The Privacy Implications of Rapid DNA Use

December 31, 2018 - When DNA first started being used to make identifications, it was a tedious process that could take months. But those time frames have dropped dramatically over the past several years. For several years now, some police departments have been using technology known as Rapid DNA (RDNA) to make identifications in just hours. Most recently, the technology has been used by first responders to identify victims in the California wild fires. But this year, the tech is going to be a lot more mainstream. The FBI is planning is building what it calls an RDNA network that will link with its criminal database. The network will allow police nationwide identify suspects in a matter of hours.

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);
})();

There is little doubt that the RDNA network will bring big benefits to law enforcement. Once implemented someone who is a rapist in one jurisdiction, but who is picked up for shoplifting several states over, is likely to be identified rather than being released. Nobody is going to argue about that being a bad thing. But what are the privacy implications of this type of database or the limitations on how it can be used? That's not something that anyone is talking about, but we should be.

Three quarters of the states currently allow DNA collection from people who have been arrested but who haven't been charged with a crime. And about half of them allow that DNA to be used by law enforcement immediately.

Once your DNA is added to the database, you've pretty well lost control of it. While some states allow you to have it removed through a court procedure, the effectiveness of having it removed is questionable. That's especially true if it is ever uploaded to a national database or other regional databases. You have to view it like the internet. Once your data is out there, it's probably out there for good. That's important because the technology is changing so quickly that we really don't know how it will be used ten years from now, or who will have the ability to use it. We already know that law enforcement agencies are now able to use close familial matches for DNA that they have samples of to find perpetrators that they don't have samples of.

The good news about RDNA is that it can't be used to build a profile of you. Currently, the technology is only good enough to match your DNA against the DNA of known individuals. But again, that's today. And that's very likely to change over the next decade.

As the uses for DNA increase, so does its value. That's true for each of us as individuals as well as for criminals. At some point, large DNA databases are likely to become attractive targets for criminal elements, just as credit card databases are. We need to make sure that this data is protected and encrypted. And we need to start having that conversation

sooner rather than later.
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