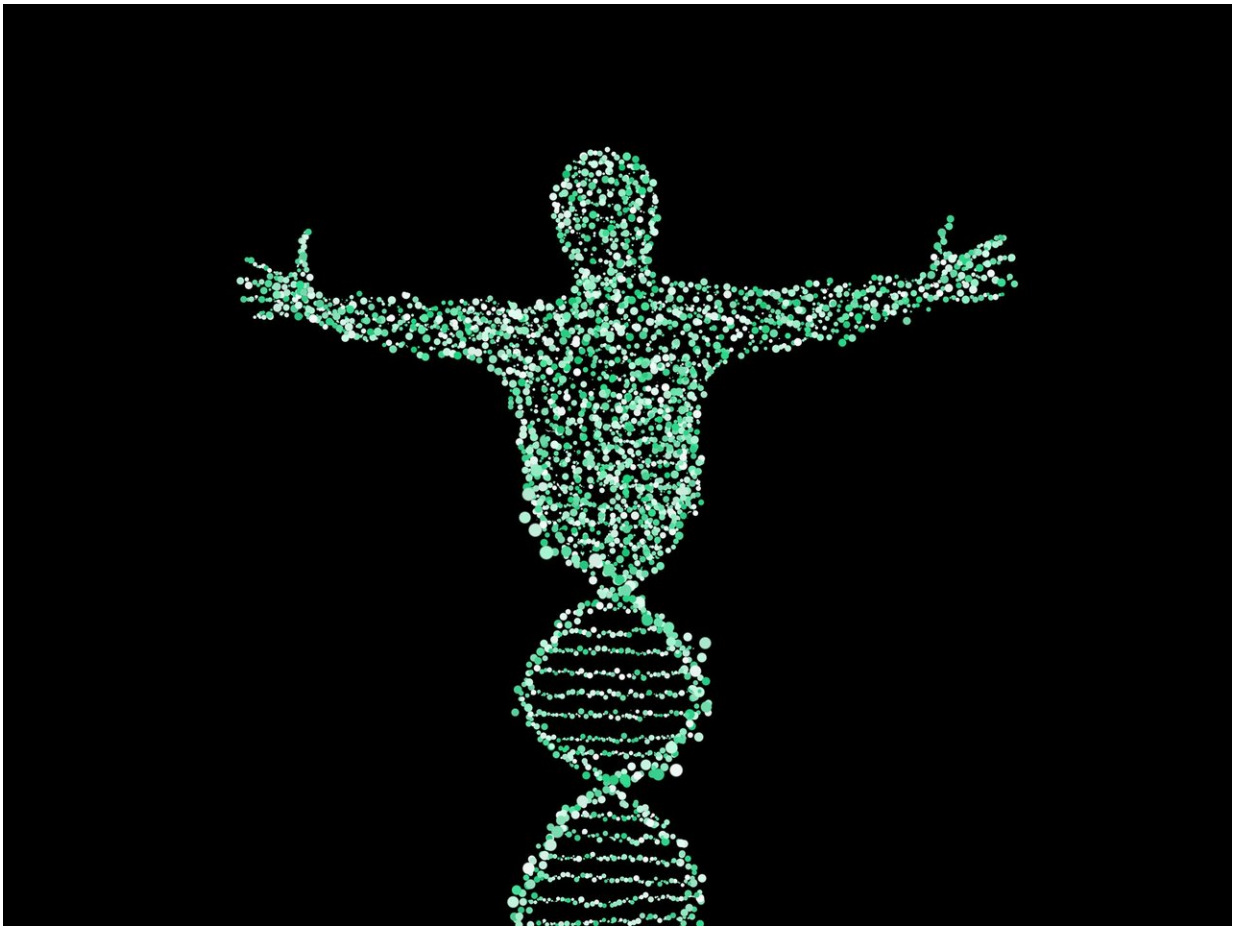
DNA testing can share all your family secrets. Are you ready for that?

July 4 2019, by Edward C. Baig, Usa Today



Credit: CC0 Public Domain

DNA testing is all about unlocking secrets. But sometimes surrendering

your saliva may also mean surrendering a bit of privacy—yours or someone else's.

