the aforementioned three major consumer-focused DNA companies created a Washington, D.C. lobby called the Coalition for Genetic Data Protection. The CGDP is in favor of clear federal legislation on the use of investigative DNA. The group’s Frequently Asked Questions document posted to its website addresses this by saying, “Currently, there is a patchwork of policies at the state level. We would instead welcome comprehensive privacy legislation at the federal level, so that we have a uniform set of rules by which to abide. The Coalition will provide a single voice on these issues, to ensure consumer trust and continued innovation” (Coalition for Genetic Data Protection). It also says, regarding interaction with law enforcement, that

> We never share customer data with law enforcement unless we receive a legally valid request such as a search warrant or written court order. Upon receipt of an inquiry from law enforcement, we use all practical legal measures to challenge such requests in order to protect our collective customers’ privacy. In addition, our companies voluntarily publish transparency reports that are available on our public websites and detail the number of valid law enforcement requests we receive, and whether or not customer data has been disclosed (Coalition for Genetic Data Protection).

carolynstoverharvey@yahoo.com

GEDmatch is not a member of the Coalition for Genetic Data Protection. As a standalone company that does not conduct tests, it has approximately one million DNA profiles in its database. However, it is not immune from demands from law enforcement. After investigative DNA was proven to work and DeAngelo was nabbed with information from GEDmatch, the site received a great deal of public pushback. In 2018, when the site was still run by its original founders Curtis Rogers and John Olson out of a Lake Worth, Florida bungalow, a *New York Times* article reported that "The site's privacy agreement had always been vague, essentially stating that its owners had no control over how any individual's genetic or family tree data could be used" (Murphy b, 2018). Just days after DeAngelo's capture, the site was updated to an opt-in model so that people could make a choice to allow their genetic information to be available to law enforcement. However, even that opt-in model cannot always protect consumers from police; in July 2019, a Florida judge granted a search warrant giving investigators access to "nearly 1 million GED match users who had not elected to help law enforcement" (Murphy, 2019). The site is now owned by Verogen, a forensic genomics company (Van Ness, 2020) which is "best known for providing police and FBI labs with tools for making predictions about suspected criminals' ancestry, eye color and hair color," according to a 2019 *New York Times* article (Murphy, 2019).

A Utilitarian Ethical Framework Review of Investigative DNA

In the simplest terms, a utilitarian ethical framework proposes that the key determination in making decisions should be: which choice will benefit society the most? In other words, what is good for society should dictate what happens. By focusing on consequences, utilitarianism eliminates looking at the collateral damage. It is the most often cited ethical justification for war, for instance, because the ends justify the means.

The use of investigative DNA in the American criminal justice system poses several ethical questions that can be examined through the lens of utilitarianism. The general public wants to be free from crime, and the criminal justice system works hard to prevent crime and to capture, prosecute, and punish criminals. As it has already been

carolynstoverharvey@yahoo.com

demonstrated, investigative DNA is a powerful tool that has led to the capture of criminals in decades-old cases that would have otherwise probably just stayed cold. But there are risks inherent to involving innocent family members and other people who may not even be involved in the case--the so-called collateral damage.

Issue One: Records-Based Research

There is great utility in DNA for solving crimes. In the Golden State Killer investigation, police would not have known about DeAngelo's relatives, nor would they have been able to build out the family trees like they did, or accurately predict his eye color--all which aided their investigation--without the help of investigative DNA obtained through an open-access DNA database. In the course of their records-based research, investigators dealt with human subjects who were intertwined with DeAngelo in ways in which the researchers were unaware. The investigators could not have predicted the impact of their inquiries, nor the impact their investigation made in the apprehending of the suspect. In records-based research, at least when abiding by best practices in an Institutional Research Board-supervised environment, researchers are supposed to minimize harm to research participants (Matuk, 2019). It's unclear if DeAngelo's family members, or research participants, ever knew of the investigator's motives. Additionally, researchers are supposed to ensure research participants privacy and confidentiality (Matuk, 2019). The question is, though, how can privacy and confidentiality be ensured when participants don't even know they are being studied?

