Why You Should Think Twice About Having Your DNA Tested

May 14, 2016 â€“ Personal DNA tests are the rage right now. Websites like 23AndMe.com and Ancestry.com have national advertising campaigns devoted them. By taking the test, you can find out things about your genetics â€“ what diseases you may be prone to â€“ and about your family history. But while that may sound absolutely great, there is also another consideration. Who else will be able to gain access to this information about you and what will they use this information for? As you read through this article, you may come to the same conclusion that I did when looking into the topic. Using one of these services to gain access to my DNA information could create a lot more problems than it is worth.

Anyone who is thinking about using a company to look at their DNA needs to do a little research first. And the place to start is with the companyâ€™s Privacy Policy and their Terms of Service. You need to understand that any company that is doing a lot of these tests may also be building a large database of DNA information. And any large database is a target for hackers. So not only is the privacy policy important, but so is the companyâ€™s network security. NOTE: These large databases are also of great interest to national governments.

Now you may be asking yourself why anyone would want to steel your DNA. Well, it is a biometric marker that clearly identifies you. In a recent hacking incident involving the US Office of Personnel Management, fingerprint and iris scan data was stolen on millions of government employees. The employees that had that data stored also had government issued security clearances. Once hackers gain access to this type of data, it is a fairly easy matter for them to be able to break into computer systems that use this data for access.

Since DNA is the holy grail of biometric markers, there is really no telling how it will eventually be used. And because of this, you have to assume that it is valuable to any hacker who can lay his hands on it.

But it isnâ€™t just hackers that you have to be concerned with. You also need to be worried about government use of these databases. The government doesnâ€™t need a search warrant to get its hands on information stored in corporate databases. In most cases, all that is required is a subpoena. That means no court supervision is required. Think about that for a minute.

If a local, state or federal law enforcement agency is trying to get their hands on your DNA, they typically need a court order to do so. Either that, or they need to go dumpster diving. But if you have had your DNA tested and stored in a corporate database, all that is needed is a subpoena. Moreover, this information is valuable to law enforcement even if you arenâ€™t the target of an investigation. Thatâ€™s because it can be used to establish familial relationships. Your DNA coul provide enough evidence for a court to compel one of your family members to submit to a test. Itâ€™s actually very Orwellian.

Now that you understand what is at stake, time to circle back to policies of any company you are considering using for that DNA test. A quick reading of the policies of 23AndMe.com and Ancestry.com will tell you that some companies have much more consumer friendly policies than others. In the case of Ancestry, the company will allow you to destroy your test results. They say that once you do that, the test results canâ€™t be recovered. But even here, the companyâ€™s DNA Privacy Policy states that your DNA test results may persist in the companyâ€™s systems for some time, and that if you shared your DNA information before deleting it, there may be duplicate copies.

On the other hand, 23AndMe Terms of Service say they may share your data for various reasons. One of those reasons is to comply with requests from law enforcement. And their â€œBiobanking Consent Documentâ€• states that they will keep your information for up to 10 years. Thatâ€™s a lot of exposure.

There are a lot of reasons that people may want to look into their DNA. But most of the good reasons have to do with health and medical conditions. Doing it just because you think it would be fun to know a little more about your family history could actually be a very bad idea. Anyone considering having this type of testing done should seriously consider the potential consequences.

As a final note, I donâ€™t have any information on the data security used by either of these companies mentioned here. It may be the best that money can buy. But it is important to note that hackers have repeatedly defeated state of the art data security deployed by some of the largest and most IT savvy companies on the planet. Because of this, I donâ€™t believe it is in anyoneâ€™s best interest to have their biometric data stored on an internet-accessible databaseâ€¦ with any company, for any reason.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS