The War Over Genetic Privacy Is Just Beginning

Description

“When you upload your DNA, you’re potentially becoming a genetic informant on the rest of your family.”— Law professor Elizabeth Joh

“Guilt by association” has taken on new connotations in the technological age.

All of those fascinating, genealogical searches that allow you to trace your family tree by way of a DNA sample can now be used against you and those you love.

As of 2019, more than 26 million people had added their DNA to ancestry databases. It’s estimated those databases could top 100 million profiles within the year, thanks to the aggressive marketing of companies such as Ancestry and 23andMe.

It’s a tempting proposition: provide some mega-corporation with a spit sample or a cheek swab, and in return, you get to learn everything about who you are, where you came from, and who is part of your extended your family.

The possibilities are endless.

You could be the fourth cousin once removed of Queen Elizabeth II of England. Or the illegitimate grandchild of an oil tycoon. Or the sibling of a serial killer.

Without even realizing it, by submitting your DNA to an ancestry database, you’re giving the police access to the genetic makeup, relationships and health profiles of every relative—past, present and future—in your family, whether or not they ever agreed to be part of such a database.

After all, a DNA print reveals everything about “who we are, where we come from, and who we will be.”

It’s what police like to refer to a “modern fingerprint.”

Whereas fingerprint technology created a watershed moment for police in their ability to “crack” a case, DNA technology is now being hailed by law enforcement agencies as the magic bullet in crime solving.

Indeed, police have begun using ancestry databases to solve cold cases that have remained unsolved for decades.

For instance, in 2018, former police officer Joseph DeAngelo was flagged as the notorious “Golden State Killer” through the use of genetic genealogy, which allows police to match up an unknown suspect’s crime scene DNA with that of any family members in a genealogy database. Police were able to identify DeAngelo using the DNA of a distant cousin found in a public DNA database. Once police narrowed the suspect list to DeAngelo, they tracked him—snatched up a tissue he had tossed in a trash can—and used his DNA on the tissue to connect him to a rash of rapes and murders from the 1970s and ‘80s.

Although DeAngelo was the first public arrest made using forensic genealogy, police have identified more than 150 suspects since then. Most recently, police relied on genetic genealogy to nab the killer of a 15-year-old girl who was stabbed to death nearly 50 years ago.

Who wouldn’t want to get psychopaths and serial rapists off the streets and safely behind bars, right? At least, that’s the argument being used by law enforcement to support their unrestricted access to these genealogy databases.

“In the interest of public safety, don’t you want to make it easy for people to be caught? Police really want to do their job. They’re not after you. They just want to make you safe,” insists Colleen Fitzpatrick, a co-founder of the DNA Doe Project, which identifies unknown bodies and helps find suspects in old crimes.

Except it’s not just psychopaths and serial rapists who get caught up in the investigative dragnet.

Anyone who comes up as a possible DNA match—including distant family members—suddenly becomes part of a circle of suspects that must be tracked, investigated and ruled out.

Although a number of states had forbidden police from using government databases to track family members of suspects, the genealogy websites provided a loophole that proved irresistible to law enforcement.

Hoping to close that loophole, a few states have started introducing legislation to restrict when and how police use these genealogical databases, with Maryland requiring that they can only be used for serious violent crimes such as murder and rape, only after they exhaust other investigatory methods, and only under the supervision of a judge.

Yet the debate over genetic privacy—and when one’s DNA becomes a public commodity outside the protection of the Fourth Amendment’s prohibition on warrantless searches and seizures—is really only beginning.

Certainly, it’s just a matter of time before the government gets hold of our DNA, either through mandatory programs carried out in connection with law enforcement and corporate America, by warrantlessly accessing our familial DNA shared with genealogical services such as Ancestry and

23andMe, or through the collection of our “shed” or “touch” DNA.

According to research published in the journal Science, more than 60 percent of Americans who have some European ancestry can be identified using DNA databases, even if they have not submitted their own DNA. According to law professor Natalie Ram, one genealogy profile can lead to as many as 300 other people.

That’s just on the commercial side.

All 50 states now maintain their own DNA databases, although the protocols for collection differ from state to state. Increasingly, many of the data from local databanks are being uploaded to CODIS (Combined DNA Index System), the FBI’s massive DNA database, which has become a de facto way to identify and track the American people from birth to death.

Even hospitals have gotten in on the game by taking and storing newborn babies’ DNA, often without their parents’ knowledge or consent. It’s part of the government’s mandatory genetic screening of newborns. In many states, the DNA is stored indefinitely.

What this means for those being born today is inclusion in a government database that contains intimate information about who they are, their ancestry, and what awaits them in the future, including their inclinations to be followers, leaders or troublemakers.

Get ready, folks, because the government— helped along by Congress (which adopted legislation allowing police to collect and test DNA immediately following arrests), President Trump (who signed the Rapid DNA Act into law), the courts (which have ruled that police can routinely take DNA samples from people who are arrested but not yet convicted of a crime), and local police agencies (which are chomping at the bit to acquire this new crime-fighting gadget)—has embarked on a diabolical campaign to create a nation of suspects predicated on a massive national DNA database.

Referred to as “magic boxes,” Rapid DNA machines—portable, about the size of a desktop printer, highly unregulated, far from fool-proof, and so fast that they can produce DNA profiles in less than two hours—allow police to go on fishing expeditions for any hint of possible misconduct using DNA samples.