Issue Two: Consent

The Golden State Killer investigation included people who likely never expressly consented that their DNA sample be included in a police investigation. Consent is a key component of the ethical treatment of human subjects as "autonomous persons" capable of making their own decisions and directing their own lives, as directed in The Belmont Report (National Commission for the Protection of Human Subjects of

carolynstoverharvey@yahoo.com

Biomedical and Behavioral Research, 1978). Even though the California police investigators were working with computer files and not test tubes in a lab, the digital DNA files they were working with are, overall, subject to the same ethical considerations, and should have been treated as such.

Discussion

While the investigative DNA work yielded the capture of the suspect, it raises ethical questions among scientists and others concerned for the fair and ethical treatment of subjects. In the Golden State Killer investigation, there were many subjects: DeAngelo, the family members making up his family tree as put together by the investigators, and the untold number of people who were erroneously pulled into the investigation. This number is bound to be very high by virtue of the nature of the investigation. Barbara Rae-Venter, a retired patent attorney and the chief genetic genealogist involved in the investigation, noted she worked with “birth records, newspaper clippings, social media profiles, and family tree data” to fill in the branches of the DeAngelo family tree, according to an interview with Heather Murphy of *The New York Times* in 2018. These types of records--even civil records such as birth records--are not always accurate. People who had absolutely nothing to do with the investigation--extremely distant relatives, many generations removed, or people who don’t even share a centimorgan of DNA with DeAngelo--were almost certainly included in the investigation in error. Reports indicate that out of 25 different family trees assembled during the investigation, 24 did not include DeAngelo; up to 1,000 family members were implicated; and at least two individuals were falsely pinpointed as suspects, with one even asked for a DNA sample (Fullerton and Rohlfs, 2018).

Prior to DeAngelo’s capture in 2018, people who uploaded their DNA to GEDMatch did so to primarily engage in deeper genealogical work, or to run experimental genetic admixture models. An April 28, 2018 article in the *Wall Street Journal* just days after DeAngelo’s capture stated that “GEDmatch’s purpose is genealogy research, according to its terms and policy statement” (Hernandez,

carolynstoverharvey@yahoo.com

Kanno-Youngs, & Elinson, 2018). The site was a resource for people who wanted to connect across consumer DNA platforms; it was a neutral site that accepted almost every consumer DNA test in raw format to upload, identify genetic matches, and assist in genealogical research. No one expected that their DNA could be used to assist in a law enforcement investigation. The terms of service didn't indicate one way or the other, and no one suspected that law enforcement was even using the site in this manner (Hernandez, Kanno-Youngs, & Elinson, 2018). It just wasn't on anyone's mind.

Utilitarian ethicists would say that in this scenario--using investigative DNA, including DNA of unknown people, like in the Golden State Killer case--society benefits and thus it is an ethical action. By using investigative DNA, society benefits from removing a vicious serial killer off the streets, and the risk of harm to the numerous family members is negligible[4]. To a utilitarian ethicist, the ends justify the means. This admittedly small intrusion, which probably went unnoticed by almost everyone in the investigation, yielded DeAngelo's capture, and has started a process of closure for numerous victims who have had to live with the physical and psychological trauma he caused, as well as a collective sigh of relief for the people of the State of California who lived in fear for decades because of his actions.

But even utilitarian ethicists draw a line. No one wants their civil liberties impeded. In the classical understanding of utilitarianism, "an action is right if it tends to promote happiness and wrong if it tends to promote unhappiness--not only for the agent but also for everyone affected" (Duignan, 38). The outcome would be different if, perhaps, investigators demanded a saliva sample of everyone in Sacramento County to test for a DNA match with DeAngelo. That would likely be viewed as too far of an intrusion into the private lives of individuals with no good connection to the case, even if it was going to result in the capture of a serial killer.

