

Ethical Use of Home DNA Testing

Home DNA testing is a booming business. Millions of Americans have sent their DNA to commercial testing companies such as 23andMe or Ancestry to learn more about their heritage or potential for disease. According to Grand View Research, "the global DNA testing market is set to reach over \$10 billion by 2022." (Brown 2018). Successful marketing campaigns have led consumers to believe that home DNA testing is fun, informative, and personal to them. However, what consumers may not realize is that once their genetic information is shared, they have limited control as to who has access to it.

Regardless of the reason consumers decide to purchase a home DNA test kit, the information they provide to the testing company is far greater than the information they receive. The benefits that these testing companies can gain from gathering, using, and selling customers' private information places them in a significant conflict-of-interest situation. Some of this information includes the IP address, name, address, email, and family history, collected from the application, as well as information provided on follow up surveys. Furthermore, according to its website, if customers opt to share their data for research, 23andMe could keep their physical spit sample and the genetic data it contains for up to a decade. Additional information that consumers upload to the companies' genealogy website, such as pictures, obituaries, family relationships, and even third-party information is probably added to the pool of data linked to customers' DNA.

Recently, some have felt that privacy and consumer rights have been violated when they used home DNA kits. In June 2019, Lori Collett sued Ancestry for allegedly misleading customers about what it was doing with their DNA. This class action lawsuit claims that personal information was released to outside parties without customer consent. Further contentions include that the waiver of consumer rights through consent forms is often vague, general in scope, and ever-changing. The fine print may not accurately spell out what the company, its third-party associates, and collaborators can or will do with customer information. (Merken, 2019)

Further concerns arise as testing companies often align themselves with pharmaceutical companies, public and private research organizations, and Google. For example, "GlaxoSmithKline purchased a \$300 million stake in the company, allowing the pharmaceutical giant to use 23andMe's trove of genetic data to develop new drugs — and raising new privacy concerns for consumers." (Ducharme, 2018) Similarly, Ancestry is sharing its data with Google through its research subsidiary Calico. Ancestry admits that "once they share people's genetic information with partner companies, they can't be responsible for security protocols of those partners." (Leavenworth, 2018).

Additionally, both 23andMe and Ancestry use Google Analytics to provide third parties with consumer information for targeted marketing. In its privacy policy 23andMe states that "when you use our Services, including our website or mobile app(s), our third-party service providers may collect



Web-Behavior Information about your visit, such as the links you clicked on, the duration of your visit, and the URLs you visited." This use of shared information allows testing services and third parties to build a comprehensive personal profile on you, which may include your genetic information.

Although privacy may be a concern of consumers, law enforcement with the cooperation of DNA testing companies, either through partnership or warrants, have brought justice to the victims of numerous unsolved cases. Over the past few years the use of consumer DNA databases have closed many high profile cold cases such as the Golden State Killer and overturned the wrongful conviction of Alfred Swinton. In some cases, such as the Golden State Killer, the DNA used to identify suspects are cross referenced through the DNA of relatives as far removed as third cousins. However, this has brought additional concerns, as a DNA expert for the American Civil Liberties Union, Vera Eidelman states, "There's always a danger that things will be used beyond their initial targets, beyond their initial purpose." (St. John 2019)

The success of consumer DNA databases has led some law enforcement to meet with Bennett Greenspan, the CEO of FamilyTreeDNA, seeking his help to convince consumers to share their genetic data with police. This partnership has resulted in the creation of the non-profit Institute for DNA Justice that has the following stated mission:

The Institute for DNA Justice was formed 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, encourage the 26 million Americans who have taken a DNA test to become genetic witnesses by participating in publicly available family-matching databases working with law enforcement using IGG, and to promote the adoption of industry leading best practices guidelines surrounding its use by law enforcement agencies around the country.

Regardless of public or private testing, laws in the United States have not yet determined a standard for the home DNA testing industry.

Discussion Questions:

1. What happens to your DNA profile and genetic material if your testing company goes out of business? What should happen to it?
2. Who should have access to your genetic information? In the case of law enforcement using consumer DNA databases, does the common good out way the individual's rights? Is there a middle ground?
3. What right do individuals have over their DNA? If you have an identical twin, with the exact same DNA, should dual consent be required?
4. What recourse do you have if the company's database is hacked and your information ends up on the internet or in criminals' hands?
5. Does the good that flows from DNA evidence being used to bring some criminals to justice and to exonerate wrongly-convicted people justify the invasions of privacy and other wrongs described in this case study?

Resources:

Amy Brown, "DNA Testing is Popular, But Many Are Unaware of Privacy Concerns," TriplePundit, Dec. 18, 2018. <https://www.triplepundit.com/story/2018/dna-testing-popular-many-are-unaware-privacy-concerns/55936>

Jamie Ducharme, "A Major Drug Company Now Has Access to 23andMe's Genetic Data. Should You Be Concerned?" Time, July 26, 2018.

David Lazarus, "DNA-testing Firms are Lobbying to Limit Your Right to Genetic Privacy," Los Angeles Times, July 2, 2019.

Stuart Leavenworth, "The Secretive Google Subsidiary with Access to Ancestry's DNA Database," Financial Review, June 8, 2018. <https://www.latimes.com/business/lazarus/la-fi-lazarus-dna-genetic-privacy-20190702-story.html>

Sara Merken, "Ancestry.com Sued for 'Misleading' Customers About DNA Data," Bloomberg Law, April 25, 2019. <https://news.bloomberglaw.com/privacy-and-data-security/ancestry-com-sued-for-misleading-dna-data-handling-claims>.

Paige St. John, "DNA Genealogical Databases Are a Gold Mine for police, But with Few Rules and Little Transparency," Los Angeles Times, Nov. 24, 2019.

N'dea Yancey-Bragg, "DNA is Cracking Mysteries and Cold Cases. But is Genome Sleuthing the 'Unregulated Wild West?,'" USA Today, May 14, 2019.

"Privacy Highlights," <https://www.23andme.com/about/privacy/>

<https://www.institutefordnajustice.org/>

Author:

Chris Apgar and Robert Prentice
The University of Texas at Austin