Journalist Heather Murphy explains: “As police agencies build out their local DNA databases, they are collecting DNA not only from people who have been charged with major crimes but also, increasingly, from people who are merely deemed suspicious, permanently linking their genetic identities to criminal databases.”

The ramifications of these DNA databases are far-reaching.

At a minimum, they will do away with any semblance of privacy or anonymity. The lucrative possibilities for hackers and commercial entities looking to profit off one’s biological record are endless.

Moreover, while much of the public debate, legislative efforts and legal challenges in recent years have focused on the protocols surrounding when police can legally collect a suspect's DNA (with or withouta search warrant and whether upon arrest or conviction), the question of how to handle "shed" or"touch" DNA has largely slipped through without much debate or opposition.

As scientist Leslie A. Pray notes:

We all shed DNA, leaving traces of our identity practically everywhere we go. Forensic scientists use DNA left behind on cigarette butts, phones, handles, keyboards, cups, and numerous other objects, not to mention the genetic content found in drops of bodily fluid, like blood and semen. In fact, the garbage you leave for curbside pickup is a potential gold mine of this sort of material. All of this shed or so-called abandoned DNA is free for the taking by local police investigators hoping to crack unsolvable cases. Or, if the future scenario depicted at the beginning of this article is any indication, shed DNA is also free for inclusion in a secret universal DNA databank.

What this means is that if you have the misfortune to leave your DNA traces anywhere a crime has been committed, you've already got a file somewhere in some state or federal database—albeit it may be a file without a name. As Heather Murphy warns in the New York Times: "The science-fiction future, in which police can swiftly identify robbers and murderers from discarded soda cans and cigarette butts, has arrived… Genetic fingerprinting is set to become as routine as the old-fashioned kind."

Even old samples taken from crime scenes and "cold" cases are being unearthed and mined for their DNA profiles.

Today, helped along by robotics and automation, DNA processing, analysis and reporting takes far less time and can bring forth all manner of information, right down to a person's eye color and relatives. Incredibly, one company specializes in creating "mug shots" for police based on DNA samples from unknown "suspects" which are then compared to individuals with similar genetic profiles.

If you haven't yet connected the dots, let me point the way.

Having already used surveillance technology to render the entire American populace potential suspects, DNA technology in the hands of government will complete our transition to a suspect society in which we are all merely waiting to be matched up with a crime.

No longer can we consider ourselves innocent until proven guilty.

Now we are all suspects in a DNA lineup until circumstances and science say otherwise.

Suspect Society, meet the American police state.

Every dystopian sci-fi film we've ever seen is suddenly converging into this present moment in a dangerous trifecta between science, technology and a government that wants to be all-seeing, all-knowing and all-powerful.

By tapping into your phone lines and cell phone communications, the government knows what you say. By uploading all of your emails, opening your mail, and reading your Facebook posts and text messages, the government knows what you write. By monitoring your movements with the use of license plate readers, surveillance cameras and other tracking devices, the government knows where you go.

By churning through all of the detritus of your life—what you read, where you go, what you say—the government can predict what you will do. By mapping the synapses in your brain, scientists—and in turn, the government—will soon know what you remember.

And by accessing your DNA, the government will soon know everything else about you that they don't already know: your family chart, your ancestry, what you look like, your health history, your inclination to follow orders or chart your own course, etc.

Of course, none of these technologies are foolproof.

Nor are they immune from tampering, hacking or user bias.

Nevertheless, they have become a convenient tool in the hands of government agents to render null and void the Constitution's requirements of privacy and its prohibitions against unreasonable searches and seizures.

What this amounts to is a scenario in which we have little to no defense of against charges of wrongdoing, especially when "convicted" by technology, and even less protection against the government sweeping up our DNA in much the same way it sweeps up our phone calls, emails and text messages.

With the entire governmental system shifting into a pre-crime mode aimed at detecting and pursuing those who "might" commit a crime before they have an inkling, let alone an opportunity, to do so, it's not so far-fetched to imagine a scenario in which government agents (FBI, local police, etc.) target potential criminals based on their genetic disposition to be a "troublemaker" or their relationship to past dissenters.

Equally disconcerting: if scientists can, using DNA, track salmon across hundreds of square miles of streams and rivers, how easy will it be for government agents to not only know everywhere we've been and how long we were at each place but collect our easily shed DNA and add it to the government's already burgeoning database?

Not to be overlooked, DNA evidence is not infallible: it can be wrong, either through human error, tampering, or even outright fabrication, and it happens more often than we are told. The danger, warns scientist Dan Frumkin, is that crime scenes can be engineered with fabricated DNA.

Now if you happen to be the kind of person who trusts the government implicitly and refuses to believe it would ever do anything illegal or immoral, then the prospect of government officials—police,

especially—using fake DNA samples to influence the outcome of a case might seem outlandish.

Yet as history shows, the probability of our government acting in a way that is not only illegal but immoral becomes less a question of “if” and more a question of “when.”

With technology, the courts, the corporations and Congress conspiring to invade our privacy on a cellular level, suddenly the landscape becomes that much more dystopian.

by John W. Whitehead & Nisha Whitehead

Date Created
06/11/2021