[4] The public interest in the Golden State Killer case was intense. Immediately after DeAngelo's arrest, curious people started posting information about DeAngelo's family members in r/EARONS, the "East Area Rapist Original Night Stalker" subreddit, "doxxing" them (publishing private information not readily available about them) (Emerson, 2018). While the great majority of those involved in the investigation have not had their private information posted or their identity revealed, for those close family members who did, the personal crisis of dealing not only with a close family member being named as a grotesque criminal, and then having one's private information exposed and the vulnerability that comes with that, cannot be underestimated.

carolynstoverharvey@yahoo.com

The Technomoral Virtues

Techno-philosopher Shannon Vallor outlines a number of technomoral virtues that must be examined in order to live wisely and well with an uncertain future in technology, which she terms “technosocial opacity.” For this issue in particular, it seems the most applicable technomoral virtues are justice and technomoral wisdom.

For Vallor, justice is “a reliable disposition to seek a fair and equitable distribution of the benefits and risks of emerging technologies” (128). Straightway, the issue of investigative DNA is unjust because investigative DNA does not ever have a fair and equitable distribution of its benefits and risks. Not everyone wants to participate in consumer DNA tests, but despite that, the technology can show enough of their DNA to make a connection: As University of Washington bioethicist Stephanie Fullerton and San Francisco State University biologist Rori Rohlfs write, “...The decisions of individuals to contribute their own genetic information inadvertently exposes many others across their family tree who may not be aware of or interested in their genetic relationships going public” (Fullerton and Rohlfs, 2018). Another aspect to consider is when investigative DNA is incorrect. DNA found at a crime scene can be an incidental finding, completely innocent--or it can be a mistake. And when it is wrong, the results can be devastating. In 2015, a Louisiana man, Michael Usry, was finally exonerated as a suspect in an Idaho murder that his father had entangled him in--all via investigative DNA. In an article from *The New Orleans Advocate*, the tale of Usry’s “false positive” was detailed:

> The elder Usry, who lives outside Jackson, Mississippi, said his DNA entered the equation through a project, sponsored years ago by the Mormon church, in which members gave DNA samples to the Sorenson Molecular Genealogy Foundation, a nonprofit whose forensic assets have been acquired by Ancestry.com…

carolynstoverharvey@yahoo.com

> Ancestry.com received a court order last summer requiring it to reveal Usry's name to the police...Following this new lead, the police mapped out five generations of Usry's family, narrowing their focus to three men.
>
> Detectives traveled to New Orleans in December [2014] and persuaded a magistrate judge to sign a search warrant ordering Usry to provide his DNA for comparison. For about a month, Usry lived in a state of suspense, fearing he'd be taken into custody regardless of the test results.
>
> On. Jan. 13 [2015], Usry received the email he'd been awaiting. His DNA, Hoffman wrote, did not match the semen from the scene of [the] murder.

Usry won't be the last person incorrectly held in limbo as investigative DNA is used. As investigative DNA is used more frequently, it is likely that more people will be caught in its helix. Usry lost a month of his life to worry and anxiety, but what will be the outcome when a jury chooses to convict based on an inability to understand that a likely match in DNA does not mean a complete match, like what Usry was facing? His DNA match was a partial match to the suspect's. If the prosecutors had somehow been able to convince a jury that any DNA evidence was enough evidence to convict, the outcome could have been disastrous for Usry. The "CSI effect," a modern courtroom phenomenon where jurors expect to see all manner of technologically advanced testing, creates an expectation among prosecutors, according to NPR's Arun Rath in "Is the 'CSI Effect' Influencing Courtrooms?" In the article, Rath reported, "Prosecutors have been complaining that shows like *CSI* are creating the expectation that every trial must feature high-tech forensic tests. They fear that when they don't show off *CSI*-style technology, juries might let criminals get away with murder" (Rath, 2011). A conviction like that would be neither just nor wise.