"I think people need to be prepared and warned that they might find out something that could make them very uncomfortable," said Jeff Hettinger, one of the growing number of people who submitted a sample and discovered a sibling he never knew existed. His dad had never told him.

DNA testing from the likes of leading services 23andMe and Ancestry, among others, has always boiled down to risk and reward, a fascination and curiosity about one's roots and/or predispositions to disease, balanced against trepidations around privacy, security, and, for sure, the possibility of an awkward or identity-altering discovery.

And yet rising concerns of data breaches or an overreach by law enforcement have made some people reticent about voluntarily spitting into a tube or taking a swab of the cheek, even as this popular pastime continues to grow.

It also has some of the top DNA testing companies in the industry banding together to put privacy front and center.

MIT Technology Review estimates more than 26 million people have taken an in-home ancestry test.

The DNA risks to uncovering secrets

But experts counsel DNA newbies to consider what for some could turn into an unpleasant flip side.

"Are there secrets in the family?" asks Whitney Ducaine, director of cancer genetics services at InformedDNA in St. Petersburg, Florida, who

knows of cases where individuals found out they had no biological connection to people they had believed were blood relatives.

James Hazel, research fellow at Vanderbilt University Medical Center, raises another issue that may cut both ways: "The ability of people to readily identify anonymous sperm donors who wished to remain anonymous when they provided that sample."

On the health front, 23andMe asks customers to affirmatively "opt-in" before receiving sensitive reports that may show a genetic predisposition for BRCA variants, which may indicate an increased cancer risk, or late-onset Alzheimer's Disease, says Adriana Beach, the company's corporate counsel for privacy.

Could someone steal my identity from DNA details?

Meanwhile, frequent reports of database ruptures in all areas of tech and business are likely to give pause to people wondering about genealogy data landing in the hands of identify thieves and scam artists. Seeking out distant relatives also means you, or your data, may have to be exposed to some degree, so that you, in turn, can be found.

A year ago, the MyHeritage testing service, acknowledged a breach of email addresses and "hashed," or scrambled, passwords of more than 92 million users that turned up on a private server the previous October.

The company's then-chief information security officer Omer Deutsch said that no other sensitive data, including family trees and DNA, was compromised since such data is stored on separate systems.

Still, the episode sounded alarm bells.

"We haven't really seen any reporting surrounding a security breach

involving the genetic data of customers in the United States with any of these large ancestry or health-testing companies," Hazel says. But "as the databases grow in size, they represent an increasingly valuable target to potential hackers or others who may wish to gain access to that info."

Even so Hazel and others think the greater risk to privacy and security is more likely to come not from genetics data, but from all the other information that can be found on the internet, including social security numbers, passport information, financial records.

"If someone wanted to work with you on identify theft, there are a lot of easier ways to do it then to try to figure out your great-grandparents," agrees David Nicholson, co-founder of the Living DNA testing service in the U.K.

When police use these DNA databases

Privacy advocates have also flagged major concerns around the use of DNA by law enforcement.

DNA forensics have helped solve decades-old cold cases, leading notably to the arrest of the suspected "Golden State Killer" in California.

Investigators were able to uncover clues via the public database GEDMatch, which hosts data people voluntarily upload from private testing services as a way to find matches with potential relatives who tested their DNA elsewhere.

The worry, though, is that by permitting law enforcement to poke around such DNA databases, a legal shadow may be cast over innocent family members, some of whom never even submitted their DNA anywhere, much less gave their blessing to be searched by the police.

"You decide to contribute your DNA to one of these services and you have by default included your parents, your siblings if you have any, your kids if you have any or your future kids, and future nieces, nephews and everybody else," says Jen King, director of consumer privacy at Stanford Law School's Center for Internet and Society.

Family TreeDNA faced a backlash earlier this year after acknowledging that it cooperated with the FBI on crime solving. The authorities were able to set up profiles on the site hoping to match DNA samples collected from crime scenes.

But I didn't sign up for this...

