

DNA Testing: Balancing Value and Privacy



How Secure Are Your DNA Test Results? What You Should Know About Privacy BEFORE You Take a DNA Test!

Recently, we sat down for an Interview with Chris Cummings, who is the Founder and CEO of Pass It Down to discuss the topic of privacy and DNA testing. Besides being a startup entrepreneur, Chris also brings a valuable legal background in Constitutional and Privacy law to the table. What he had to share with us should make anyone who has or is about to test their DNA research the privacy policy of the DNA testing company they are using.

Should anyone interested in personal DNA testing be concerned about their privacy when testing with the popular DNA companies such as 23andMe or Ancestry DNA?

I think people should certainly be concerned about their privacy and know the potential risks that come with any online service that is storing your information. One thing to always remember is that your information is only as safe as the site's security. Over the last two years, we've seen a number of major companies hacked, which resulted in **billions** of users' information being compromised. From Equifax, to Yahoo, to Uber, the threat of hacking is a real and growing threat online.

In fact, a University of Washington Study published in 2017 found that “the security practices of common, open-source DNA processing programs” were “in general, lacking.” The study found that “all that super-sensitive information those programs are processing is potentially vulnerable to hackers. If you think social security fraud is bad, imagine someone hacking your genetic code.” Separately, the University of Washington researchers studied how non-genetic information was being stored and found it's also vulnerable to malware.

In addition, it's important to review the privacy policies of 23andMe or Ancestry DNA which do raise some red flags. For example, while Ancestry revised its privacy policy in 2017 to state it "does not claim any ownership rights in the DNA that is submitted for testing," another clause gives Ancestry an incredible amount of power over your own DNA.

"By submitting DNA to AncestryDNA, you grant AncestryDNA and the Ancestry Group Companies a royalty-free, worldwide, sublicensable, transferable license to host, transfer, process, analyze, distribute, and communicate your Genetic Information for the purposes of providing you products and services, conducting Ancestry's research and product development, enhancing Ancestry's user experience, and making and offering personalized products and services."

Overall, I think that the DNA testing companies do a pretty good job when it comes to privacy, but I think consumers should be aware of the risks.

Would a consumer be better off working with a professional genetics testing company? Are there any better privacy protections when using a service that doesn't offer "data matching" for family history purposes?

I think the safest genetic testing option in regards to protecting your privacy is to use a service that doesn't offer data matching. One option might be to work with a company like FuturaGenetics who prioritizes privacy and data protection. Their CEO, Auro Pontes has stated that *"it is important for us that you feel relaxed and safe. That's why our company's politics are transparent. On the contrary, any personal information [is] subject to the highest levels of data protection. Your privacy is our legacy."*

For example, FuturaGenetics takes several steps to maintain privacy including 1) not disclosing private information via email, 2) keeping your genetic information and personal identity stored separately and 3) destroying your DNA sample after the test is done.

While DNA testing is exciting and has the potential to break through some of those brick walls, a consumer should keep the risks in mind as well, particularly in regards to potential insurance consequences.

Do the DNA testing companies sell your DNA data to third party companies? And what type of data? Is it all of your information or a metadata extract to look at data statistics and trends?

The quick answer is yes. Ancestry, 23andMe, MyHeritage and Family Tree all reserve the rights to sell your information in their Terms and Conditions or Privacy Policy, but you have to opt in or give them consent to do so.

If you do choose to opt in, your information could be sold and used but maybe not in the ways you are imagining. For example, 23andMe is selling your information but it's primarily for research partnerships with entities like Genentech, Stanford and the Michael J. Fox Foundation.

DNA testing companies are forming research partnerships because it has incredible potential to evolve the way that doctors treat diseases. 23andMe partnered with the Michael J.Fox Foundation because it "will help [23andMe's] research goals of understanding, treating and preventing this disease," said Anne Wojcicki, 23andMe CEO and co-founder. "Making the data available to the wider research community will accelerate our understanding of Parkinson's disease."

If you have opted in and have concerns, then do know that you typically have the ability to opt out. For example, Ancestry's terms provide that:

Yes, you can withdraw your consent at any time on the AncestryDNA settings page. Until you withdraw or we end the Project, there is no limit to how long we will use your Biological Samples and Data for the Project. If you withdraw, we will cease using your Data for the Project within 30 days and the Data will not be used in future research. However, Data cannot be withdrawn from research already in progress or completed, or from published results and findings. In those cases, Researchers may have access to such Data about you indefinitely. There is no negative impact to you for withdrawal of your consent, and you will continue to be able to use our Services as before. Withdrawing your consent will not result in destruction of your DNA Sample or deletion of your Data from AncestryDNA products and services, unless you direct us otherwise. If you want your DNA Sample destroyed or your Data deleted from AncestryDNA products and services, we will promptly do so at your request but additional steps are required. Please contact Member Services at the applicable number below for assistance.

This Informed Consent does not have an expiration date. If you do not withdraw consent, it will remain in effect until you withdraw or we end the Project.

One company that has raised concerns from DNA experts is Family Tree DNA. Why? Well, their terms provide that "your participation in these initiatives is entirely voluntary and your DNA test results will not be used or disclosed without your consent. **Once given, however, consent cannot be revoked.**"

Law enforcement: do they have access to your DNA test data? Can your data be used in legal or criminal proceedings?

