TIME

A DNA Site Helped Authorities Crack the Golden State Killer Case. Here's What You Should Know About Your Genetic Data Privacy

By **JAMIE DUCHARME** April 27, 2018

TIME Health *For more, visit TIME Health.*

Police this week arrested a man suspected to be the notorious Golden State Killer with the help of a resource they could only have dreamed of in the 1970s, when a gruesome spree of rapes and murders began terrorizing California: databases filled with individuals' genetic data.

Genetic information listed in a largely unknown, open-source genetic database called GEDmatch proved instrumental in cracking the case, *the Mercury News* reports. Investigators used genetic databases to find relatives who matched genetic material taken from an old crime scene, the Sacramento *Bee* reports. They then cross-referenced family data from GEDmatch, potentially bolstered by that from other databases, with evidence gathered by investigators, eventually pinpointing and arresting a suspect: 72-year-old former police officer Joseph James DeAngelo.

Investigators were able to use GEDmatch, which says it has between 900,000 and a million users, so easily because — unlike with commercial companies such as 23andMe, which in comparison boasts more than 5 million users — individuals upload and share their information for free, making it accessible to law enforcement, researchers and private citizens alike. Nonetheless, the case has thrust the issue of genetic privacy into the spotlight, particularly as direct-to-consumer tests become both increasingly popular and increasingly extensive in their insights. Millions of Americans have spit into tubes and pricked their fingers and swabbed their cheeks in pursuit of knowledge about their health and family history — but how many have considered what happens to that data next? And how important is it that they do?

"I would say consumers should not be worried, but they should be aware," says Dr. Robert Green, a medical geneticist at Brigham and Women's Hospital and Harvard Medical School. "It's not necessarily a reason for concern, because we haven't seen, to my knowledge, abuses of these databases. We have seen appropriate uses by law enforcement. I think we're all glad a serial killer was caught."

While the circumstances may not have been as high-profile, most of the big-name genetic testing companies have previously been called upon to cooperate with legal investigations. Not all requests are honored — many aren't, as STAT reports — but most companies clearly warn customers that it's a possibility.

A representative for 23andMe, probably the biggest player in the space, tells TIME that, "Broadly speaking, it's our policy to resist all law enforcement

inquiries to protect customer privacy. 23andMe has never given customer information to law enforcement officials."

Even still, a post on the company's website warns customers that, "Under certain circumstances, your information may be subject to disclosure pursuant to a judicial or other government subpoena, warrant or order, or in coordination with regulatory authorities." Competitors such as Ancestry, Helix, MyHeritage, Family Tree DNA and Orig3n all have similar advisories readily available on their websites, and many allow users to control where their data goes, consenting to sharing it for research, with third parties or with other consumers.

The equation is different when it comes to open-source platforms such as GEDmatch. Sharon Zehe, an attorney for the Department of Laboratory Medicine and Pathology at Mayo Clinic and a genetic privacy expert, urges caution when it comes to these sites. "A DNA sequence is the biometric equivalent of a fingerprint," Zehe says. "Would they load their fingerprints onto a publicly available database? Probably not."

GEDmatch, for its part, told TIME that, "Although we were not approached by law enforcement or anyone else about this case or about the DNA, it has always been GEDmatch's policy to inform users that the database could be used for other uses, as set forth in the Site Policy. While the database was created for genealogical research, it is important that GEDmatch participants understand the possible uses of their DNA, including identification of relatives that have committed crimes or were victims of crimes. If you are concerned about non-genealogical uses of your DNA, you should not upload your DNA to the database and/or you should remove DNA that has already been uploaded."

Whether customers read these warnings, of course, is another matter. Zehe says she's seen them become clearer and easier to understand as privacy concerns mount, but stresses that consumers should "be thoughtful about reading privacy policies and understanding how genetic data is shared with third parties."

Even if people don't read the privacy policies, Green says the situation isn't so different from using search engines or social media — two actions that have certainly been plagued by data scandals of their own, but that most people still continue to do on a daily basis.

"Genetics is a particularly sensitive arena for people to think about and talk about, but I don't think all of this is exclusive to genetics," Green says. "If you're going to live in this society, you're going to take part in search engines, you're going to take part with credit cards, it's very hard to stay off the grid. I think that applies now genomically."

That's particularly true as more and more people use genetic testing and sharing services, allowing them to accumulate more robust databases, Green says.

"If your relatives have contributed and then you are part of even a family tree that appears online in one of these shared resources, you can be indirectly

tracked through the combination of their DNA and the publicly available family history," Green says. "If you've never participated in one of these services but someone else lists you as a family member because they're doing genealogy and they have participated, now someone can find you, even though you've never participated."

Green allows that this makes the privacy issue significantly murkier — "terms of service don't apply" if you haven't voluntarily submitted your DNA, after all — but again says it's not all that unique. Any time a doctor asks for your family history, for example, you're essentially exposing someone else's sensitive personal data. But while this information is protected by medical privacy laws, internet genealogies are not.

The bottom line, Green says, is that the potential for abuse of genetic material exists — he offers as examples insurance companies refusing coverage based on genetic data found online, or genomic information being used to smear opponents in legal disputes such as divorces — but the systems in place to prevent this misuse appear to be working. One is the Genetic Information Nondiscrimination Act, a federal law known as GINA, which was passed in 2008 specifically to protect consumers from issues such as these. And as long as that's the case, he says, the good seems to outweigh the bad.

"Absent examples of abuse, or clear-cut potential for abuse, or loopholes that would allow abuse," Green says, "I think we ought to be very careful about jumping to the notion that we should restrict it."

Zehe takes a slightly more cautious approach.

"Genealogy services can be fun, but make sure you are using a reputable organization that has robust privacy policies in place," she says. "When in doubt, don't consent to other uses, or potentially don't use the direct-to-consumer service at all."