Investigative DNA would not be possible without websites, all of which require registration and agreement to the terms of service and privacy policy for the site in order to participate. The terms of service and privacy policy documents are often contained in

carolynstoverharvey@yahoo.com

one “clickwrap” document that is designed to speed along registration and get users into the app or social network site as quickly as possible, regardless of how life-altering the terms of service could be. According to communications researchers Jonathan Obar of York University and Anne Oeldorf-Hirsch of the University of Connecticut, the term “I agree to these terms and conditions” is “the biggest lie on the Internet” (Obar & Oeldorf-Hirsch, 129).

To investigate this theory, in the fall of 2015, Obar and Oeldorf-Hirsch devised a study in which they introduced 543 undergraduate communications students to a new social networking platform called “NameDrop.” The students were to conduct a pre-launch evaluation of the site, including signing up, reviewing the site, and deleting their account. The signup design was similar to Facebook, Twitter, and LinkedIn, with a clickwrap that “bypass[ed] consent materials, accepting policies without having to access or read them;” students also had the choice to review the terms of service and privacy policy in long-form. The researchers estimated that the privacy policy and terms of service would take the students approximately 45 minutes to read (Obar & Oeldorf-Hirsch, 133). Tucked away within the terms of service were two “gotcha” clauses. One indicated that all data gathered and generated by NameDrop would be shared with the National Security Agency. The other “gotcha” clause indicated that in exchange for using the platform, the user’s firstborn child would be required as payment (Obar & Oeldorf-Hirsch, 134).

As expected by the researchers, very few of the students--these “communication scholars-in-training,” took the time to review the terms of service or privacy policy, and just accepted the clickwrap. While the researchers acknowledged the possibility that the students did not act entirely as they would in a “real world” situation because they could have placed their trust in the university’s vetting of the site, or because the students were not actually signing up for the site, they also say that this supports their claim that terms of service are the “biggest lie on the Internet” even moreso (Obar & Oeldorf-Hirsch, 140).

carolynstoverharvey@yahoo.com

The authors of the study also bring up two points that are very germane to the topic of investigative DNA and technomoral wisdom. One is the “privacy paradox,” which is explained as, “...When asked, individuals appear to value privacy, but when behaviors are examined, individual actions suggest that privacy is not a high priority” (Obar & Oeldorf-Hirsch, 142). In the context of their study, the researchers say their study results support this conflict; the research subjects, communications students who should be highly aware of the implications of not knowing the details of their data in the hands of a new website, skipped the opportunity to learn about it in favor of a quick sign-up. The privacy paradox is especially relevant when DNA is concerned; when DNA is at stake, more than one person’s information is vulnerable. People who wouldn’t hesitate to protect their children from the public’s prying eyes by limiting their exposure on social media, for instance, don’t realize they are making their children’s DNA available by putting their own DNA online.

The second point the researchers make is about what they call the “I’ve got nothing to hide” argument, which Obar and Oeldorf-Hirsch characterize as, “A common justification for privacy disinterest, this fallacy incorrectly assumes, as one participate in this study noted when justifying clickwrap use, ‘Nothing too bad happened yet, but it’s not like a I post anything interesting or worthy’” (Obar & Oeldorf-Hirsch, 143). In the investigative DNA world, the “I’ve got nothing to hide” argument is often used by people who want to contribute to police investigations; they want to put their DNA out on open databases in the hopes that it will someday assist law enforcement in catching a criminal. In the context the authors were involved in, the “I’ve got nothing to hide” crowd eschew privacy because in this moment, they do not have anything they want to obscure from anyone’s prying eyes. However, they are not considering the future technologies that may come about, or the calculations that could be made based on their current actions. It is similar with DNA; while the “I’ve got nothing to hide” people say they would like to help catch a criminal, what if the police come knocking on their door because they are incorrectly fingered as a suspect? Or perhaps there is an algorithm that is developed that can somehow predict criminal behavior based on DNA,

carolynstoverharvey@yahoo.com

and law enforcement use DNA in open-access DNA databases to identify who will become a criminal in 10 years? This altruistic gesture may end up ruining lives.