Family TreeDNA subsequently changed its privacy policy allowing users to opt out so that their DNA could not be matched up against such profiles.

GEDMatch also recently changed its policy. It now requires people to specifically state if they'll allow their information to be shared with law enforcement.

"Prior to that time, we had always warned our users in our terms of service that our site might be used by some for purposes other than genealogy," says co-creator Curtis Rogers, who insists there are many misconceptions about GEDMatch.

"Criminal suspects are not identified on our database," Rogers says. Rather, "genetic genealogy is only the beginning of a long-complicated process that if ultimately successful will lead to a person or persons of interest. Law enforcement still have to do a complete investigation, often including getting a traditional DNA sample, before they can name a suspect and make an arrest."

Such investigations may involve social media, census data, family trees, newspaper articles, cemetery records, and courthouse records.

Rogers adds that the family history site surfaces matches, not the DNA itself, the raw data of which is encrypted and used to determine those matches.

For its part, Ancestry, which has sold more than 15 million DNA kits, insists on a search warrant or court order if investigators request DNA data on a customer, says chief privacy officer Eric Heath. Even then the company may challenge the order. Were that to happen, Heath says, it will notify the customer in question, unless ordered otherwise by the courts.

The reality is such requests are rare.

In its 2018 transparency report, Ancestry says it received just 10 "valid" requests from law enforcement for user information. It provided information on 7 of those requests, all related to investigations involving credit card misuse, fraud, and identity theft. The report indicated that Ancestry received no valid requests for information related to genetic information of any member and the company did not disclose any such information to law enforcement.

It added that as of the end of last year, Ancestry has never received a classified request related to the national security laws of the U.S. or any other nation.

In its own transparency report, 23andMe also said it hasn't received such a national security request. It too resists law enforcement requests when legally possible.

Promoting privacy around DNA

Last year, Ancestry, 23andMe, Helix, MyHeritage, Habit, African Ancestry and Living DNA joined up with the non-profit The Future of Privacy Forum around a set of best practices for consumer genetic testing services. Among them: The companies agreed to promote transparency, while also giving consumers control over how their data is collected, accessed, corrected, used in research, and deleted.

Around those same guidelines, Ancestry, 23andMe and Helix earlier this month formed The Coalition For Genetic Data Protection to lobby "for reasonable and uniform privacy regulation that will ensure the responsible and ethical handling of every person's genetic data."

"We understand that the trust of our users is paramount to the success of the business," Heath of Ancestry says.

Heath advises consumers considering this or that DNA service to read the terms and conditions and privacy policies posted on each site, something people typically ignore or have trouble understanding on most sites.

"In as much as people get freaked out about DNA, this might be one where it would behoove you to read those documents," he says.

Vanderbilt's Hazel concurs.

In 2017, he researched the policies of 90 companies in the DNA space. Results were all over the map: 40% had either no policy available to consumers on their website or policies that did not even mention genetic testing or genetic data. Among the companies that even had a visible policy, some boiled down to a vague sentence or two though Hazel notes that 23andMe posted a far more comprehensive if at times difficult to comprehend policy.

Know who you're doing business with

His research also pointed to a large subset of companies that permit surreptitious genetic testing where people could submit DNA samples that were not their own —maybe collected off a spouse's underwear to catch the partner cheating or to covertly determine the parentage of a child.

(A Google search for "infidelity testing DNA" pulls up a number of these companies.)

Nicholson of Living DNA also urges consumers to check out the privacy policies of the companies. He says companies that may sell DNA testing at a much lower cost compensate by attempting to monetize the data.

"Are you looking for a service as cheap as possible but (one where) your data may be shared or sold? Or are you looking for a company (like ours) where you may pay a little bit more, but that data is private, safe and secure?" Living DNA test kits cost between $99.

Even as he hasn't taken any steps to further unravel the secrets of his unknown half-brother, Hettinger has no second thoughts about his 23andMe test. "I would still do it and I would still encourage others to do it," says the 49-year-old from Atlanta.

Tracing your family and health roots via DNA can bring rich rewards. Just make sure those rewards match your tolerance for risk, privacy, and awkward surprises.