I think anyone purchasing a DNA Test should be aware there is a risk your information could be turned over in a legal proceeding and the government has shown a strong interest in DNA. Five years ago, the United States Federal Government won a huge case called Maryland v. King at the United States Supreme Court. In Maryland v. King, the government successfully argued that they have the right to take the DNA of anyone who is arrested for a serious offense and that no citizen has the right to refuse because your DNA is being taken for "identification purposes." What you should know, is that 1) this case illustrates how much the government and law enforcement wants your DNA (a lot) and 2) that this case opens the door for anyone's DNA to be taken if arrested, even for minor offenses.

Why would law enforcement want your DNA? Across the country, there are DNA Databases for every state and there are also national databases where DNA is stored. These databases are maintained to preserve DNA that's been found in relation to a crime and the hope is that the DNA evidence will help in someday closing these cases.

Genetic information is incredibly valuable to law enforcement because it gives them the ability to search to see if you, or a relative, is potentially linked to any cold crimes in the past.

For example, in 2014 the Idaho Falls Police Department was trying to crack a 20-year-old murder and issued a subpoena to Ancestry.com to conduct a “familial DNA search.” A familial DNA Search is a “search by law enforcement in DNA databases for genetic information indicating a relative of a person they seek to identify.” That test led the police to suspect that Michael Usry, Jr. was the perpetrator. While Michael Usry, Jr. was eventually found to be innocent, it's important to know he became a suspect because of DNA that was stored from a personal genetic test.

I would encourage everyone to read 23andMe and Ancestry's guides for Law Enforcement here:

- [23andMe Guide For Law Enforcement](#)
- [Ancestry Guide For Law Enforcement](#)

One positive thing to note is that both companies indicate they will fight for user rights and resist overly broad searches. In fact, 23andMe has already successfully resisted five requests for information from police departments.

Insurance companies: what is stopping insurance companies, including health, life and even auto, from using your DNA data to set insurance rates or even deny you coverage?

If there is one area that should give you pause about personal genetic testing, it's insurance. The Electronic Frontier Foundation (EFF) has found that the existing laws dealing with DNA fall very short of protecting user privacy and pose some major unaddressed issues.

The Genetic Information Nondiscrimination Act of 2008 (“GINA”) are the federal laws that deal with genetic information. As the EFF notes,

GINA is essentially an anti-discrimination law that has nothing to do with privacy. It prevents group health and Medicare supplemental plans—but not life, disability, or long-term care plans—from using genetic information to discriminate against you when it comes to insurance.

The problem is there are gaps in the law that do not cover life, long-term care or disability insurance providers. What this means is that if you choose to share your genetic information with your doctor, a health care provider or even friends and family **it can be used against you**. Don't believe me? 23andMe's [Terms of Service](#) specifically state that *"if you are asked by an insurance company whether you have learned Genetic Information about health conditions and you do not disclose this to them, this may be considered to be fraud."*

To be clear, your genetic information could be used by insurance companies to deny you coverage or raise your rates. What the insurance industry fears is ["Asymmetry of information- when the customer knows more than the insurer."](#)

Can our legislators help with the privacy issue? What current legislation exists and/or is anticipated?

Yes, our legislators can help with privacy issues significantly and you should be calling your local representatives to push for changes. [One option would be to follow the lead of France, Sweden and Austria](#) by prohibiting insurers from using genetic information. There is one big potential downside here... the insurance companies may just raise your premiums to ["cover the known unknown."](#)

One other option comes from the United Kingdom where their laws allow insurers access to genetic information with the caveat that it can only be used to help underwrite customers' coverage. In the US, California is leading the way in expanding privacy laws for genetic testing, and I think the other 49 states should follow suit.

Finally, are there any future developments you foresee in terms of protecting our DNA data and privacy? Could blockchaining, the data mechanism behind cryptocurrency, assist in tracking ownership of use of DNA data?

Yes, there is a company called [EncrypGen](#) that is using blockchain security to protect genomic data. Essentially, by storing your DNA information in blockchain, you have the ability to keep this information secure and/or allow others access in exchange for payment. Over the next ten years, I believe you will see growth in this area as it's actually one of the best use cases for blockchaining currently. Blockchain technology has incredible potential to transform the way we keep our DNA secure.

About Chris Cummings



Chris Cummings is the Founder & CEO of [Pass It Down](#), an award-winning storytelling company that helps families, businesses, and communities around the world bring their stories to life. Prior to founding Pass It Down, Chris received his JD from the Paul M. Hebert LSU Law Center and has clerked for numerous judges, including the honorable Chief Justice Johnson of the Louisiana Supreme Court. Chris is a panelist for the Federal Public Defender's office on both the Trial and Appellate level. Chris specializes in Constitutional and Privacy law.

PLEASE NOTE: *The post content above contains affiliate links. This means I make a percentage of sales via these links. This does not INCREASE the price you pay as a consumer. It simply supplements my income so I can continue providing as much free genealogy content as possible through my “abundance model.”*

Disclaimer: *All prices and offers are subject to change. Some items may be sold out and have limited inventory. Also check to see if you have automated purchase settings enabled, such as Amazon Buy with 1-Click: it is your responsibility to make sure you are getting the correct price for an item before you check out and finalize the transaction.*

Disclosure statement: *I have material connections with various vendors and organizations. To review the material connections I have in the genealogy industry, please see [Disclosure Statement](#).*

©2018, copyright Thomas MacEntee. All rights reserved.