Vallor's position is that technomoral wisdom is the "general condition of well-cultivated and integrated moral expertise that expresses successfully--and in an intelligent, informed, and authentic way--each of the the other virtues of character that we, individually and collectively, need in order to live well with emerging technologies" (Vallor, 154). When placed in this context, investigative DNA fails as an ethical tool. Vallor's utopian dream of intelligent and informed technology users just isn't realistic when users whiz through clickwraps to access websites, regardless of the consequences. In the current model, people using consumer DNA sites or GEDmatch do not understand what they are getting themselves (and others) into. Currently, there are just too many risks that preclude investigative DNA from being part of any version of a good life.

Solutions

The most efficient way to solve this problem just might be through federal law. As previously stated, the industry lobby, the Coalition for Genetic Data Protection, has stated its preference for federal legislation regarding privacy for consumer DNA tests. A simple way to address this would be to add consumer DNA test companies as a covered entity under the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-191). Title II of HIPAA is the main federal law that governs the confidentiality of medical information in the United States. Title II regulates the dissemination of protected health information (PHI) held by covered entities (usually, healthcare providers or those involved in care). In very simple terms, the intention of Title II was to keep medical information private and disclosed only on a business need basis, for instance, in healthcare operations or payment operations. However, there are many misgivings among the general public about the Privacy Rule and what it does and does not cover. Many people do not understand that the genetic information gathered through consumer DNA testing is not subject to HIPAA Privacy

carolynstoverharvey@yahoo.com

Rule protections, because these companies are not healthcare providers.[5] [6] But this solution also has the potential to severely bureaucratize the direct-to-consumer model with layers of privacy personnel, paperwork requests, tiered fee schemes to obtain records, and other familiar sights borne of the HIPAA Privacy Rule era. For a service that is completely online, this doesn't make much sense. But a uniform federal rule would optimize efficient operations for the test companies.

Another way to solve this might be through federal consumer law. Traditionally, this "notice and choice" privacy framework developed as consumer protections under the umbrella of federal departments, including the Federal Trade Commission. According to Obar and Oeldorf-Hirsch, "ongoing efforts to strengthen data protections continue to draw on the old framework" which attempt to "put individuals in charge of the collection and use of their personal information" (Obar & Oeldorf-Hirsch, 129). But as their study demonstrated, people are wont to ignore privacy and terms of service documents, which suggests "regulatory failure" (Obar & Oeldorf-Hirsch, 130). But what if the regulation shifts from consumer notice, to regulation of the companies offering the services? A "consumer bill of rights" would state in plain language what consumers should and should not expect from consumer DNA testing companies, standardized across all platforms, with the heft of the Federal Trade Commission to enforce it. The FTC is already charged with protecting consumers by "stopping unfair, deceptive or fraudulent practices in the marketplace," so this would be a natural fit for the FTC (Federal Trade Commission, 2014). Tightening up the consumer rights--and protecting them under the umbrella of a powerful federal agency--could have huge implications for protecting consumer DNA against all law enforcement agencies, and unscrupulous open-access DNA databases that aren't crystal clear about their intentions with law enforcement involvement.

[5] Ancestry even spells it out in their privacy policy (https://www.ancestry.com/cs/legal/health-privacy) under Section 3, "What Information Does Ancestry Collect From You?": "Ancestry is not a covered entity under the Health Insurance Portability and Accountability Act ('HIPAA'), and as a result no Additional User Information provided by you is subject to or protected by HIPAA."

[6] The tests are also not regulated by the FDA, as they are not considered medical devices.

carolynstoverharvey@yahoo.com

As bioethicist Stephanie Fullerton and biologist Rori Rohlfs point out in their article, “Should Police Detectives Have Total Access to Public Genetic Databases?” the crux of the issue is that “police interaction with such databases must be addressed as a public policy issue, not left to the informed consent of individual consumers” (Fullerton & Rohlfs, 2018). They posit that the rights of those who do not want their genetic information revealed to the public--but that would be revealed by nature of DNA--should be respected. After all, they say, there is no opt-out for your relative posting her DNA profile to GEDmatch, and in the process, revealing you, too. Fullerton and Rohlfs (2018) propose strict regulation of law enforcement use of DNA databases, including limiting it to only those people who are either convicted of crimes, or arrested for suspicion of committing a crime; using it only for the most “serious crimes with public safety implications where all other investigatory methods have been exhausted,” and where excellent DNA samples are available. They also suggest two separate teams of investigators, with the detectives and genetic investigators separated, “so as to minimize the impact of incidental findings” (Fullerton & Rohlfs, 2018).

At a very minimum, companies engaged in consumer DNA testing and the retention of consumer DNA data should abide by the same standards established for all other medical research and/or clinical laboratory tests, including the principles outlined in the Belmont Report and other relevant guiding documentation. They should also owe strict liability solely to their users and research subjects. In all instances, law enforcement agencies should have to show a court that their investigation cannot be furthered without the use of investigative DNA. A forensic genealogist familiar with forensic science and/or records-based research practices should be engaged to perform the work to ensure a high rate of fidelity to the applicable research and ethical principles.

Conclusion

In the United States, where the accused is innocent until proven guilty in a court of law, investigative DNA should never be considered a panacea. It is one of many tools available to law enforcement and prosecutors. Because investigative DNA has the

carolynstoverharvey@yahoo.com

possibility to trample the rights of the innocent, it must be weighed carefully when it is used. This paper has proposed a few solutions to the ethical use of investigative DNA. It is likely that, like in many instances of technology applied to life-or-death scenarios, the answer is multi-faceted and will include stricter federal health- or consumer-based protections in how DNA is treated; state-based laws about how investigative DNA can be used by law enforcement; and adoption of the same policies, standards, and practices for internal police forensic investigations as are in place in scientific laboratories. Oversight by external committees or boards made up of community members, faith leaders, the press, academics, and others is also needed. In short, the use of investigative DNA needs regular external examination, criticism, and reform, because the technology is developing exponentially faster than legislation can address it.

Regardless of the framework or lens, the work of ethics is concerned with the same goal: how to live a good life. For binary issues, where there is a clear good or bad option, this is an easy decision. Investigative DNA is not a binary issue. There are many grey areas found that present incredible challenges to humanity and our justice system. We should only expect to be faced with more challenges, because crime won't stop, and technology won't stop advancing.

carolynstoverharvey@yahoo.com

Works Cited

Center for Drug Evaluation and Research. (2019, December 20). Direct-to-Consumer Tests. Retrieved May 7, 2020, from https://www.fda.gov/medical-devices/vitro-diagnostics/direct-consumer-tests

Coalition for Genetic Data Protection. (n.d.). Website FAQ. Retrieved April 20, 2020, from https://geneticdataprotection.com/wp-content/uploads/2019/10/Coalition-for-Genetic-Data-Protection-Website-FAQ.pdf.

CODIS and NDIS Fact Sheet. (2016, June 8). Retrieved April 30, 2020, from https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet

Department of Justice. (2019, September 24). Department of Justice Announces Interim Policy on Emerging Method to Generate Leads for Unsolved Violent Crimes. Retrieved April 30, 2020, from https://www.justice.gov/opa/pr/department-justice-announces-interim-policy-emerging-method-generate-leads-unsolved-violent

Duignan, B. (2011). *Thinkers and theories in ethics*. New York: Britannica Educational Pub. in association with Rosen Education Services.

