

## Company Admits It Shared DNA Data With FBI

February 21, 2019 - We've been warning readers for a couple of years now that submitting DNA samples to private companies for analysis could lead to privacy invasions. Companies like 23andMe and Ancestry.com have been quite public about the DNA testing services that they offer. They sell their test to consumers by claiming they will make them aware of potential medical conditions, or reunite them with long lost family. But the reality is that when you submit a sample to one of these companies, law enforcement can gain access to it with a simple subpoenaâ€”at least, that used to be the reality. Now a company by the name of FamilyTreeDNA has made sharing your DNA and opt-out option. Put another way, they will share your DNA with law enforcement unless you tell them not to. That's a very frightening precedent.

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();
```

FamilyTreeDNA has admitted to the New York Times that it has shared information directly with the FBI, without requiring a search warrant or a subpoena. And that information is being used to track people down.

Now, we're not suggesting that putting criminals behind bars is a bad thing. As far as I know, absolutely everyone that I work with would view that as a positive. But sharing DNA data without specific permission from the person who donated it is very troubling. That's especially true when we don't really know what the future use for that data might be.

Once your information is shared, all control over it has been lost. You have absolutely no way of knowing if the FBI will actually share your data with other agencies or ever with other companies. And if they do, you have no idea how those organizations will use it.

As with other biometric data, once DNA is stored in a database, it is reduced to a series of numbersâ€”as all data is. And anything stored in a database can be replicated. Biometric markers such as DNA, retinal scans and even fingerprints are now regularly being used alongside technology in computers, security systems, etcâ€”The more databases your biometric data appears in, the greater the chances that it will be exposed to some unwanted third party. And the greater the chances are that it will come back to bite you at some point.

Anyone who provides DNA samples to a third party company is taking a real risk. Do so could well turn out to be one of those "curiosity killed the cat" sort of things. If you have long lost family out there somewhere, maybe there is a reason for them being "long and lost."

And any third party company that collects your data and then shares it without your permission is betraying a trust and they don't deserve your business. That's true even if they have the best of intentions. Our recommendation to our readers is think long and hard before you submit to one of these tests. You could wind up regretting your decision, and there is probably no way for you to reverse it.

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 ACCESS