Emerson, S. (2018, April 26). Internet Sleuths Are Harassing the Family of the Golden State Killer Suspect. Retrieved May 4, 2020, from https://www.vice.com/en_us/article/8xkpmv/internet-sleuths-are-harassing-the-family-of-the-golden-state-killer-suspect

Federal Trade Commission. (2014, April 15). What We Do. Retrieved May 6, 2020, from https://www.ftc.gov/about-ftc/what-we-do

Fullerton, S., & Rohlfs, R. (2018, July 23). Should Police Detectives Have Unrestricted Access to Public Genetic Databases? Retrieved April 30, 2020, from https://leapsmag.com/should-police-detectives-have-total-access-to-public-genetic-databases/

carolynstoverharvey@yahoo.com

GEDmatch Login Page. (n.d.). Retrieved April 30, 2020, from https://www.gedmatch.com/login1.php

Hare, B., & Taoushiani, C. (2019, April 24). What we know about the Golden State Killer case, one year after a suspect was arrested. Retrieved April 30, 2020, from https://www.cnn.com/2019/04/24/us/golden-state-killer-one-year-later/index.html

Institute for DNA Justice: Investigative Genetic Genealogy. (n.d.). Retrieved April 30, 2020, from https://www.institutefordnajustice.org/

Kaye, D. H. (2014). Why So Contrived - Fourth Amendment Balancing, Per Se Rules, and DNA Databases after Maryland v. King. *Journal of Criminal Law and Criminology*, *104*(3), 535–596.

Matuk, J. (2019, May). Records-Based Research. Retrieved April 30, 2020, from https://www.citiprogram.org/members/index.cfm?pageID=665&ce=1#view

Murphy, H. (2018a) (2018, August 29). She Helped Crack the Golden State Killer Case. Here's What She's Going to Do Next. Retrieved March 28, 2020, from https://www.nytimes.com/2018/08/29/science/barbara-rae-venter-gsk.html

Murphy, H. (2018b) (2018, October 15). How an Unlikely Family History Website Transformed Cold Case Investigations. Retrieved March 28, 2020, from https://www.nytimes.com/2018/10/15/science/gedmatch-genealogy-cold-cases.html

Murphy, H. (2019, December 22). What You're Unwrapping When You Get a DNA Test for Christmas. Retrieved March 28, 2020, from https://www.nytimes.com/2019/12/22/science/dna-testing-kit-present.html

Mustian, J. (2015, March 12). New Orleans filmmaker cleared in cold-case murder; false positive highlights limitations of familial DNA searching. Retrieved April 30, 2020, from https://www.nola.com/article_d58a3d17-c89b-543f-8365-a2619719f6f0.html

National Conference of State Legislatures. (2013). DNA Arrestee Laws. Retrieved March 28, 2020, from https://www.ncsl.org/Documents/cj/ArresteeDNALaws.pdf

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1978). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research*. [Bethesda, Md.]: The Commission.

carolynstoverharvey@yahoo.com

Obar, J. & Oeldorf-Hirsch, A. (2020) The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services, Information, Communication & Society, 23:1, 128-147, DOI: 10.1080/1369118X.2018.1486870

Rath, A. (2011, February 6). Is The 'CSI Effect' Influencing Courtrooms? Retrieved March 28, 2020, from https://www.npr.org/2011/02/06/133497696/is-the-csi-effect-influencing-courtrooms

Selk, A. (2018) The ingenious and ‘dystopian’ DNA technique police used to hunt the ‘Golden State Killer’ suspect. *Washington Post*. Retrieved from https://www.washingtonpost.com/news/true-crime/wp/2018/04/27/golden-state-killer-dna-website-gedmatch-was-used-to-identify-joseph-deangelo-as-suspect-police-say/?utm_term=.2f38c4320092

Van Ness, L. (2020, February 20). DNA Databases Are Boon to Police But Menace to Privacy, Critics Say. Retrieved April 30, 2020, from https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/02/20/dna-databases-are-boon-to-police-but-menace-to-privacy-critics-say

Vallor, S. (2018). *Technology and the virtues: a philosophical guide to a future worth wanting*. New York: Oxford University Press.

carolynstoverharvey@yahoo.com